The Digital Manufacturing and Design (DiManD)

Grant agreement No 814078– H2020-MSCA-ITN European Training Network Grant

Deliverable 5.1

State-of-the-art on integration of cutting edge interoperability approaches in manufacturing and cyber-safety and security requirements

November 2020

Lead parties for Deliverable : UNINOVA
Deliverable due date : M19
Actual submission date : M19
Dissemination level : Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Table of Content

Acronyms

3GPP	3rd Generation Partnership Project
ACL	Agent Communication Language
AI	Artificial Intelligence
AM	Additive Manufacturing
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
CMI	Cyber-Machine Interface
CML	Context Modeling Language
CPS	Cyber-Physical Systems
CPPS	Cyber-Physical Production Systems
CSN.1	Concrete Syntax Notation One
DNS	Domain Name System
DPWS	Device Profile for Web Services
ERP	Enterprise Resource Planning
FaaS	Fog as a Service
FIPA	Foundation for Intelligent Physical Agents
GML	Generalized Markup Language
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IAS	Information Assurance and Security
ICT	Information and communications technology
IEC	International Electrotechnical Commission

IEEE	Institute of Electrical and Electronics Engineers
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of things
IIRA	Industrial Internet Reference Architecture
IMC-AESOP	ArchitecturE for Service-Oriented Process - Monitoring and Control
IMSA	Intelligent Manufacturing System Architecture
IoT	Internet of things
IP	Internet Protocol
IT	Information Technology
JADE	Java Agent Development Framework
JSON	JavaScript Object Notation
KQML	Knowledge Query Communication Language
MAS	Multi Agent Systems
MES	Manufacturing Execution Systems
NIST	National Institute of Standards and Technology
OEE	Overall Equipment Effectiveness
OEM	Original Equipment Manufacture
OPC	Open Platform Communication
OPC-UA	OPC Unified Architecture
P2P	Peer-to-Peer
PaaS	Platform as a Service
PLC	Programmable Logic Controller
PoW	Proof of Work
QC	Quality Control
R&D	Research and Development
RAMI 4.0	Reference Architecture Model Industrie 4.0
RDF	Resource Description Framework
RFID	Radio-Frequency Identification
SaaS	Software as a Service

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

SaaS	Software as a Service
SDN	Software Defined Networks
SGML	Standard Generalized Markup Language
SME	Smart Manufacturing Ecosystem
SOA	Service-Oriented Architecture
SOT	Service-Oriented Technologies
SQL	Structured Query Language
TCP	Transmission Control Protocol
XML	Extensible Markup Language
W3C	World Wide Web Consortium
WSN	Wireless Sensor Network
WIA-FA	Wireless networks for Industrial Automation-Factory Automation
WIA-PA	Wireless Networks for Industrial Automation and Process Automation
WSM	Web Services Management
WSN	Wireless Sensor Network

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Summary

The Global needs for higher efficiency, lower cost and mass personalization of products and services has transformed manufacturing from traditional automation pyramid for manufacturing control to an integrated network of automated devices and services. Recent advances in manufacturing like Cyber-Physical Systems, Cloud technologies and Artificial Intelligence has driven this evolution. This new manufacturing paradigm is called as smart manufacturing which calls for the integration of diverse and distributed services, enterprises, smart factories, smart devices, and processes. This integration requires seamless exchange of information between heterogeneous systems and arises an integration problem. Interoperability in smart manufacturing refers to the way how these services and devices exchange information and interact. This is still an exploratory topic and despite the increasing number of applications, many challenges remain open. This deliverable presents an integrative framework to understand common practices, concepts and technologies used in trending research to achieve interoperability in production systems. The deliverable first gives a brief introduction to smart manufacturing and then explains what is interoperability based on influential works in the field. It is followed by an explanation of the different approaches in achieving interoperability. It then continues by discussing the contribution of emerging technologies in achieving interoperability and cyber-safety and security in manufacturing. This deliverable ends with a discussion of the open challenges and final remarks.

Team involved in deliverable writing:

ESR 1 : Fan Mo, The University of Nottingham
ESR 2 : Agajan Torayeva, The University of Nottingham
ESR 4 : Ngoc Hien Nguyen, Mondragon Unibertsitatea
ESR 10 : Luis Estrada, UNINOVA
ESR 11 : Terrin Babu Pulikottil, UNINOVA
ESR 14 : Hamood Ur Rehman, TQC Ltd.

Supervisors : Prof. Jose Barata & Sanaz Nikghadam, UNINOVA

Chapter 1

Introduction

New Technologies has always been the driver of Manufacturing evolution from Steam Engines and electricity to computers and micro-processors. In recent years, manufacturing has experienced several changes as a result of the intensive development and research in sciences and technology and the provision of necessary equipment and systems to optimize industrial processes. The fourth industrial revolution or industry 4.0 precisely describes a new manufacturing paradigm engaging emerging technologies like machine learning, big data, internet of things, etc. [1] and offering several benefits like increased efficiency, fault tolerance, cognition and autonomy. In this regard, Cyber-Physical Production Systems (CPPS) emerge as one of the main enablers of Industry 4.0. Components of CPPS are smart and autonomous units connected in all levels in the production life cycle and provide fundamentally "intelligence, connectedness and responsiveness" [2]. They are composed of physical and digital elements which allow communication, computation and control [3]. Usually, a smart manufacturing environment, is composed of various CPPS which are continuously exchanging information and interacting. Currently, this is a focus of continuous research considering the high degree of heterogeneity in production systems [4] also known as manufacturing interoperability. In this work, we refer to interoperability as a set of methodologies, tools and strategies needed to achieve information exchange among all components in a smart manufacturing ecosystem. This also includes strategies and technologies utilized for the digitalization of machines, products, and the utilization of internet platforms for data storage and data analysis that can facilitate its integration. The development of interoperability among CPPS has been mostly tackled by industries with the idea of standardization. In fact, many authors consider that the creation of standardized interfaces and protocols may decrease the scepticism for the introduction of CPPS in industry [5, 2]. On the other hand, many researchers have implemented approaches using emerging technologies to show the benefits of principles of CPPS. Some examples are agent technologies, service-based frameworks and cloud platforms. These technologies, standards and protocols have shown very promising results but at the same time new challenges that need to be overcome to reach a seamless integration in manufacturing. In this context, this deliverable presents an integrative framework to explore common definitions, concepts, architectures, standards, technologies and a real case scenario about the implementation of interoperability approaches in smart manufacturing. The main objective of this study is to be a supportive conceptual text for researchers and practitioners in future implementations.

This deliverable conducts a state-of-the-art review of cutting-edge interoperability approaches in manufacturing and cyber safety and security requirements. First, an overview of the emerging concepts and paradigms in smart manufacturing is provided, along with their detailed characteristics (Chapter 2). Next, different definitions of interoperability are introduced, and the approaches and

perspectives in achieving the interoperability is discussed in detail. A brief insight to the emerging standards and protocols are also explained in this chapter (Chapter 3). Finally, the emerging technologies for achieving interoperability in smart manufacturing is explained in detail with main focus on the technologies like Multi Agent Systems (MAS), Service-Oriented Technologies (SOT), Cloud, Fog and Edge technologies (Chapter 4). This is followed by a discussion on cyber-safety and security in smart manufacturing (Chapter 5) and concludes with a summary of challenges and recommendations for future research and development (Chapter 6).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Chapter 2

Smart Manufacturing

National Institute of Standards and Technology (NIST) defines smart manufacturing as a system that is fully integrated and collaborative which is responsive to the changing demands and conditions of the factory in real-time [6]. To accomplish the defined goal, a smart manufacturing system utilizes recent advances in technology such as smart sensors, Cyber-Physical Systems (CPS), cloud and service-oriented computing, Artificial Intelligence (AI) — consequently, current advances and available methods in science and technology define the advance, as well as barriers in the development of the smart manufacturing.

Kusiak et. al [6] identifies the six pillars of manufacturing:

1. **Manufacturing technology and processes**: Additive manufacturing, new manufacturing tools to aid various operations, hybrid processes such as traditional and additive processes, integration of sensors and software capabilities will help the emergence of the manufacturing technologies and processes.

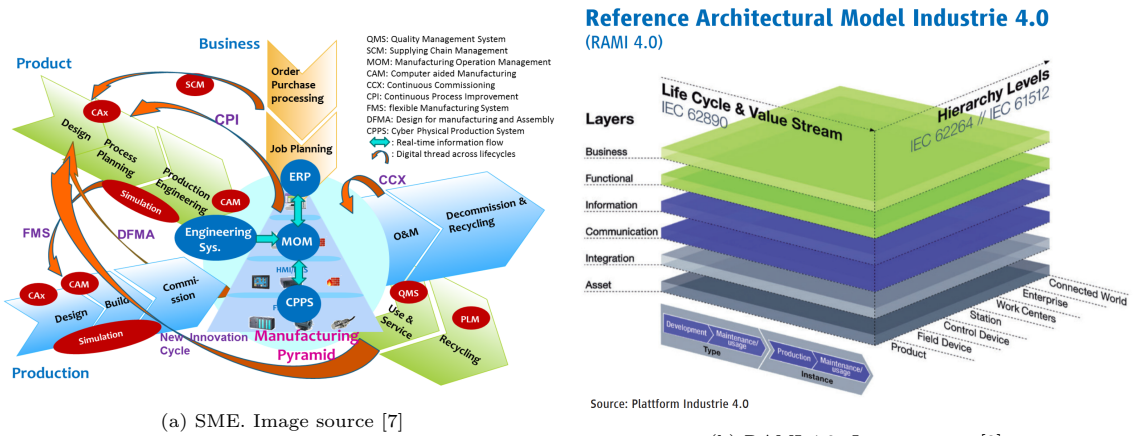
2. **Materials**: The emergence of smart materials and smart products will enhance the development of smart manufacturing systems.

3. **Data**: Nowadays, data plays a crucial role in modern life in digital technological advances, and hence the manufacturing will benefit more if the relevant data can be efficiently collected and managed by smart algorithms. Currently, there is a lot of software and hardware solutions waiting to be implemented in the manufacturing domain.

4. **Predictive Engineering**: Predictive engineering alongside with data engineering will facilitate the development of proactive solutions rather than reactive solutions. If the traditional way of utilising is to monitor and analyse using historical data, predictive engineering will enhance systems to prepare for future situations like disturbance and preventive maintenance.

5. **Sustainability**: If the goal of sustainability is achieved, which is about how the manufacturing process is performed, the borderline between manufacturing and service will be blurry.

6. **Resource sharing and networking**: Manufacturing domain will adapt the resource sharing methods and strategies which are currently popular among humans such as Uber and Airbnb. The adopted methods will benefit smart manufacturing concerning equipment, software and expertise sharing as well as collaboration.



(a) SME. Image source [7]

(b) RAMI 4.0. Image source [8]

Figure 2.1: Smart Manufacturing Architectures

Standard development organizations of countries such as USA, Germany, China and others have developed their roadmap and standardization solutions for smart manufacturing. To fully integrate the emerging ICT technologies into the manufacturing domain, and hence achieving smart manufacturing, there is a need for a reference architecture. Different industrial organizations and standard development organization have developed their architectures [7]. These architectures are used to describe top structures and internal relationships of manufacturing systems. Some of the smart manufacturing architectures are:

- Smart Manufacturing Ecosystem (SME) (Figure 2.1a) developed by NIST of the United States [7];
- Reference Architecture Model Industrie 4.0 (RAMI 4.0) (Figure 2.1b) architecture which consists of a three-dimensional coordinate system that describes all crucial aspects of Industrie 4.0 [8];
- Intelligent Manufacturing System Architecture (IMSA), developed by Ministry of Industry and Information technology of China (MIIT) and Standardization Administration of China (SAC).

Alcacer et al [9] defines the following as key technologies used in smart manufacturing:

The Industrial Internet of Things: Internet of things (IoT) provides a ubiquitous connection and encompasses everything connected to the internet. Industrial Internet of things (IIoT) connecting all the industrial assets, including machines and control systems, with the information systems and the business processes. IIoT increases productivity and efficiency through smart and remote management and provides opportunities to enhance efficiency, safety, and working conditions for workers. However, several challenges exist which prevent wide adoption of IIoT such as requirements in energy-efficient operation, real-time performance in dynamic environments, the need for coexistence and interoperability, and maintaining the security of the applications and privacy [10].

Cloud Computing: Cloud computing has emerged as a new computing paradigm that offers various solutions to provide a dynamic and flexible infrastructure. It can be considered a promising solution for the industrial automation systems of the future [11]. Even though Cloud computing allows higher utilization without increasing investment and degrading performance, there are still

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

many problems that limit the expansion of smart manufacturing such as overfull bandwidth, unavailability, latency, data validity, security and privacy, inefficient interaction [12].

Big Data: With the volume of growing data collected in a manufacturing domain, it becomes obvious that Big Data technologies will play a crucial role in the development of smart manufacturing systems. Volume, velocity, variety, veracity and value (5V of Big Data) are the five key characterizations of Big Data. The adoption of Big Data will empower data-driven strategies to become more competitive. Therefore, data is considered a key enabler for smart manufacturing by some authors [13].

Simulation: Simulation has been used by manufacturers to analyze their operations and provide decision supports for decades [14]. It helps to reduce development costs, decrease development cycles and increase product quality by allowing experiments for the validation of products, processes or systems design and configuration [15]. Simulation is especially important in integrations of Machine Learning methods such as Reinforcement Learning where the exploration of the agent in a real physical environment may not be desirable due to safety constraints.

Augmented Reality: Augmented Reality is an integral part of smart manufacturing since it enables workers to access digital information and overlay that information with the physical world [16]. Applications developed with AR-technology can enhance human operators in maintenance, diagnostics, human-machine interaction and decision support systems.

Additive Manufacturing: Additive Manufacturing (AM) is the industrial production name for 3D printing. It aids greater customization of products without extra tooling or manufacturing cost and suitable when there is a need for on-demand manufacturing and excellent scalability. Some challenges for AM lies in the development of a self-contained, robust, user-friendly, safe, integrated system to provide required deposition scan motion, and speed, the high feature-volume resolution with concomitant energy for part fabrication and dimensional control [17].

Horizontal and Vertical Systems Integration: Horizontal integration is integration between companies, which is essential for collaboration between different companies and achieving the interoperability. Vertical integration is integration within a company which is essential for achieving collaboration among the different level of the enterprise's hierarchy [9].

Autonomous Robots: Autonomous robots can achieve goals and perform tasks without human intervention. As the autonomy level of the system increases the role of human shifts from low-level and so-called 4D (dangerous, dirty, difficult, and dull) tasks to high-level and safe tasks [18, 19]. While machines are good at tasks requiring fast computations, reacting quickly to known situations and finding patterns in massive amounts of data, humans are good at resolving new and ambiguous situations. Autonomous systems will require human support to guarantee correct, complete and safe behaviour in all situations. Therefore, humans, machines and software must interact and collaborate to achieve the desired key performance indicators derived from manufacturing objects associated with constraints [20, 21].

Cybersecurity: As technology progresses and many devices are connected and sharing information through the network, there arises a problem of securing the communication and proprietary data. Hence, cybersecurity stands as one of the most important aspects of achieving smart manufacturing. Therefore, careful implementation of connection and synchronisation protocols are important to manage the manufacturing infrastructure. The more devices are connected to the network, the more risk of cyber-attacks. The valuable information must be carefully protected to keep the competency level [22].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Chapter 3

Interoperability in smart manufacturing

3.1 Definitions of Interoperability

CPPS are a set of computational systems with high interconnection with physical resources and a high computation capacity. In the context of smart manufacturing, CPPS emerge as autonomous elements that abstract machines', computational units' and people's behaviour as digital entities. The communication and interconnection of these units is considered a challenging process because of the high degree of heterogeneity of technological resources, different abstraction levels and the inclusion of legacy systems. This process refers to the capacity of interoperability of systems and it has been mostly addressed in information and communication technologies.

The IEEE standard computer dictionary defines interoperability as "the ability of two or more systems or components to exchange information and to use the information that has been exchanged" [23], which emphasizes the capacity of systems to understand each other despite their different technological levels. This definition may look general or ambiguous; for this reason, different categories, approaches and perspectives of interoperability have been described in previous years i.e. semantic, syntactic and technical interoperability [24], they will be examined in more detail in the next section.

Overall, different definitions of interoperability in the context of smart manufacturing have been proposed, some of them are presented below:

- Rojas et al [25] describe interoperability as a process to ensure continuous information accessibility and availability, and the capacity of a system to use information from other systems. Interoperability is referred as a problem of data representation, networking and platform information exchange. They also argue that the issue of integration is an issue of interoperability. To integrate higher levels in a company with the shop floor (vertical integration) or different companies (horizontal integration) optimal interoperability strategies are needed.

- Zeid et al [26] argues that interoperability in manufacturing refers to the process of machines and control systems interaction, not just in normal operations but also in case of failures or alarms. Interoperability requires a high availability and collaboration from services inside and outside the shop floor and the utilization of cloud base technologies, for this purpose a well common understanding and data representation is required.

- Noura et al [27] refers to interoperability as a property needed to transfer data from heterogeneous platforms and devices so that little or none human involvement is needed. Also, they suggest that interoperable systems may include different levels.
- Napoleone et al [28] points out that a high degree of interoperability equals to a high degree of standardization. A common understanding and a well-structured knowledge representation as well as a proper integration of legacy systems is essential to implement CPPS and to ensure a greater and easier integration of manufacturing components.
- Van Der Veer et al [24] explains interoperability as "the ability of equipment from different manufacturers (or different systems) to communicate together on the same infrastructure (same system), or on another while roaming".

Indeed, the challenge of interoperability is born with the need of a seamless and high integration and cooperation of all levels in a factory: people, machines, business, organizational aspects, etc. and in these in turn with the whole value chain i.e. logistics, sales marketing, services. Previous definitions suggest that the challenge of interoperability in smart manufacturing is not a single issue and several aspects should be taken into account. For example, compatibility of data types, needed abstraction levels, proper technological enablers, etc. Additionally, in smart manufacturing, interoperability should be address in a robust manner. Aspects like real time communication and high availability of services and resources are imperative to achieve the high expectations of industry 4.0 optimizing processes and making them autonomous with little or non-human intervention. The common understanding, standardization and continuous evolution of technologies are paving the way to fulfil these current expectations and even though there are many challenges that need to be overcome in this aspect; there is currently a strong baseline of concepts, research and applications.

The following sections of this document are dedicated to address common approaches, emerging technologies and applications with regard to interoperability in smart manufacturing.

3.2 Approaches and perspectives in achieving Interoperability

3.2.1 Device interoperability

The term device is mainly used in the Internet of things to refer to "smart objects" with capabilities of integration and communication [27]. In smart manufacturing, devices that include high computation capabilities are also called CPS [26]. In this context, devices are highly heterogeneous and can be exemplified as sensors, actuators, parts to be assembled, and several low-level control hardware. The literature classifies the different types of devices in low level and high level according to the embedded computational power and communication capabilities they show. For example, high level devices can be considered PLCs or high computational boards (e.g. Raspberry); on the other hand, low level devices may include single sensors, actuators, RFID tags or barcodes. Those need additional computational capabilities or hardware to be integrated. Additionally, for a seamless communication these devices (low level and high level) need to manage necessary standards and protocols. Thus, we can refer to device interoperability as the way how these heterogeneous devices are integrated into a smart manufacturing ecosystem, including standards, protocols and different technologies. Throughout this document, we will analyse many of these technologies and protocols. Nevertheless, in this section we will discuss some use cases in which we can differentiate some type of devices and standards used [27, 26].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Device interoperability applications

The literature in device interoperability is by far extensive. Even though the term has been not quite popularized in manufacturing approaches like it is in the IoT, the applications of high end and low end devices are growing. In [29], the utilization of a Raspberry pi allows the integration of agent technology, which in turn allows the communication among all entities in the shop floor and an adaptable behaviour. This development board is later interfaced with a PLC which acts as main controller of the process. Additionally, this work shows the utilization of RFID technology as a method to integrate and identify products in different production stages. In [30], with the purpose of demonstrating self-organization in a modularized conveyor system, agents are implemented through the utilization of a raspberry which also receives signals from different sensors and communicates with other boards via WIFI technology. In [31], a CPPS system has been developed based on the virtualization of several stations via two platforms: Arduino and Raspberry pi. Those are in charge of receiving and handling input/output signals from the connected stations and of interfacing them in the network using MODBUS TCP and OPC-UA technologies.

Previous evidence suggests that interoperability at the device level is normally challenged using state of the art standards and protocols (to be presented in following sections). Additionally, the scarcity of support of some emerging technologies confirm the need of using high level devices. Overall, high-level and low-level devices allow the integration of any component (simple or complex) into the manufacturing ecosystem.

3.2.2 Syntactic interoperability

Even though in recent year we have seen the emergence of different categories or perspectives of interoperability like technical, organizational, device, networking, platform interoperability etc [24, 27], the IEEE Guide to Enterprise IT Body of Knowledge (EITBOK) has categorized the interoperability approaches mainly into two types: Syntactic and Semantic interoperability [32]. These two types are also present in other literatures while categorizing (taxonomy) or explaining about different perspectives of interoperability. In general terms, if two or more systems are capable of communicating and exchanging data, then they exhibit syntactic interoperability. The European Telecommunications Standards Institute (ETSI) defines syntactic interoperability as follows : “Syntactical Interoperability is usually associated with data formats. Certainly, the messages transferred by communication protocols need to have a well-defined syntax and encoding, even if it is only in the form of bit-tables. However, many protocols carry data or content, and this can be represented using high-level transfer syntaxes such as Hypertext Markup Language (HTML), Extensible Markup Language (XML) or Abstract Syntax Notation One (ASN.1)” [24].

Technical Interoperability is usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place and is generally represented as a layer inside the syntactical Interoperability (Figure 3.1). This kind of interoperability is often centered on (communication) protocols and the infrastructure needed for those protocols to operate[24].

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

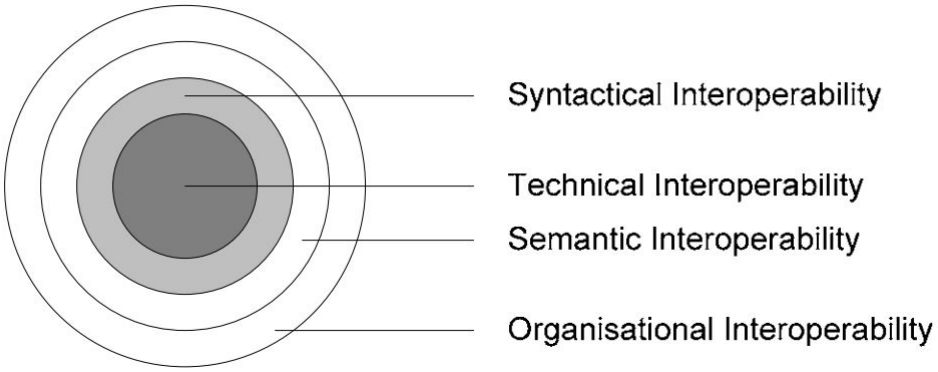


Figure 3.1: levels of interoperability (Reprint from Reference [24])

While exchanging information or service from one system to another, the content of the message needs to be serialized. The sender encodes the data in the message and the receiver decodes the received message. The sender and receiver use syntactic rules specified in some grammar to encode or decode the messages. Syntactic interoperability problems arise when the sender's encoding rules are incompatible with the receiver's decoding rules, which leads to mismatching message parse trees [27].

A major limitation of this type of interoperability is that it merely considers the format of the data and simply gets the information from one place to another intact. It does not take into account the meaning of the transferred data nor applies logic to the fact being transferred and used [26].

Syntactic interoperability is achieved through the use of standard sets of data formats, file formats and communication protocols. In data formats, high level transfer syntaxes are among the tools of syntactic interoperability. This includes standards like HTML, XML, Structured Query Language (SQL),ASN.1,Concrete Syntax Notation One (CSN.1) or JavaScript Object Notation (JSON). This is also true for lower-level data formats, such as ensuring alphabetical characters are stored in a same variation of ASCII or a Unicode format (for English or international text) in all the communicating systems.

XML is considered as the basis for a rapidly growing number of software development activities and is widely known in the internet community for markup in documents of arbitrary structure [33]. XML is a free open standard markup language maintained by the W3C organization. It is an evolutionary product of Generalized Markup Language (GML) and Standard Generalized Markup Language (SGML) and is designed for markup in documents of arbitrary structure, as opposed to HTML, which was designed for hyper-text documents with fixed structures. A well-formed XML document creates a balanced tree of nested sets of open and close tags, each of which can include several attribute-value pairs. There is no fixed tag vocabulary or set of allowable combinations, so these can be defined for each application [34]. XML is used to serve several purposes including Serialization syntax for other markup languages, Semantic markup of Web pages, Uniform data-exchange format etc. An XML serialization can also be transferred as a data object between two applications.

3.2.3 Semantic interoperability

Interoperability, based on agreements between requesters and providers, is an ability to exchange services and data among systems; semantic interoperability ensures that these exchanges make sense,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

that the requester and the provider have a a common understanding of the "meanings" of the requested services and data [35]. The quality and flexibility of the information models affect the level of interoperability in distributed manufacturing systems [36]. Interoperability in manufacturing systems is a key concept to face the challenges of new environments, especially in the manufacturing domain and semantic integration is an important approach that helps to deal with heterogeneity within large and dynamic enterprises [37]. Ontologies for various application domains or industries, are key to avoiding semantic problems. Therefore, numerous amounts of work are done using ontologies for the manufacturing domain.

Context modelling facilitates interoperability of manufacturing systems. To this end, [38] compares different context modelling and reasoning techniques by describing the following requirements for the context models and context management systems:

- **Heterogeneity and mobility**: a context model should be able to express different types of information, and context management system should provide management of the information depending on its type.
- **Relationship and dependencies**: various relationships between different types of context information have to be captured to ensure the correct behaviour of applications.
- **Timeliness (context histories)**: a feature of context information that allows context-aware applications to access the past and future states. It should be captured by context models and managed by context management systems.
- **Imperfection**: ability to model context information quality (incorrect, incomplete, conflicting context information) to support reasoning about context.
- **Reasoning**: ability to support consistency verification and context reasoning techniques to derive new context facts from existing facts and/or reason about high-level abstractions of real-world situations. Reasoning techniques should be computationally efficient.
- **Usability of modelling formalisms**: the ease of translating real-world concepts to the modelling constructs, the ease of usage, and context manipulation by context-aware applications.
- **Efficient context provisioning**: efficient access to the context information in the presence of large models and numerous data objects.

Concerning the requirements outlined above, authors discuss and compare the following modelling techniques:

- **Object-role based models**: with focus on Context Modelling Language (CML).
- **Spatial models**: fact based models that organise context information by physical location.
- **Ontology-based models**: context is considered as a specific kind of knowledge.

It was discussed that ontological models of context provide clear advantages both in terms of heterogeneity and interoperability can be obtained only by adopting expressive languages—consequently, a substantial number of authors employed ontologies in their works to achieve interoperability in the industrial domain.

[39] proposes ontology-based context modelling to represent concepts and relations in the industrial domain. Authors discuss two different approaches of context handling in smart environments:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

data-driven and the knowledge-driven approaches. Data-driven approaches can better handle uncertain knowledge, but they require large datasets to train models. Knowledge-driven approaches such as ontology-based approaches can handle heterogeneous and imprecise data but require expert knowledge to build models.

[40] presents a survey of the ontologies for Industry 4.0, including different domains such as aerospace, construction, steel production, etc. and manufacturing processes such as packaging, process engineering, resource configuration, etc. The primary purpose of this work is to give a broad overview of the current state of the art ontologies for industry 4.0 and the standardization efforts. Although there are a variety of ontologies, there is a need for standardization of ontologies. Authors discuss different ontologies such as Core Ontology for Robotics and Automation (CORA), Ontology for Autonomous Robotics (ROA), Ontology for Robotic Architecture (ORArch), Ontology for Industry 4.0 (O4I4) and their benefits in the representation of vocabulary to describe the key concepts in Industry 4.0.

In [41], the authors propose an ontology-based approach to model context-sensitive manufacturing information from heterogeneous data sources. This manufacturing knowledge is used to make a real-time decision in Flexible Manufacturing Systems. The proposed approach is modular and can be further extended to develop context-aware services in other manufacturing domains. For modelling the context, authors used RDF/OWL-based ontology modelling since the ontology-based approach provides flexible representation to support modelling of context in a structured way. The context management system is used to process the raw monitored data. The context management system consists of context identification, context reasoning, and context provisioning. Inferred high-level context is used to support for optimization.

[42] proposes a context-aware architecture to deliver information between the factories' systems such as ERP/MES and the people working in the shop-floor. Context-awareness is regarded as the system's ability to provide relevant information to the human user to avoid potential errors proactively by delivering expert knowledge. The proposed context-aware architecture consists of the layered approach in which context detection and context processing are separated. The crucial part of this architecture is context modelling. The authors used the ontology-based approach to model the manufacturing context due to its superiority in expressing relations and dependencies in context data, interoperability, and heterogeneity.

Interoperability in the manufacturing domain is challenged with different terms that people working within a particular company or group develop their vocabulary or common terms for particular issues, elements or activities with which they often work. Ontologies provide a solution for this problem, common understanding of manufacturing-related terms, and therefore enhance the semantic interoperability [43].

Current limitations of semantic interoperability, therefore, inevitably affect manufacturing knowledge sharing capability. Authors of this work [44] discuss the possible configuration of frameworks, and understanding of the potentials that ontology-driven frameworks possess, to capture semantically enriched manufacturing knowledge for manufacturing interoperability.

3.2.4 Factory interoperability

Recent advances in information and communication technologies have allowed manufacturing enterprise to move from highly data-driven environments to a more cooperative information/ knowledge-driven environment. Enterprise knowledge sharing (know-how), common best practices use, and open source/web based applications are enabling to achieve the concept of integrated enterprise and hence the implementation and interoperability of networked enterprises. Enterprise integration and interoperability in manufacturing systems is a key concept to face the challenges of these new

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

environments. Supply chains are the dominant organizational structure in manufacturing today. That structure can be viewed as a global network of suppliers, manufacturers, transporters, retailers, and customers who must share technical and business information seamlessly. This information, previously shared in a variety of ways including paper and telephone conversations, must now be passed electronically and correctly among all the partners in the supply chain. Disparate corporate and national cultures, a plethora of international and regional standards, and numerous commercial products make this task of sharing information all the more difficult. These facts further underscore the need for a clear and unambiguous, standards based, interoperability infrastructure.The term manufacturing interoperability refers to the capability of manufacturing enterprises to exchange information that maybe technical or enterprise related in a coherent manner within and between each other.

A recent study conducted on the U.S. automotive industry reports an annual economic loss of $1 billion due to the lack of interoperability throughout the supply network,which reveals the significant impact of interoperability on the manufacturing sector in terms of both cost and performance quality. There are three principal approaches used to reduce these exorbitant costs.

- **Machine-to-machine solution:** A point-to-point customized solution is developed for each pair of partners. The idea behind this approach is making each individual machine interoperable with every other machine it is linked to or integrated with. The challenge is that each of these machines may communicate based on their own manufacturer-specified communication protocol. Achieving interoperability under this scenario requires a thorough understanding of their unique semantics along with translation of their syntax. This approach is clearly not effective and would be very expensive in the long run because each pair of software systems needs a dedicated solution. When there are, for example, ten partners in the chain, this would require up to 90(10*9) interfaces. Moreover, should any system provider release a software upgrade, many of the translators would likely need modification.

- **Industry-wide standardization solution:** In the second approach each original equipment manufacturer (OEM) mandates that all partners conform to a particular, usually proprietary solution. The idea here is to ensure that all the manufacturing industry service partners follow a single solution. For example, a manufacturing unit may be integrated and interoperable until the period of production. However, if further processes have to be performed on the product in later stages, it may have to move to another plant to complete those operations. In this case, not only is a common protocol required for operations within the manufacturing setup, there is also a need for another protocol between different manufacturing units. This approach can be extended to various industries.The drawback of this approach, however, is that the manufacturing units used to process a given product may belong to different enterprises with different integration/communication protocols. For example, this approach has been the practice in the automotive sector. While this is a cost-effective solution for the OEM, it causes nightmares for the partners because they are forced to purchase and maintain multiple, redundant systems if they want to do business with several major OEMs. The current trend of global outsourcing has made this approach practically impossible to implement.

- **Open Standards or Platforms:** In the third approach neutral, open, published standards form the foundation of the infrastructure. This is considered as the most effective approach to achieve interoperability. By adopting open standards, the combinatorial problems associated with the first approach go away as it is now of order N rather than order N2. The nightmares associated with the second approach because partners can buy any software they want, provided the vendors implement the standards. Furthermore, standards also offer stability in

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

the representation of information, an essential property for long-term data retention. Increasingly, this retention issue is recognized as a costly and critical problem for industries with long product life cycles, such as aerospace.

A number of reference models and architectures have been developed in recent years to address the issues of integration and interoperability in the context of smart manufacturing and can be categorized into physical, functional and allocated architectures [45]. One of the most widely discussed architecture model have been proposed by Platform Industrie 4.0 named Reference Architecture Model for Industry 4.0 (RAMI 4.0). RAMI 4.0, as discussed in the previous chapter is an architecture that was designed primarily for applications in the manufacturing industry. The RAMI 4.0 model was built after studying existing approaches and incorporating them into the interoperability stack. Approaches [46] used includes

- OPC-UA (for communication and networking)
- Basis IEC 62541 (for the Communication layer)
- IEC Common Data Dictionary (for the Information layer)
- Field Device Integration technology (for the Functional and Information Layer)
- AutomationML and ProSTEP (for design and end to end engineering)
- IEC 62890 functions (for life cycle improvement and value stream mapping)

Another important reference model designed for all industries related to the Industrial Internet of Things was proposed by Industrial Internet Consortium (IIC) [47]. This reference model named Industrial Internet Reference Architecture (IIRA) was not specifically designed for manufacturing applications but the functional layers of RAMI 4.0 and the domains of IIRA are related and have the same high-level tasks distribution (Figure 3.2). Both also applies OPC-UA to model its communications and network. This linkage with RAMI 4.0 establishes a foundation for its application in the manufacturing domain. Other similar reference architecture introduced which are important in achieving factory interoperability include IBM Industry 4.0 Reference Architecture [48] and NIST service-oriented architecture [49].

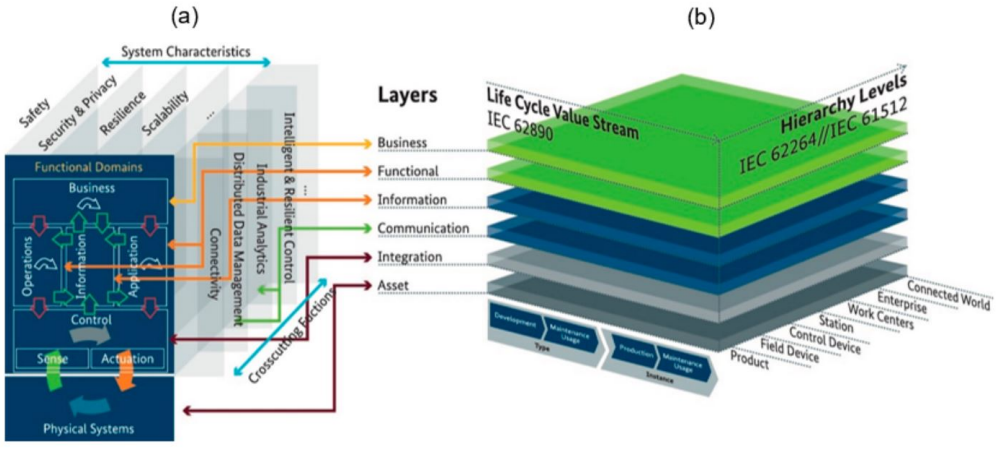


Figure 3.2: Relation between functional layers of RAMI 4.0 and the domains of IIRA (Reprint from Reference [26])

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

3.2.5 Cloud manufacturing interoperability

Cloud computing is changing the way industries and enterprises do their businesses with resources and services provided over the internet. Cloud computing is emerging as one of the major enablers for the manufacturing industry. Two types of cloud computing adoptions in the manufacturing sector have been suggested, manufacturing with direct adoption of cloud computing technologies and cloud manufacturing—the manufacturing version of cloud computing. The Notion of cloud computing could be extended to cloud manufacturing where distributed resources are encapsulated into cloud services and managed in a centralized way. In the context of cloud manufacturing there is a need to introduced additional types of interoperability like Transport interoperability, Behavioural interoperability and Policy interoperability. A generic cloud manufacturing architecture consists of five layers namely Application layer, application interface layer, core service layer, virtualization layer, and physical resource layer. For example, in explaining interoperability in the domain of cloud manufacturing a service oriented system called Interoperable Cloud-based Manufacturing System (ICMS) was proposed by Xi Vincent Wang et al [50]. ICMS provides a Cloud-based environment integrating existing and future manufacturing resources by packaging them using the Virtual Function Block mechanism and standardized description. The proposed system consist of 4 layers namely, manufacturing resource layer, virtual service layer, global service layer and application layer (Figure 3.3) similar to the generic cloud manufacturing architecture.

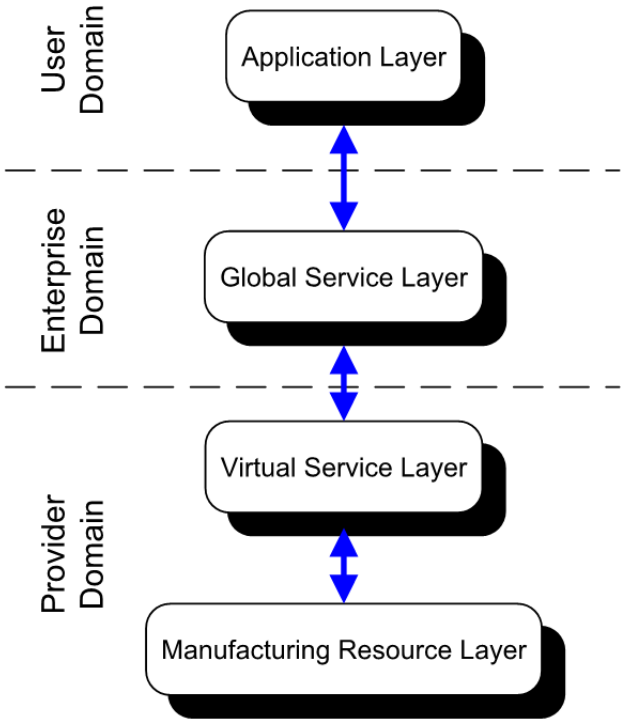


Figure 3.3: Layered architecture of a Cloud Manufacturing system. (Reprint from Reference [50])

A detailed explanation of cloud based services, platforms, the different layers of cloud manufacturing and examples of interoperability in the domain of cloud manufacturing is explained in later chapter.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

3.2.6 Emerging standards and protocols

IEEE or 3GPP communication standards specify the physical layer and the medium access control sub-layer for user data traffic. If no higher layers of the Internet such as IP, TCP or HTTP should or can be used for industrial communication systems, corresponding standards for services, protocols and profiles are available in the IEC 61158-1 and IEC 61784-2 standards series. Industrial radio communication systems are standardized in IEC 62591:2016 (WirelessHART), IEC 62601 (WIA-PA), IEC 62734 (ISA100a) and IEC 62948 (WIA-FA). In addition, the series of standards on coexistence management for radio communication solutions IEC 62657-2 is to be mentioned. The requirements for communication in Industrie 4.0 will be very diverse. Consequently, very different wired and wireless communication systems will be used. With OPC UA, an interface standard has been established that bridges the heterogeneity of industrial communication systems on both the communication and the information level. This interface standard supplements the existing communication solutions. It is based on concepts such as a Service-Oriented Architecture (SOA) and information models (OPC-UA Companion Specification) to describe devices and their capabilities. An SOA makes it possible for components, machinery and plants to act more flexibly if they are not configured and programmed to carry out a specific production task, and are able to offer their basic capabilities in the form of services. These include the ability not only to transport data from devices (measurement values, settings and parameter values), but also to describe them semantically in machine-readable form[51].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Chapter 4

Emerging technologies for interoperability in smart manufacturing

4.1 Multi agent systems

Multi-Agent Systems MAS have been extensively applied in distributed artificial intelligence and software engineering to implement software units (agents) with cognitive capabilities. Michael Wooldridge [52] defines agent as "a computer system that is situated in some environment capable of autonomous action in this environment in order to meet its design objectives". Furthermore, agents have cognitive capabilities i.e. they can acquire external information, reason and perform defined preprogramed tasks.

MAS as part of a society, do not have global contextual knowledge of the operation environment; instead, they present a partial local understanding and the global reasoning is the result of the social ability, communicating necessities and objectives among all the entities in the group. Some attributes associated with the concept of MAS proposed by [53] are: autonomy, social ability, reactivity, proactivity, continuous operation, adaptability.

There is no clear consensus of the main attributes of MAS. In fact, no every scenario which implements agent technology shows the same properties. This depends on the type of application and sometimes some features are more desirable than others [52] For example, the proactivity of an agent depends on how well its designer implements the rules that describe the environment where it is located. This is not an easy task because most real scenarios do not have a structured and static configuration. Therefore, if a specific agent was programmed with proactive rules under uncertain conditions this may result in undesirable behaviors.

Agent communication

The Foundation for Intelligent Physical Agents (FIPA)[1] is a IEEE Computer Society that promotes agent-based technology and its communication. This organization was founded in 1996 and has produced several agent standards traduced in an Agent Communication Language (ACL). A set of

[1] http://www.fipa.org/

22 performatives describe formal semantics for information exchange. Certainly, FIPA-ACL is not the only agent communication language. Another relevant and well-known communication protocol is Knowledge Query Communication Language (KQML). KQML presents a standard format for the description of their messages as objects in an object oriented way where the arguments needed for the communication are instantiated as attributes [52]. Both protocols make use of ontologies which support the understanding of the terminology and semantics used by the agents.

The JADE framework

Java Agent Development Framework (JADE)[2] is a widely used framework for developing multi-agent based applications. It supports the development of agents under the FIPA-ACL protocol. JADE is implemented in the JAVA language which facilitates the implementation of agents as classes. Furthermore, JADE can distribute agents in various computers over the networks and in mobile devices. JADE also offers the deployment and testing of the agent communication using a graphical user interface. These properties have made that JADE be used in countless industrial applications and uses cases.

Multi-agent systems in manufacturing

Traditional centralized industrial control approaches are not prepared for dealing with novel business paradigms i.e. mass customization or total personalization of products. Furthermore, the development of Information and communications technology (ICT) technologies and the globalized economy have brought the necessity of industries of having lower production costs, higher flexibility, higher quality of production and the necessity for a rapid response in case of dynamic events, disruptions or achieving process optimization. For this purpose, the future of manufacturing systems should be highly automated, flexible, modular, interoperable, and easily changeable[54] .

MAS appear as a powerful technological enabler for achieving not just modularity and autonomy but also interoperability among the resources in the workshop, accomplishing a decentralized control [55]. This general conception takes the definition of resource virtualization, which means the encapsulation of the digital behavior, properties and functionalities of physical resources as intelligent entities, in this case agents. These smart units can interact, have social abilities and communicate their necessities just like ants do in nature.

In manufacturing this is translated to machines that can communicate with mobile elements, resources, products, humans, etc. Additionally, agents can inform their current state and can also show intelligent behavior, see (Figure 4.1).

[2]https://jade.tilab.com/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

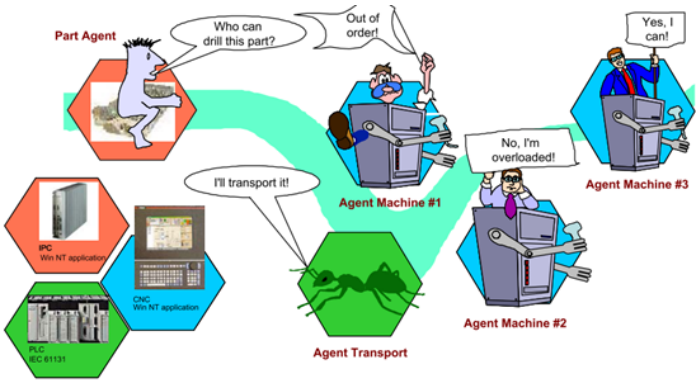


Figure 4.1: Multi-agent systems in manufacturing (Reprint from Reference [56])

The application of MAS in manufacturing is not new. In fact, various industrial projects were already implemented in the 90's in different contexts e.g. smart production, smart grids and logistics [57] where agents showed very good results in several distributed approaches. For these reasons, agents are considered by many authors as very powerful enablers of integration and interoperability for smart CPS [57].

Multi-agent systems for achieving interoperability and integration in Cyber-physical systems

The general conception of CPS requires the confluence of physical devices (in the case of manufacturing machines, resources and people) with communication and computation aspects, which as stated before can be achieved using agent technology. Agent based-CPS also provide several characteristics that improve the agility and flexibility in smart manufacturing, some of these are summarized below [58] [59] [60].

- The vertical and horizontal integration is possible through the resource agentification and its communication over the network.
- The resulting integration can be also improved by the intelligence capacity of agents optimizing energy, time and resource utilization
- Human resources can be also represented by software agents which makes feasible its integration in the manufacturing process.
- The integration of CPS becomes very robust since it can handle unexpected situations and even find autonomous solutions.

Agents and different standards for achieving interoperable CPS

The CPS-standardization is a key aspect for the design and development of industrial CPS. However, there are currently not many standards available for its implementation and it is a topic of continues research. Present works rely to a large extend in reusing and combining IT technologies like web services and service oriented design. Besides, many standards from low level control automation like

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

IEC-61131 or IEC-61499 are also being introduced as a way to overcome the lack of agent technology in industrial controllers [57].

As stated in previous sections, FIPA-ACL has introduced an agent communication language that provides performatives and the necessary semantics for an agent understanding (generally by means of ontologies) and communication. Furthermore, FIPA-ACL is mostly implemented using the JADE framework.

Agents and web services can be integrated to provide the best of both worlds, considering the autonomy of agent technology and the interoperability provided by service oriented architectures. Generally, the components at the lowest level e.g. controllers or PLCs (device layer) provide their functionalities as services using the Device Profile for Web Services (DPWS) protocol (Device Profile for Web Services) [61]. This creates a kind of virtual resource which highest control and interoperability can be implemented using a multi-agent approach (execution layer).

The integration of low level controllers with MAS normally relies on legacy PLC programming standards like IEC-61131 and IEC-61149. These standards are based on a control logic and in service based function block respectively. In higher levels this control logic is managed by a multi agent based logic [60].

This execution is normally designed in a higher level which can adapt its behavior to different scenarios (logic layer). To complete the orchestration, this process is normally governed by business or higher functions that manage the whole enterprise integration [61]. This representation is shown in (Figure 4.2).

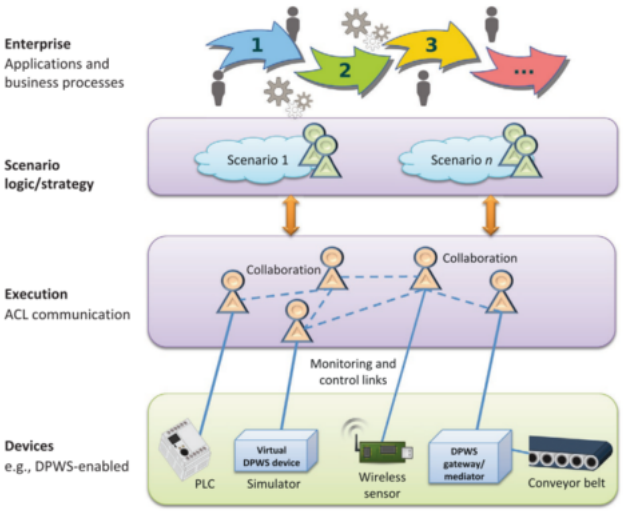


Figure 4.2: A CPS infrastructure relying on MAS and web services (Reprint from Reference [61])

Patterns for agent integration and interoperability in cyber physical production systems

The application of agent technologies in smart manufacturing is wide in terms of the type of functionalities or level of integration. For example, in [62] manufacturing resources and their functionalities are abstracted by single mechatronic agents and those in turn can be abstracted by different coalitions according to the needed collaboration and skills. In [63], in addition to the resource virtualization of machines, the abstraction includes management functionalities and customer operations allowing a broader integration i.e. in cloud platforms. This also involves the interoperability of various entities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

in the value chain. This evidence suggests that MAS have been implemented using different patterns depending on the type of applications. A complete discussion and classification of these patterns is made in [59] and it is summarized below.

- Resource access: this type of agents generally includes the abstraction of field devices or machine virtualization, resources and their operational control. Besides, they are also referred as the ones who promote the modularization and integration with higher layers.
- Communication agent: This pattern includes agents that manage and unify the communication of resources through upper layers considering the conversion from heterogeneous protocols. For example, resource agents normally are integrated using OPC-UA, FIPA, by broker agents, ontologies, etc.
- Process agent: This type of pattern usually orchestrates and manages resource agents (locally). They normally do not interact with field devices but with their agent abstraction. They are in charge of the coordination, diagnosis and supervision of processes and of their proper execution.
- Agent management system: The agent management system usually has a global supervisory role. Unlike, the process agent which refers to local supervision, this pattern can have a broader vision of the process control aiming to optimize and organize processes.

Additionally, this agent pattern classification makes a good fit with the rami 4.0 [59].

The asset layer represents physical resources: machines, conveyors or robots. The integration layer is conceived as the abstraction of field devices by the resource agents. In other words, the integration layer includes the virtualization of resources (its translation to the cyber world). The communication layer integrates the different communication protocols and standards; therefore, it can be referred as an instance of communication agents which are used to abstract the level and type of communication. The information layer refers to the creation of models or instructions to manufacture products (manufacturing assembly instructions). This can be easily coupled with the objective of process agents (sometimes also called product agents). Finally, the functional layer includes services and functions to manage resources in the asset. The Agent management system by a direct or indirect communication with agents in lower levels fits this level of abstraction.

Applications of agent technologies

Several small and large scale EU research projects have reported important results in the context of agent technology in smart manufacturing. The results of these projects paved the way towards the evolution of smart and autonomous industrial systems. In this context, the next subsection summarizes state of the art projects that combine specially agent and different technological enablers to achieve innovate solutions as a mean to overcome challenges of the manufacturing technology. In particular, this summary will be focus on the use of agent technology to achieve interoperability and integration.

- The FP7-IDEAS Project [62] was conceived with the notion of integrating manufacturing components as multi-agent based resources. It is based on the evolvable production system paradigm considering the ability of resources to adapt to changing or dynamic environments. The mechatronic architecture uses four types of agents namely: machine resource, coalition leader, transport system and human machine interface agents. The resource integration allows the self-organization of the system according to a set of available skills and a recipe product assignment.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

- PRIME Project : The FP7- PRIME Project [3] (Plug and Produce Intelligent Multi Agent Environment based on Standard Technology 2012 – 2015) is based on a multi-agent architecture and like The FP7-IDEAS is founded on the Evolvable Production System paradigm. FP7-PRIME considers the following types of agents HMI, monitoring, production management and production components. The HMI agent allows the integration of the operator for monitoring and controlling activities. The monitoring agents provides the needed information of the resources to perform data analysis and giving a feedback to the operator. The production management and production component allows the agent communication for the reconfiguration of the available skills and resources.

- The H2020 openMOS [4] (Open dynamic Manufacturing Operating System for Smart Plug-and-Produce Automation Components 2015 – 2019) presents an architecture that allows the integration and adaptability of manufacturing products according to dynamic requirements. It is mainly based on a manufacturing service bus which orchestrates and control the process and its resources. The system presents a high level process optimization which is based on the abstraction of their resources and products as agents. In this case the agent technology eases the data analysis and communication of the architecture.

- The H2020 GO0MAN [5] (aGent Oriented Zero Defect Multi-stage mANufacturing 2016 – 2019) presents an architecture that supports the distributed diagnosis of manufacturing products based on a multi agent system. In this context, agents collect data from resources and allow an intelligent data analytics based on KPIs, rules and knowledge storage. Various types of agents abstract products and resources and these in turn are managed by high level entities that take into account a global perspective of the components to monitor, diagnose and predict.

- The myJoghurt project [63] implements an agent-based CPPS architecture for yogurt orders customization and production. Customers can choose different parameters to order and personalize the product. This is translated in the automatic organization of the production plants according to the availability of machines and to specific schedules. In this work agents allow the integration of production plants distributed in several places from Germany. All the communication channels are distributed through the cloud supported by customer agents that abstract parameters from the customer and coordination agents that have predefined knowledge of the process.

Barriers in the implementation of agent based technology to achieve interoperability in smart manufacturing

The application of agent based technologies has brought opportunities to face with many of the current industrial interoperability requirements of smart manufacturing. The underlying objective of developing autonomous systems relies in the characteristics of agents i.e. communication, social ability, autonomy, etc. This has been enhanced with the combination of several technological enablers and industrial standards e.g. cloud computing, web services, etc. to achieve a wider integration of the shop-floor resources with all the elements in the value chain. Agents allow the abstraction of resources in different granularity levels, which can in turn be orchestrated or managed with higher level agents to perform global optimization processes, control, monitoring, diagnosis, etc. Additionally, the higher abstraction level of agents (in business layers for example) can be utilized to take

[3] https://cordis.europa.eu/project/id/314762/reporting
[4] https://cordis.europa.eu/project/id/680735/es
[5] http://go0dman-project.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

autonomous decisions considering internal and external factors. This whole evidence suggests that multi-agent based technologies have paved the way towards performing not just high interoperability and integration but the necessary autonomous behavior required in industry 4.0. It is important to consider many of the barriers exemplified in the literature towards the implementation of a seamless interoperability using this technology and their supporting enablers. For example, the lack of low level control devices that support the Jade framework, has caused that most agent implementations depend on CPUs processing, causing a lack of real time communication and real time response which is not acceptable in real implementations. A few approaches show the opportunities of using low level devices like Raspberry pi platforms or similar ones. However, these devices are not prepared for industrial environments and have therefore lack of reliability. Leitao et al [57] consider that more efficient tools should be developed to manage multi agent approaches. Since a high interoperability is expected in future manufacturing environments, these tools should also enable high security and safety. This is very important considering current security polices and very high risks in industrial scenarios. Future protocols and standards should allow the integration of agent technologies with legacy systems and its connection to the network, higher scalability and more efficient discovery mechanisms that allow a more agile communication [57]. Agile and robust communication is imperative to achieve future integration requirements of Industry 4.0.

4.2 Service oriented technologies

An increasing complexity in manufacturing systems is often composed as a set of numerous multi-disciplinary and heterogeneous systems, such as maintenance, engineering, warehouse and management. Those systems are considered as active components offering their capabilities as services representing mechatronic functions of equipment [64, 65]. That leads to the requirements of communication, data processing and interconnections among these services [66, 67] to fully utilize the benefits of flexibility, adaptability, scalability, seamless and effective integration offered by smart manufacturing [68, 69, 70, 71, 72, 73, 74]. The requirements are also well-recognized limitations of traditional manufacturing systems whose architectures have encountered the following main issues [75, 76, 77, 73] which is also illustrated by the Figure 4.3

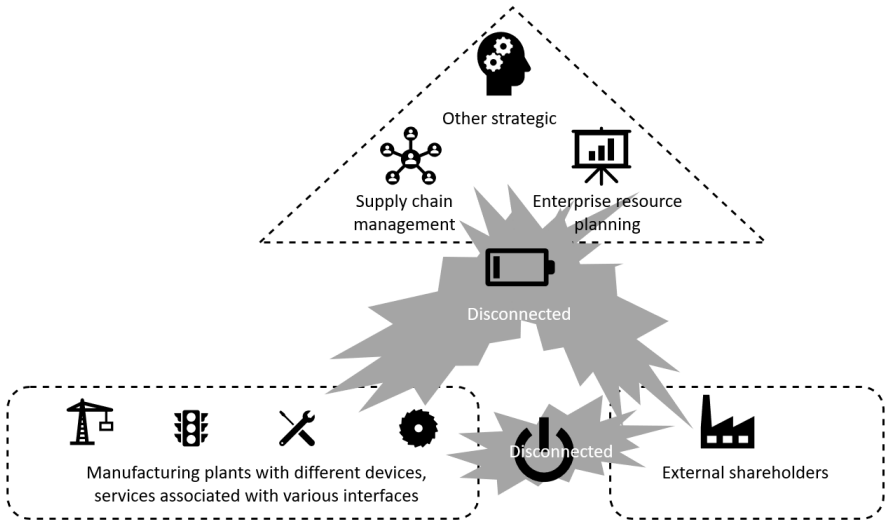


Figure 4.3: Traditional manufacturing with disconnections among business functionalities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

- Complex and time-consuming reconfiguration to adapt the market changes.
- Highly centralized resource utilization, unidirectional information flow and discrete decision making.
- Exponential complexity in scalability.
- Incompatibility between different manufacturing equipment and standalone specialized engineering tools in both internal and external business systems, which eventually results in all types of proprietary data format.
- Machines and other operating units in shop-floor systems are still commonly isolated from higher level business environments, although Manufacturing Execution Systems (MES) or similar enterprise management systems are starting to become increasingly available in the industry.

At the same time, manufacturing today requires a dynamic manufacturing environment to meet the turbulent market demand for highly customized products with high quality at low cost, fastest possible time-to-market via a complex supply chain from product level to connected business world [75, 76, 78] as described by Figure 4.4. These limitations and the challenges could be overcome by leveraging the information technology (IT) infrastructure of web services with the concept of SOA emerged at multiple organizational levels in business, and applied into the factory automation domain, which is characterized by a multitude of heterogeneous devices, networks, specific protocols and applications, and autonomous systems [69, 79, 65, 72].

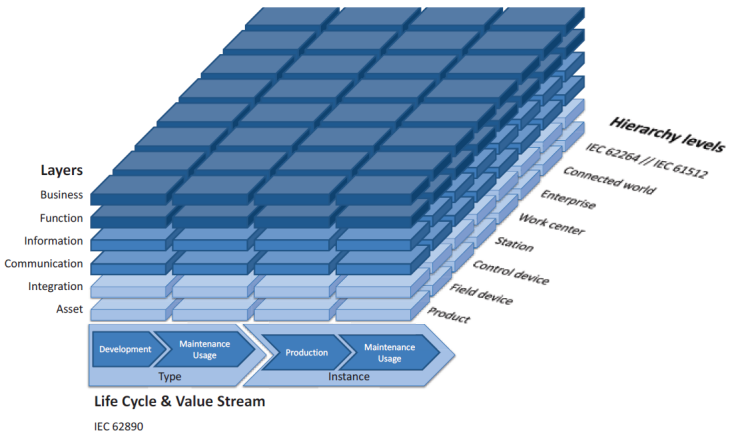


Figure 4.4: Complete integration supply chain along the life cycle of a production system, referenced by [80]

Generally, a SOA is composed by consumers and services that are participated and coordinated, meaning that they interact with one another to request services and resolve these requests via interactions determined by the service interface and typically expressed as a message as described by the Figure 4.5. A SOA is a multiple-layer and distributed information system architecture containing software resources packaged as consumers and services which are well defined, self-contained applications providing standard business functionality, and communicated among each other to request execution of their operations in order to collectively support common business tasks or processes [81, 79, 82, 83]. Even though the mentioned description of SOA could be incomplete, but two key properties of SOA are revealed as autonomous but interoperable systems, which can be achieved

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

with the following sub-section giving an overview of the design principles and supporting standards most frequently stated in research literature.

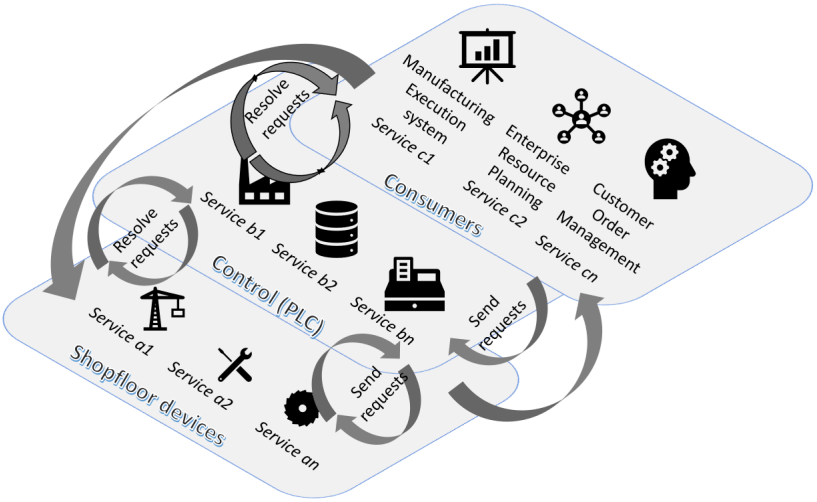


Figure 4.5: Send and resolve service requests among SOA consumers and services via exchanging messages in different system layers

Main SOA principles

To have an effective and sustainable implementation of SOA, there are more then technical capabilities. As other business systems, a successful SOA needs to integrate and embrace critical design principles related to development and management. In the context of SOA, a set of design principles is to define the framework of guidance in which service provides and business customers will plan for collaboration during the design and development of the system. Even though, the essential SOA design principles have still been under discussion [82], Table 4.1 summarizes the critical SOA principles recorded in SOA publications.

Main SOA principles	Jammes et al., 2005 [79]	Legner et al., [82]	Pagazoglou et al., 2007 [83]	Bean et al., 2009 [84]	Candido et al., [75]	Lojka et al., [85]
Business values	x	x		x	x	
Discoverability	x			x	x	
Reusability		x		x	x	
Loose coupling	x	x	x	x	x	x
Stateless	x	x		x	x	
Interoperability	x	x	x	x	x	x

Table 4.1: Agreed by authors in main SOA principles

- Business values: a SOA service is defined by focusing on how the service may fit in a larger business process context by following an outside-in approach and adapting a business process

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

centric instead of technology centric approach where the service often represents a business task [75, 79]. The scope of functionality on each SOA service is regarded as a key design decision in which the fine-grained services address small units of functionality or exchange small amounts of data whereas the coarse-grained services exchanging a larger quantity of data in one operation and supporting largely complete process activities are considered to be more appropriate [84, 75, 82].

- Discoverability: as the SOA service is designed, discovering a service is the first step to service consumption and reuse. it is largely ineffective if the service cannot be discovered even though a service might provide extensive functionality [84]. This principle makes sure that SOA services must have been published with a set of descriptive information to be found and accessed through discovery mechanisms [84, 75].

- Reusability: a SOA service should be developed in the right extent of generalization so that the original users as well as new users can exploit the functionality of the service [82]. This can be achieved with the service logic divided into different composable services. The objective is to avoid having to design and develop another new service even though the new users express their requirements that can be met by the functionality of the existing service [84].

- Loose coupling: when this principle is applied to the SOA design, the purpose is to protect the individual independency of each SOA user and SOA service to mitigate the impact of changes in underlying technology and behavior [84, 85]. In this sense, when SOA users and services are loosely coupled, the ability to add new functionality to the service would be highly enhanced without affecting previous users who are unaware by new additions to the service functionality. By means of dynamic service addressing via a logical name (e.g. a uniform resource identifier), asynchronous, message-based communication among SOA users and services and stateless service interaction, this principle can be accomplished [82].

- Stateless: this principle is also represented by the granularity of services where a service interface is mostly coarse-grained and based on the exchange document and messages [79]. By using a message to exchange requests and replies any direct technical connections between users and services can be avoided, which is realized by the service interface with a combination of a Web Service Definition Language artifact and an Extensible Markup Language (XML) Schema Definition Language as its referenced meta data [84]. In contrast, dependencies between the communicating entities, resulting in rigid and fragile systems, are weakness of the tightly coupled, context-related and stateful interactions typical of distributed object architectures create [79].

- Interoperability: by applying this principle, the SOA system allows users and services that are developed and platformed on different technologies to exchange information and collaborate among services [84, 83]. Specifically, an application installed in the machine to visualize its performance data might be programmed using Python, platformed on a server using Linux operating system and accessing a Structured Query Language database whereas users of this service might be developed using Visual C++. They may run on Windows platforms. These heterogeneous characteristics and possibilities in different platforms in a system are almost endless. The major advantage of SOA is to allow these users and services to be seamless integration, coordination and assembled to composite services, regardless of the technology on which they are built [75].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

A successful building architecture of SOA and services deployment will incorporate services and artifacts that take business values, discoverability, reusability, loose coupling, stateless, interoperability into account. The designers also need to have a framework with a set of rules from which compliance to these principles can be measured, monitored and even the contingency plan for appropriate remediation of noncompliance can be made [84].

Main SOA applications and supporting standards for achieving interoperability

It is very clear that SOA paradigm is currently expanding its impact in many fields of technologies, not only in the Information Communication Technology sector where it originated, but also in other domains of applications in which industrial applications have been adopted with several business collaborative initiatives [75, 79]. Many service-oriented solutions have been proposed by several European research projects, such as the Internet of Things at Work, Production Logistics and Sustainability Cockpit, Architecture for Service-Oriented Process - Monitoring and Control (IMC-AESOP), Embedded systems Service-based Control for Open manufacturing and Process automation, and Arrowhead framework projects, to build a software reference architecture based on the concepts of SOA in order to advance technologies in industrial systems [86]. Those SOA solutions are not specific to any one technology, vendor, or product, but there is a combination of different technology capabilities enabling SOA functionality, such as Enterprise Service Business, Service Registry and Repository, Business Process Management, Business Activities Monitoring, and Web Services Management (WSM) which is considered as one of the most common SOA service types [84]. In the context of WSM, the specification of the services standards is then necessary to have the exact definition, including the services discovery, services communication, service management, services security. Each services standard has various methods and tools [84, 87] as described by the Figure 4.6:

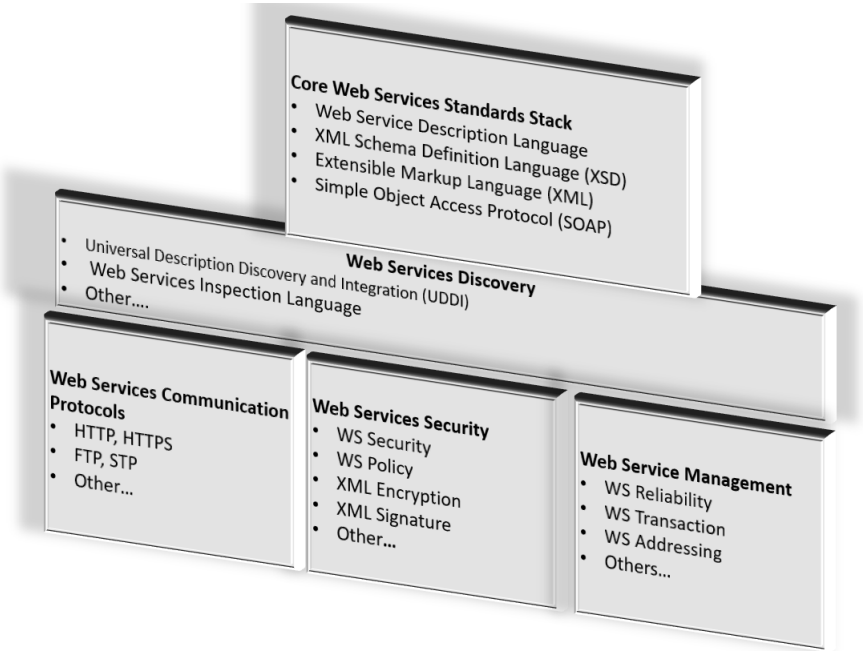


Figure 4.6: Web Services Standard Stacks, adapted from [84]

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

As mentioned, SOA is not restricted to any one technology, standard or tool and different SOA application may combine or mix different service types, technologies or standards based on the extent to which the SOA principles can be fulfilled. Table 4.2 briefly summarizes some SOA applications in industries, which shows different and various techniques.

Several SOA applications have been already starting to present their products and services compliant with the SOA approach. However, the current developments are now starting to put together a complete, unified and open solutions by following SOA guidelines and principles [75, 82], but many requirements and challenges indicated as the following part still needs to be overcome.

Challenges for SOA technologies

Not to mention possible implementation technical problems, designers also need to take into account several aspects and SOA principles while modelling a particular SOA-based application:

- Human-centered design: service interfaces should be designed and easily understood by humans and can be used by reasoning systems to understand and functionality for added-values [75]. This is linked to the SOA principle of business values.
- Granularity: It is often difficult to define the fittest granularity for a service to adapt to a specific application, which is also one of key points to distinguish the differences in approaching SOA-based applications developed by different companies [75, 82]. The service granularity indicates the overall quantity of functionality encapsulated by the service. For instance, an application releases a request to retrieve a complex machine status will have a coarser level of granularity than another application that simply needs status of an engine on the same machine. This is also linked to the SOA principle of business values.
- Reference architecture models: there is still a need to validate the reference architecture models that have been in the conceptual phase with lack of documented implementation of SOA-based cases [88], which is also recognized by the Table 4.2 showing some case studies in need of implementation validation.

There are still many important areas of interest for research. Table 4.3 indicates a comprehensive list of challenges in R&D identified by the industry Experts in area of manufacturing [89]. The first topic that was mostly expressed by the experts is the integration of shop floor, business processes and cloud services for plug-and-and product work. Asynchronous and interoperable communication mechanisms and publish / subscribe API were also equally received the concerns of the experts. Similarly, common language (e.g., OPC-UA) for standardizing object and services were also emphasized for future research and development agenda. Three mostly expressed topics above address directly interoperability in smart manufacturing.

4.3 Cloud technologies

The manufacturing sector is undergoing a change in which the demand of customised product is increasing [90] and the supply chains are taking a globalised perspective. This globalisation of manufacturing and supply chains has brought with itself the need and use of globally distributed,scalable, sustainable and service-oriented manufacturing platforms. A platform that takes this into account and builds on computing technologies, cloud computing, semantic web and associated service-oriented architecture is Cloud Manufacturing that caters to resource sharing. distribution and management of manufacturing services across the network [91].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Table 4.2: SOA-based case studies

Authors	Background	Standardized format	Result	Future focus
Cardoso et al., 2014 [81]	Integrate the strategic vision, to the shop floor and defined it through a formal semantic understood by humans and interpretable and processable by computers.	Business Process Execution Language will be the source for the architecture implementation of services using the DPWS or, (XML).	A useful approach that allows an integrated view of a field in its various disciplines, from an available database and strategic alignment with the organization's goals	Require further implementation of context-sensitive paradigm applied to industrial automation.
Colombo et al., 2014 [64]	Demonstrated with real industrial use cases various aspects with respect to next generation supervision control and data acquisition, paving the way from web-service enabled systems to cloud-based industrial CPS	Device profile for web services, combined with Efficient XML Interface (EXI), OPC Unified Architecture (OPC-UA)	Optimization of the operation of the plant provided by new monitoring indexes and control functions exposed and/or applied as Web Services	Security is largely ignored by limiting its security capabilities to Hypertext Transfer Protocol basic authentication and Role-Based Access Control for service calls [86]
Luder et al., 2017 [80]	Integrate the production plant model of a demonstration plant based on Fischertechnik plant models created for teaching purpose	AutomationML, which is a kind of data format for the exchange of information based on XML, which is an open standard in IEC 62714	An Open Platform Communication (OPL) client has been installed on a standard mobile PC able to browse the AutomationML project and accessing the functions on the PLC.	The presented approach is far from being a fully standard compliant implementation. Especially, the provision of adequate services for accessing technical functions and information is still in a draft state
Ye et al., 2018 [73]	Propose the architecture for an industrial process control system	Using integrated AutomationML and OPC UA technologies	An entire process-control system was modelled, and horizontal and vertical interconnections between the enterprise layer and field devices were achieved	Require further implementation into the proposed production-control system to fully assess comprehensive performance, and more field devices
Zhang et al., 2020 [74]	Solve the information exchange and manufacturing resource sharing for CPPS integrated with Digital Twin in the context of blisk machining	AutomationML	Through the experimental platform, it realizes the integration and sharing of resources, although all these resources are not located in the same plant	To research further on how CPPS can diagnose and predict their own state based on simulations.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Research and development challenges	Moghaddam et al., 2018 [89]
Integration of shop floor, business processes, and cloud services for plug-and-produce work	Highly voted
Asynchronous and interoperable communication mechanisms and publish/subscribe API	Highly voted
Common language (e.g.,OPC-UA) for standardizing object and services	Highly voted
Standardized taxonomy of manufacturing processes as services	Medium voted
Mechanisms for orchestration, filtering, aggregation, and sharing of cloud services	Medium voted
New models for automated, on-the-fly creation and governance of value networks	Medium voted
Fully-integrated industry—inter-enterprise, cloud-based publication and sharing of services	Lowly voted
Service representation, composition, discovery, registration, and matching	Lowly voted
Service definition—shift of focus from macro to micro services in manufacturing SOA	Lowly voted
Representation of complex capabilities such as cognitive systems or analytics as services	Lowly voted
Need for 'smarter' objects to execute more complex services	Lowly voted
New models for the economics of acquisition, implementation, and integration	Lowly voted
Horizontal integration of product life-cycles through micro-services	Lowly voted
Need for autonomous, self-/environment-aware, intelligent devices for service-orientation	Lowly voted
Concurrent optimization of order-to-cash and design-manufacture-maintenance cycles	Lowly voted
Lack of horizontal integration and reconfigurable manufacturing capabilities in ISA-95	Lowly voted
Integration of ISA-95 into a cloud-based architecture	Lowly voted
Lack of modularity of legacy manufacturing systems hindering 'composability	Lowly voted

Table 4.3: SOA-based research and development challenges towards to interoperability in smart manufacturing, adapted from [89]

[91] proposes the widespread utilisation of manufacturing resources by cloud following a pay-as -you-go model. Microsoft showed a favorable viewpoint of people towards lowered cost of IT infrastructure, geographic collaborations and effective response to dynamic market demands. The section goes into detail with the cloud manufacturing environment and associated technologies.

The Concept of Cloud Manufacturing

The changing manufacturing environment has brought with itself a trend of cloud computing. The basic embodied idea is of conversion of manufacturing resources and capabilities into entities capable o being componentized, combined and enhanced. [92] established an idea of cloud concept in detail and presented a system that was service oriented and inter-operable. The system revolved around the customer/cloud user and enterprise user. Methodologies and data models that elaborated the concepts of cloud manufacturing were discussed. These concepts revolved around on-demand basis resources that followed a deployed-as-you-need model so that resources may be used with minimalist

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

interaction. The cloud services can be mainly divided into Platform as a Service (PaaS), Software as a Service (SaaS), Infrastructure as a Service (IaaS). Application of such services in manufacturing environment is fundamentally the concept behind cloud manufacturing.

Cloud manufacturing builds its foundation by strongly deriving forces from respective technologies like reconfigurable, flexible manufacturing, collaborations and simulations. However, the system in the manufacturing environment in itself needs to be setup for combination and inter-operability to cater the requirements for cloud manufacturing. The effective utilization of these modelled resources is carried out in manufacturing cloud to establish a framework for manufacturing process. For such kind of integration it is essential that a neutral API should be utilized to establish a direct connection to manufacturing environment without changing enterprise wide structure.

Cloud Manufacturing Architecture

A multitude of architectures have been proposed for cloud manufacturing environments with underlying principles catered to integration at all manufacturing levels. [93] developed a architecture based on four-layers i.e. manufacturing resource, virtual service, global service and application layers. [94] developed a five-tier cloud manufacturing system that dealt with co-operation between manufacturing resources, resource management and implementation, portal for cloud manufacturing, a unified cooperation platform and cooperation support application layer. A cloud manufacturing solution for automotive sector was explored by [95] in which it was treated as a SaaS based on four layer architecture (core service, business service, cloud sub-system service and related business service). [96] proposed an intelligent perception system based four-layer architecture that accessed cloud resources based on IoT data. The resources can change dynamically based on acquired data. A case for factory automation based on cloud manufacturing services was laid down by [97] based on service and application layer, manufacturing resource and system virtualization. A detailed architecture for cloud computed manufacturing environment was established by [98] comprising of resource, perception, resource virtualization, cloud service, application, portal, knowledge, cooperation layer, security and internet layer. [99] proposed addition of data layer in their cloud manufacturing architecture. They presented a three-tier architecture with functional, interaction and data layers. Knowledge-as-a-service was developed as an additional layer for product design knowledge integration in cloud architecture by [100]. [101] focused on manufacturing-as-a service description usage in manufacturing cloud environment. However, [102] focused on developing of a front-end for providers and consumers to communicate their services and demand.

Other architectures for cloud manufacturing were developed by [98] with resource, perception, service, application and middle-ware layers acting as a five-tiered hierarchical environment.[103] formulated a 12 layered service platform architecture with optimal and required layers. [104] introduced the concept of broker services in cloud platforms.[105] presented a six-layer architecture with focus on resource access. [106]presented a resource service composition with flexible management with control for function, monitoring and co-ordination. A detailed four layer and six layered architecture was presented by [107] and [108] respectively. [109] developed semantic descriptions for peer-to-peer based advertisement, composition of services and discovery of resources in cloud environment. [110]combined cloud computing with SOA to develop a unified cloud manufacturing architecture.[111] based their six-tiered architecture on product information sharing and integration of cloud security modules on cloud platforms. A knowledge management system reliant six-layered architecture (knowledge source, acquisition, storage, retrieval, innovation and publishing) was proposed by [112]. [113] presented a interoperable cloud based manufacturing system (ICMS) comprising of three layers namely user cloud, smart cloud and manufacturing cloud layer.

Common data models supported by control rules are fundamental requirement for incorporating

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

such architectures for a wide product scheme. The data models in this case should support a common data standard like STEP/STEP NC for inter-operability purpose. In spite of this a significant gap is available of cloud solution for the whole supply chain. A knowledge fusion architecture was defined by [114] that provided knowledge assignment and acquisition capabilities at different phases of design activities. [115]gave a cloud architecture for cloud applications in manufacturing environments.[116] expanded the standard cloud manufacturing architecture by introducing internet of things, service oriented technologies and high performance computing into the mix. The research built up a prototype system for cloud manufacturing for targeting TQCSEK (Faster time to market, higher quality, lower cost, better service, cleaner environment and high knowledge). However, the prime issue with such kind of manufacturing environments is the lack of fluidity in centralized management, lack of proper service distribution mechanism, efficiency, quality and timeliness.

The realization of resources is usually carried out by a perception layer which is comprised of perception, connection, information technology and processing. Service layer builds on the perception layer to establish service pool of resources and capabilities. The working layer is responsible for interaction protocols, extensive transactions and management of tasks. The application layer is primarily concerned with interacting with users through APIs and cloud-end interface.

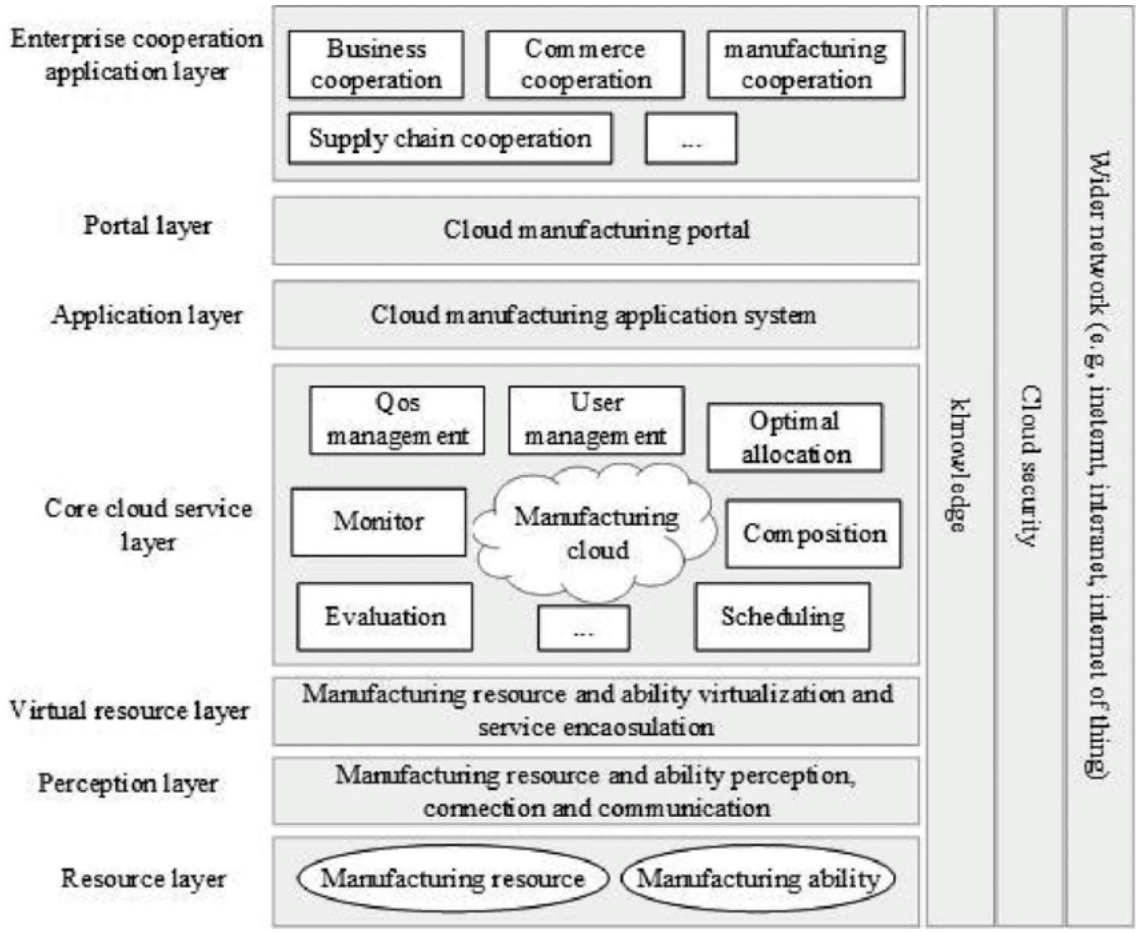


Figure 4.7: Architecture of Cloud Manufacturing [117]

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Cloud Manufacturing Models

The established architecture gives infrastructure of the data layers for cloud manufacturing in the manufacturing however models have been formed that represents the concepts and rules on which these architectures will be based on. One such model was developed by [118] for cloud based design and manufacturing. The model deals with interaction between consumer, broker, carrier and provider. [119] developed a distributed infrastructure with centralized interfacing system model that defines interaction between users and management with humans and manufacturing processes. The cost effect and breakdown model for cloud manufacturing service platform was developed by [120]whereas [107] presented a model by combining resources, functional information, process information and related concepts. [121] proposed a CM model for running and functional view of services. A more generalized principle model of Cloud manufacturing was given by [122].[98] presents a detailed cloud manufacturing model with seven phases namely task description and definition, modelling, service search, match, evaluation, composition and selection, control, implementation and evaluation. Work in model has also been done on capability [123],process and virtual resource [124]and sharing of manufacturing resources [125]. Cloud manufacturing models should as per research provide certain characteristics including on-demand service, support agile virtual organisation, means of perception and knowledge based manufacturing.

Cloud Manufacturing Frameworks

Cloud manufacturing frameworks provide support to developed architectures. These define the underlying principle by means of which the layers of the architecture communicate and move data from each other. [126]utilized UDDL and OWL-S for discovery of manufacturing resources. A method of defining correlation between cloud service relationship was developed by [127] . [122] proposed a process route for task scheduling in a cloud architecture. An idea for cloud manufacturing task scheduling for resources was developed by [128](Li et al. 2012) wherein tasks were decomposed and matched with resource requirement by matching static properties. [129] presented a process framework for optimal allocation of computing resources. A framework for sensor-driven process planning environment for distributed setups was established by [130] name Wise-Shop Floor dealing with scheduling, monitoring, control and planning of resources. A three layer virtualization cloud manufacturing framework was proposed by [99]. A service and web oriented architecture framework with SaaS offering collaboration of internal operation with customers and supply chain network was established by [131]. A semantic web-based system framework reliant on modelling, acquisition and retrieval of manufacturing resources was laid out by [132]. On the other hand a detailed framework for perceiving and accessing of manufacturing resources was developed by [133].

The majority of literature builds the cloud environment in manufacturing on grounds of manufacturing resources, manufacturing capability and cloud manufacturing services. The containerization here is of vital importance as the very concept can be considered as a container wherein the resource is contained inside capability and the capability deployed in the manufacturing cloud as a cloud service. Design capability, production capability, experimentation, management and communication capability set up the baseline for manufacturing capability concept. On the other hand the resources could be broken down into hard and soft resources with combination of them and capabilities yielding into a capability description model. In cloud manufacturing environment the platform users can be categorized as cloud provider and cloud request maker. Manufacturing cloud services consists of resources and capabilities encapsulated in cloud environment. This service is responsible for containing libraries of resources (virtualized and distributed) which could be queried and allocated as per needs of the user. An on-demand resource pool can be deployed and published as potential usable services in this manner.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Manufacturing cloud fulfills the fundamental requirements of manufacturing by aggregating the cloud services per rules and algorithms. Manufacturing cloud can be further extended to public and private cloud. Private cloud is organisational whereas the public cloud is society oriented i.e. a group of manufacturers come together to offer services which are not bound by organisational boundaries. In both cases the cloud services comprises of service layer, transmission network layer, resource layer, perception layer, virtual access layer and terminal application layer.

The Underlying Assumptions in Cloud Manufacturing Environment

For an effective cloud manufacturing platform first steps involves formulation of virtual supported subsystem. This subsystem is responsible for mapping of resources, customization, faults and status of resources and accessing operation which the resource needs to perform. This assumes that there exists a cloud service management system that controls these aspects. Further also it deals with ontologies, semantics and service registration.

Cloud Manufacturing Platforms

Research into Cloud manufacturing platforms involves integration of data and resources across environment. [134] presented a cloud-manufacturing platform XMLAYMOD that supported manufacturing collaboration and data integration on ISO 10303 (step standard). Distributed Integrated Manufacturing Platform (DIMP) by [93] provided basis for integrative CAx environment in production. The interaction happens on requests and task from the user. Research done by [109] presented a CMfg platform for multi-user and service based interactions. Cloud Agent for integrating services in platform was developed by [135] . For cloud based manufacturing environment a cloud service for resource sharing was discussed by [125]. Functionality of cloud manufacturing services and control was explored by [136]. A communicational ability embedded cloud platform was presented by [137] to enhance interoperability.

Cloud Manufacturing Applications

Practical applications for cloud manufacturing environments have been developed. BISTOP developed by [103] served as a means for validating CMfg in SME. Manucloud [138] served as an MaaS infrastructure with service disruption structure capability. A cloud service monitoring system was also developed by [136]

Barriers of Cloud Manufacturing

Usually parallel execution of tasks takes place in a manufacturing environment at different resources guided by a schedule either a manual one or guided by a scheduling program. The resource service provider in case of cloud manufacturing environment is responsible for for such scheduling tasks. However, the current issue with such a method is the lack of optimal allocation of resources and prioritization conditions for jobs. One of the major barriers for cloud service in manufacturing despite of network system of manufacturing is the lack of intelligence in effective matching capability of resources to job, resource changing dynamics and quality of service.

The on-demand service criterion of cloud manufacturing although aided by networked resources for optimal allocation lacks a proper mode for transactions and re configuration management. In this regard a definite cloud manufacturing environmental model needs to be established for promoting flexibility, standards, operational mechanism and safety aspects. Embedded technologies in recent

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

research have been worked upon to provide intelligent access to physical devices. In order to introduce such interconnections both of information and physical resources high computing requirements are present.

4.4 Fog/Edge

4.4.1 Edge computing

Edge computing may be referenced as the accompanied tasks performed at the very Edge of the in-house platform that is in direct communication with the cloud environment. The major advantage Edge computing has is to minimize latency, reduce cost, reduce bandwidth and improve bandwidth in industry 4.0 applications.

The increase in IoT device usages in complex scenarios like monitoring manufacturing devices, controlling production applications [139], energy optimization [140] and other applications [141] has brought about new opportunities and challenges [142]. Cloud computing follows a centralized structure wherein the resources are centralized to a region or distributed on a remote Cloud servers. A major drawback in cloud computing is presented towards reduced latency and real-time response. This is going to further increase only as more and more devices get connected to IoT networks.Edge computing application caters these problems by optimizing storage and computing process before processing them to cloud services. So majorly processing then plays out at a prior stage before being sent to remote servers [143]. Also, these processing tasks utilize essential parts of storage and computing near to the 'Edge' of device locally and no longer require Cloud services for these. This benefits in reducing the associated cloud costs, network traffic overloads, computational requirements for IoT applications.

The Internet of Things devices deals with interaction and communication that occurs between devices generating and exchanging data with real world [144]. This compliments with the characteristics of IoT such as heterogeneity [145], capability to interact with a large volume of events [146] and generate data in real-time [144]. Digitization of acquired data enables measurement of physical world and through data transmission this data could be processed and analyzed and converted to information to be used by intelligent production machines. The large amount of data transmission required for Data Analytics and Machine Learning scenarios however requires much higher bandwidth [147] that brings much higher cost association requirements.

Moreover, this enables that data can be filtered and prepossessed at the edge of the network instead of being propagated to the cloud environment. This results in faster service and significant reduction in response duration [148]. Open platform, enabling technology and computer resources are the major components of cloud computing definitions. [149] proposes cloud computing to be a paradigm wherein the computation can happen close to the data source, all the enabling technologies for this may come under edge computing. The concept of cloud lets was discussed in [150] that comprises of storage resources, computing nodes, micro data centers and fog nodes are placed within the vicinity of device's internet edge, near the sensing technology of the device. The Edge Computing Consortium sees the Edge Computing as a combination of network, storage and applications that offers distributed open data platforms near network edge. Edge computing by offering intelligence services at the edge of network fulfills the requirements of security, connectivity and real-time services. This elimination of time and distance required for transport to and from cloud data service environments enhances the speed of processing and enhances the performance of data as loss of data is minimized.

This shifting of the computation capacity to edge nodes near the data source offers saving of bandwidth and storage resources [151]. This is because that data which offers no value is filtered at

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

the edge before being transported. Higher proximity and low latency along with enhanced scalability are realized due to decentralized storage and processing. This in turn enhances security and improves privacy as edge computing provides each computation node a certain degree of isolation.

Edge Computing Architecture

The reference architectures of Edge Computing consists of recommended structures, products and services that form industry specific standards, suggestions, best-practices and optimal technologies that act as an enabler for edge computing. These architectures provide a means of collaboration and communication in an organisation around an implementation project [89].

This architecture was developed to aid the adoption of decentralized automation as a part of H2020 FAR-Edge project. The architecture in itself presents a framework for implementing FAR-Edge project platform. The enabling technologies realised, similar to block chain, is based on Edge Computing and Distributed Ledge Technologies (DLT).

On a general level the architecture could be divided on scopes and tiers as their constituents. The scope consists of elements that form the industrial environment such as machines, field devices, SCADA, MES and ERP system among others. Tiers on the other hand detail the system components and their association with each other.

The architecture consists of three fundamental layers namely field layer, edge layer and cloud layer. The field layer is the lowest layer consisting of devices at the work place. They may be machines, sensors, actuators or any other component linked to edge node. The edge layer consists of software for running on respective edge nodes, These serve as Edge gateways that provide the computing devices with a dynamic link between field layer and digital world providing capability of performing real-time data analytics. The architecture security is assured by providing a Ledge based on blockchain technology by means of smart contracts. Cloud layer on the other hand consists of cloud servers responsible for planning, monitoring and managing resources and performing logical execution of functions.

The main advantage that FAR-Edge architecture presented was implementation of Edge computing while ensuring information security through block chain. This architecture provides reference use case of automation and analysis in industrial environments.

Huawei, Shenyang Institute of Automation (SIA), Intel, ARM, iSoftStone and China Academy of Information and Communication Technology (CAICT) created Edge Computing Consortium (ECC). ECC jointly working with Industrial Internet Alliance (IIA) presented Edge Computing Reference Architecture (EC-RA) 2.0 based on international standards like ISO/IEC/IEEE 42010:2011.

Edge Computing Reference Architecture 2.0 follows vertical and horizontal service and layer model. The vertical services involved are management, data life-cycle and security offering intelligence based service for complete life cycle. Horizontally EC-RA 2.0 open interface layer model is projected with smart layer, service fabric and connectivity and computing fabric. Smart service basis its realization of model-driven service framework. Important components of these layers is development service frameworks and deployment and operation service framework. The components enable uniform software development and implementation. Service fabric is responsible for fast deployment of service policies and parallel processing of products. This layer defines tasks, processes, path plans and control parameters that may aid to such notion. The connecting and computing fabric is responsible for deploying operations and coordinating between needs and computational resources services of the organisation. The Edge Computing Node (ECN) is compatible with diverse heterogeneous connections. At this layer the ECN provides real-time processing and response capacities along with security integration with hardware and software.

Industrial Internet Consortium (IIC) like ECC also developed its own reference architecture using

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

ISO/IEC/IEEE 42010:2011 standard. This standard assists in identification of convention, principle and practices for coherent architectures and frameworks . This architecture majorly consists of three layers mainly edge, platform and enterprise layer.

Edge layer is responsible for data acquisition from edge nodes through its nearest proximity devices. The constituents features of the layer are depth of distribution, nature of proximity network, the location of nodes and devices and governance policy. The intermittent Platform layer is mainly responsible for sending command from Enterprise to Edge layer. It groups the processes for analysis of data flows and manages the active devices by consultation and analysis through domain servers. Enterprise layer houses support platforms responsible for generating control commands to Platform and Edge layer and receiving data flow.

The architectures provide a means of complimenting Cloud services as the last level of architecture rather than replace them. This presents a beneficial case whenever significant population of IoT data exists. Edge nodes in such cases could be the initiating point for accumulation, controlling and reducing the data before passing it forwards to cloud services. By this approach reduction in storage requirements, decrease in latency and real-time response is achieved.

From the established architectures FAR-Edge architecture has main significant focus on security of data transfer. It proposes an intermediate Ledger layer based on smart contracts over block chain. It follows a evaluation and approval by peer nodes model for each consecutive change in state. Edge Computing R.A 2.0 emphazises the use of ISO/IEC/IEEE 42020:2011 standards and drives the application through IEC 61499 standard proposing Functional Block based architecture design. This makes the setup modular as the basic unit of model is accompanied by input, output and internal functions. These blocks remain restful until they receive input signal and maintain independence and portability. IIC architecture has its significance at Enterprise Layer where process and application specific software maybe hosted on private or public cloud.

In all of these architectures the main driver is the ability to analyze data at the level of local devices and edge nodes and offer real-time processing capability before transporting the data to cloud. However, further effort could reduce operating and management costs as a result of traffic and data transfer reduction between Cloud services and Edge nodes. Edge computing present a case for latency reduction as application can transfer and receive data near to source. Moreover, security could be enhanced by development and deployment of secure data transfer protocols.

4.4.2 Fog computing

Just like challenges served by edge computing i.e. high latency, low capacity and network failure, the fog computing brings devices closer to cloud. Locally available data processing and data storage at the device is offered by fog computing hence faster response and better quality. This makes fog computing an enabler for efficient and secure services for IoT device.

Initially IoT was envisioned as a means of reducing human data entry efforts and utilize sensors to collect, store and process the data [152, 153]. IoT has multiple pertaining issues like performance, security, privacy and reliability because of limited computational capability however integration with cloud can mitigate these issues. The heterogeneous platforms in different IoT devices the development and integration becomes a tedious task [154]. Large amounts of data generated by IoT device requires high bandwidth to send the data to and from the cloud [154]. This is one of the factor for usage of fog computing platform.

Fog computing was coined by Cisco [155]. Fog computing works to compliment the challenges face by traditional cloud computing. It provides data processing capability along with storage on fog devices locally. It therefore ends up reducing amount of data transfer, improving efficiency and performance. This integration enforces the idea of Fog as a Service (FaaS) wherein a service provider

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

could provide multiple fog nodes along its domain and house and give out data processing, storage and networking capabilities as desired [156]. FaaS presents the advantage of a scalable solution environment in order to operate and deploy computing, control and storage services to a varying customer density [157].

Fog computing helps in overcoming challenges of latency, capacity constraints, resource-constraints in IoT devices, network failure and enhanced security [158]. The greatest challenge in cloud computing comes in face when the tasks are time-sensitive and internet connectivity not the most optimum [159]. To address these issues Cisco presented an alternative in form of Fog computing [155].

Definition and Concepts

Fog computing offers limited capabilities in terms of computing, storing and network services between different end devices. It offers capability in latency-sensitive environments [160].

Researchers have built up on the definition from the original term as coined by Cisco [155]. [161] provides a general definition of fog computing as geographically distributed computing environment that consists of connected heterogeneous devices that offer elastic computing, storage and communication in an isolated environment to a large scale of clients in proximity. These services may or may not be backed by cloud services. [162] provides a definition wherein a large number of ubiquitous and decentralized devices communicate and cooperate among themselves and network to prove networking and computation capability for application and services in an incentives setting. OpenFog consortium defines such a paradigm as a horizontal system-level architecture wherein the resources are distributed for computing, storage, control and networking along Cloud to Things.

Characteristics of Fog Computing

Fog computing is considered to be an extension of cloud computing having nodes closer to end devices themselves. Fog devices act as an intermediary between cloud and end devices bringing processing, storage and networking closer to end devices deployed anywhere in a network. Any such device can act as a fog node [160]. [154, 161] lay down the characteristics of fog computing.

Fog computing provides low latency and location awareness. Fog computing nodes therefore could be employed at multiple locations. Since fog nodes are near to devices they provide low latency when data processing. Fog computing nodes are geographically distributed instead for centrally distributed like in cloud computing. They could be deployed anywhere. Fog computing architecture is scalable in nature. They can be scaled up to meet the processing needs. They provide support for mobility. They provide incentives for being paired up with mobile devices and enabling mobility methods such as locator id separation protocols (LISP).

Fog computing provides basis for real-time interactions, heterogeneity, interoperability and support for on-line analytic and cloud communication. Since fog nodes are designed by different manufacturers they come compatible with multiple platforms. Therefore, they can inter-operate and working with multiple domains and service providers. Since they are present near to source they serve as a medium of absorption and processing of data close to cloud services.

Fog computing architectures

Main preference of fog computing in comparison to cloud computing lies with providing low and predictable latency for IoT application that are time-sensitive [163]. Traditional fog computing architectures consists of six layers namely physical and virtualization, monitoring, pre-processing, temporary storage, security and transport layer [164, 165, 166].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

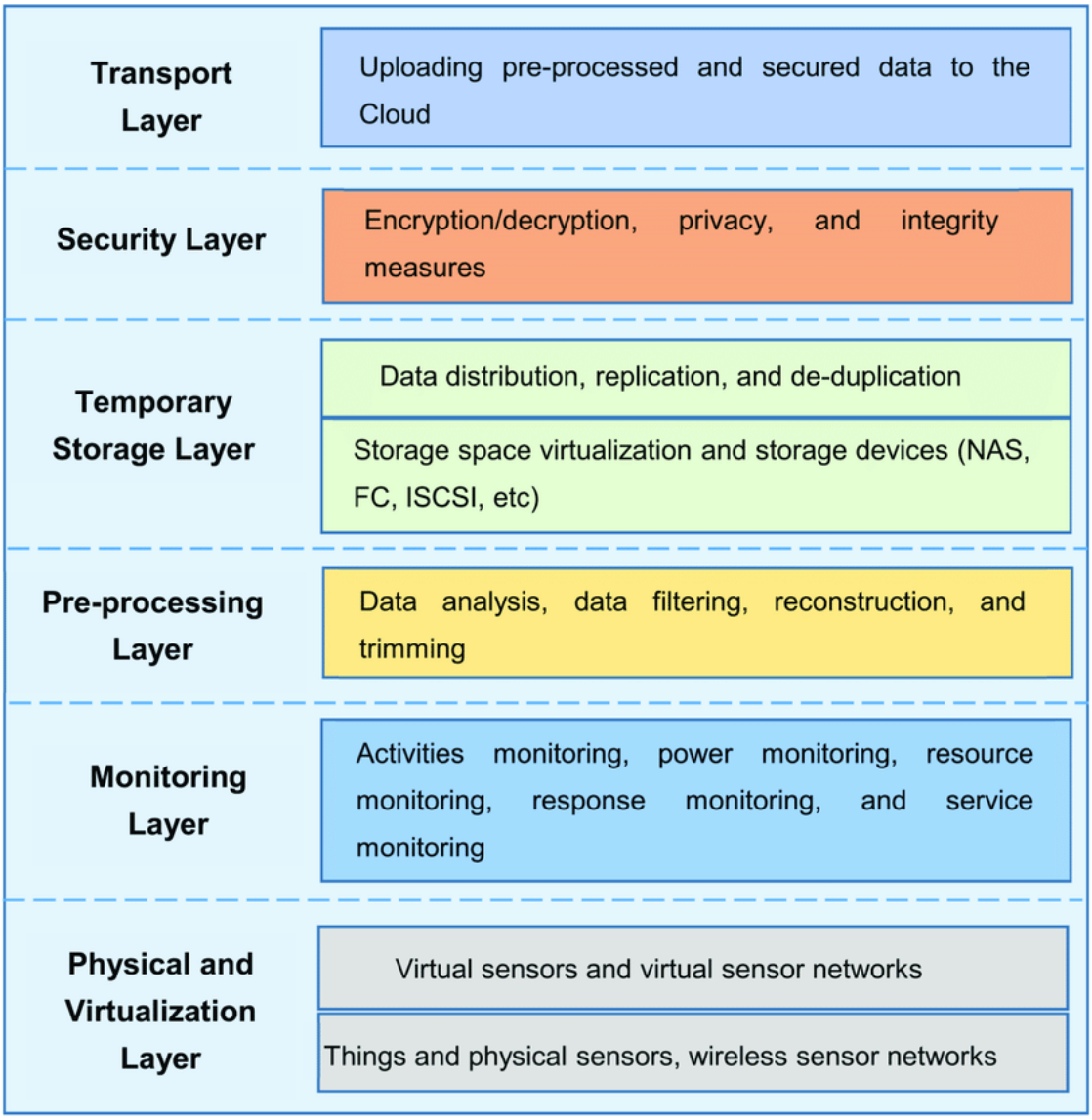


Figure 4.8: Architecture of Fog Computing [167])

The physical and virtualization layer involves physical nodes, virtual nodes and sensor networks. The management of nodes in this case is dynamic depending on their types and service demand. Sensor network deployed over geographical locations sense the surroundings and send data to higher layers via gateways for analysis and processing [168]. Monitoring layer on the other hand keeps check on availability and usage of resources, sensors, fog nodes and network infrastructure. This layer also deals with the type of tasks that need to be performed by this and consecutive nodes, time of requirement and monitoring of the current status of the node [164]. Energy consumption may also serve as a driver for this layer as fog nodes uses many devices with varying energy requirement conditions [164, 166].

Data management is primarily deal in at pre-processing layer. Data collected, analyzed, filtered,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

and trimmed to drive useful information. The data stream from this layer is then housed in temporary storage layer. The data transferred to cloud is redacted from the local temporary storage layer. The transmission of data is effected by security layer where the encryption and decryption of data comes into play. Moreover, privacy and integrity features extend the security of data making it prone from tampering. This data, which is now hosted in transport layer, uploads the data in cloud for further usage [164, 166]. Fog computing enables segments of data to be uploaded in cloud through a smart gateway [169] that manages data distribution to cloud. This emphasises on proper communication protocols for fog computing with efficient, lightweight and customization of data stream to be major concerns. Therefore fog computing communication protocols depend on application scenario of fog.

Fog computing and internet of things

Fog computing is a relatively new research stream and the convergence of IoT application with fog computing are still being expanded upon. [155] proposed a fog computing platform to provide support to resource-constrained IoT devices. [170] deals with aggregation and processing data locally along with load balancing. [171] proposed a hierarchical distributed architecture for fog and applied it to technological applications. [172] expanded the safety and security concerns of fog computing paradigm whereas deals with those issues when integrating fog computing in existing environments.

[173] provided the viewpoint of fog computing as an extension of cloud computing. [174] presented the case for congestion and latency problem handling along with practical applications. A dynamic methodology of management of resources was given by [166] along with adaptation to different requirements of cloud services. [175] presented a survey of existing challenges and barriers while fog computing implementations. An adaptive operations platforms (AOP) [176] provide end-to-end management of fog computing infrastructure regarding operational demands of industrial process. [163] discusses application of fog computing on healthcare sector in terms of characteristics. A reference architecture for fog computing was proposed by [177] serving requests to fog nodes rather than cloud services. Challenges and barriers with respect to networking context of IoT in fog computing was discussed by [157]. Delay-sensitive utilization of fog computation resources was elaborated by [178] in their work wherein a framework was proposed for fog resource provisioning. [179] discusses an application of fog computing in vehicular control by establishing a Vehicular fog computing (VFC) architecture to enable communication and collaboration between end users for resource management. VFC was further extended in [180] wherein they proposed a cross-layer architecture for decision making process and discussed service disruption effects and types in fog computing.

A general framework was established in works of [181] to understand, evaluate and model service delay in fog computing applications. Fog computing challenges with respect to mobility was discussed [182] while presenting three scenarios. [183]provide a taxonomy of fog computing according to challenges and features of fog computing.

Challenges and Application of Fog with IoT

[157] discussed the challenges of cloud technologies and how fog computing can solve such issues. The prime challenges discussed relate to latency constraints, network and bandwidth, resource, service interruption and security constraints in cloud services. The new challenges in fog computing is essentially accompanied by a wide implementation of fog computing in significant areas of research. Autonomous cars is an area where fog computing can be more beneficial than cloud computing because of time-sensitive response needed. Research towards hands-free cars are gaining popularity and talks of infrastructure that talks with each other is becoming norms. Smart traffic lights in this

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

sense can play a pivotal role [174]. This technology can be quite beneficial on ensuring vehicle and pedestrian safety [184].

Other applications include smart homes with devices on different platforms communicating with each other and other resources[161].Wireless Sensor Network (WSN) provide the opportunity to link up sensors and actuators for optimizing energy consumption in control scenario. This reduces bandwidth utilization, energy consumption and processing power. Health care and activity tracking [163], CPS [155] and augmented reality [185, 186] also see significant utilization of fog computing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Chapter 5

Cyber-safety and security in smart manufacturing

In recent years, 'Cyber Security' has emerged as a widely-used term with increased adoption by practitioners and politicians alike. However, as with many fashionable jargon, there seems to be very little understanding of what the term really entails. Although this is may not be an issue when the term is used in an informal context, it can potentially cause considerable problems in context of organizational strategy, business objectives, or international agreements.

A key challenge highlighted is the ambiguity introduced by the thoughtless use of the term 'cyber security,' where nuanced definitions (Information Security or IT Security) are more appropriate and descriptive. They suggest that the term cyber security is only used in context of security practices related to the combination of offensive and defensive actions involving or relying upon information technology and/or operational technology environments and systems.[187] In the analysis of national cyber security strategies of European Union member states, it is provided a terminology guidance in the annex explaining that there is no universally accepted nor straightforward definition of 'cyber security.' They write that some people regard cyber security as overlapping with information security but no definitive conclusion is provided. Cyber security is a branch of information security.

Figure 5.1 shows these nested categories where information assurance and security (IAS) topics are the broadest category, encompassing cybersecurity (CySec) topics, which in turn encompasses the more specialized computer security (CSec) topics.

Recent high profile hacking's have cost companies millions of dollars resulting in an increasing priority to protect government and business data. Universities are under increased pressure to produce graduates with better security knowledge and skills, particularly emerging cybersecurity skills. Although accredited undergraduate computing programs recognize the need to solve this problem, these computing programs are constrained by accreditation standards and have limited ability to modify their curricula. This paper discusses a case study on how one Accreditation Board for Engineering and Technology (ABET) accredited undergraduate IT program created a strategy to continue to teach existing security-related topics as well as emerging cybersecurity topics within its IT curriculum without increasing credit requirements. The faculty developed an IT Security-related and Cybersecurity Curriculum Taxonomy to identify strategies to move security-related topics taught in the higher level courses to lower and intermediate courses. Thus, emerging cybersecurity topics could be added to high-level courses.

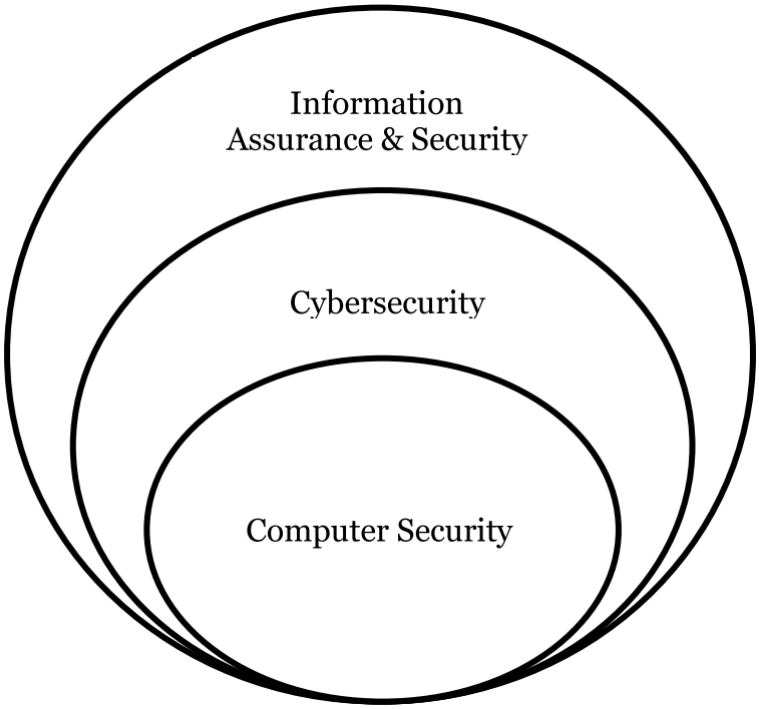


Figure 5.1: Computer Security, Cybersecurity, and Information Assurance and Security Relationships

5.1 Vulnerability of manufacturing systems

A cyber-physical vulnerability impact analysis using decision trees then provides the manufacturer with a stoplight scale between low, medium, and high levels of cyber-physical vulnerabilities for each production process. The stoplight scale allows manufacturers to interpret assessment results in an intuitive way. Finally, a case study of the pro- posed approach at an applied manufacturing research facility and general recommendations to securing similar facilities from cyber-physical attacks are provided. [188]

With the goal of identifying cyber-physical vulnerabilities within a manufacturing process, the proposed vulnerability assessment approach is based upon the idea that vulnerabilities in manufacturing systems occur at intersections (and intra-sections, referred to collectively as intersections) of cyber, physical, cyber-physical, and human entities that embody a manufacturing system. A visual representation of how these entities and vulnerabilities interact within the vulnerability space can be seen in Fig. 1, where intersections should result in an expected transformation. How- ever, the actual transformation could differ from the expected one, even when considering nominal variability within the production process; due to the existence of some type of vulnerability. This transformation would then act as input to the next intersection and this procedure would continue through every intersection in the manufacturing process.The proposed approach starts with mapping intersections and analysing the vulnerability impact at each intersection node; as shown in Figure 5.2.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Figure 5.2: Outline of the proposed vulnerability assessment approach

5.2 Cyber threats and risks

In these internet-based inter-operable manufacturing contexts, the cybersecurity threads represent one of the most significant challenges. The entire business model can be affected due to the vulnerability of manufacturing systems. In 2009 and 2010, the famous attack was recorded with a worm called Stuxnet that controlled the computers connecting to programmable logic controllers to change configurations of centrifuges to cause the possible destruction of the equipment in the Iranian nuclear enrichment plant in Natanz [189]. In 2014, another cyber-attack record was well documented with the case study of German Steel Mill, causing failures in multiple components of the system [190]. The cybersecurity accidents happen in different scales and areas, even from the lower levels of inter-operable manufacturing management such as Overall Equipment Effectiveness (OEE) to cross-site attacks on different targets and types [191, 192, 193], which is summarized on the table 5.1.

There is an increasing recorded cases related to cyber threads, which is also reported by the Cisco 2018 Annual Cybersecurity reports, referenced by Lezzi et al [195], 38 percent attacks have expanded from IT to operational technologies while 31 percent of organizations have reported cyber-attacks on those technologies. Although cybersecurity is perceived as a priority, the majority of companies have not been well prepared yet, which is further evidenced by the report in 2017 on McKinsey&Company [196], indicating that “75 percent of experts, but only 16 percent say their company is well prepared.”. One of the reasons that limit the ability to deal with the cybersecurity threads is that those threads associated with the scales and objectives have been evolved and adapted in different ways [192, 195, 197], summarized in the Table 5.2:

- Intellectual property: Some threads target only some security attributes and do not intend to disrupt physical processes.
- Physical sabotage: Some threads try to cause significant damage to system equipment and assets.
- Denial of service: Some threads take advantage of internet-connected products, leading to production stoppage or denying intended services.
- Compliance violation: some threads may cause environmental damage and even some threads endanger human life and safety.

The complexity to deal with the cyber threads has also significantly increased by considering the impact of them on different affected entities in the context of inter-operable manufacturing systems [192, 193], as summarized in the Figure 5.3. Firstly, the physical targets of those threads

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Incident report	Attack type	Attack mechanism	Affected entity	Consequences	Affected Performance
CMS malicious void, 2017 [193]	Malicious Cross-site request (cyber)	User compromise	Manufactured parts (physical)	Defective parts Risk of injury	Quality
Iranian Nuclear Centrifuges 2010 [189]	Worm (cyber)	Malware installation	Actuator (physical)	Machine breakage	Availability
German Mill, 2008 [190]	Human social interaction (physical)	Privilege compromise	Privilege compromise	Machine failures	Availability
Japanese Automobile Manufacturer, 2008 [194]	Virus (cyber)	Denial of service	Localhost (cyber)	Machine failures	Availability
American nuclear power plant, 2003 [193]	Worm (cyber)	Denial of service	Machine (physical)	System shutdown	Availability

Table 5.1: Background of reported cybersecurity attacks

include connected-manufacturing physical components (sensors, actuators, machines, finished and non-finished products) and humans. While sensors and actuators play a critical role for the controlled manufacturing processes, the loss in data integrity due to cyber attacks can cause machine malfunctions or system failures leading to the possible physical sabotage. Humans also are a target victim as well, such as assembly workers working next to robots can be endangered when hackers can send malicious control to actuators. Secondly, the information targets can be operating systems that can be formulated with attacks in some unforeseen vulnerabilities in these systems while the network, local-host, website, cloud services and applications are also potentially targeted.

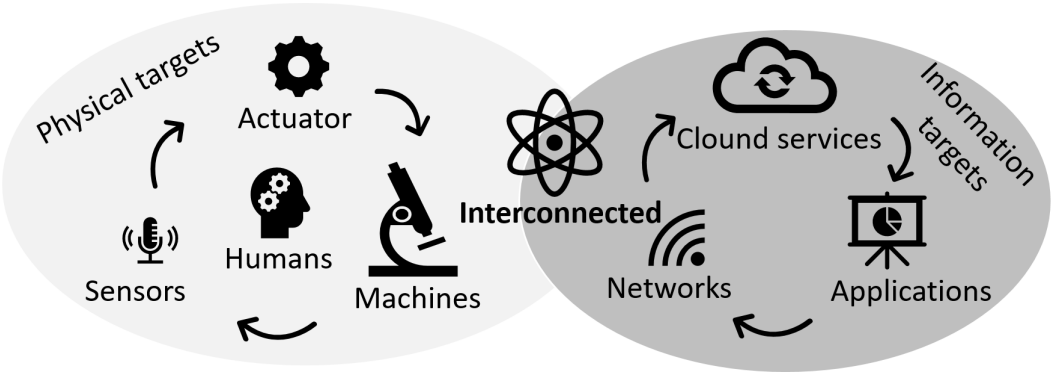


Figure 5.3: Cybers attacks on effected entities in inter-operable systems

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Group	Common threats
Intellectual property	Transfer data from and to unauthorized devices
	Escalation of privilege
	Data tampering, spoofing or man-in-the-middle attacks
	Eavesdropping or data interface
	Insider attacks and unwitting behavior
	Insider attacks and unwitting behavior
	Malware, worms and viruses infection (in accidentally or intentionally way)
Denial of service	Denial of service attack using massive traffic
	Repudiation attacks
	Jamming, Collision, Fake Location Injection, Sybil, Node Replication, Wormhole, Sinkhole, False Routing Information, and Selective Forwarding
	Abnormal operations induction by using abnormal Distributed Network Protocol (DNP3) function code
	Zero-day attacks
Compliance violation	Phishing attacks
	Social engineering attacks
Physical sabotage	Physical destructions

Table 5.2: Common cyber threads and their intentional objectives

Risk management

The cyber risks are considered as the level of impact on organizational operations, including mission, functions, image, or reputation, organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring [195]. To encounter and minimize the risks, risk management starts with the identification of threats (internal and external) and vulnerabilities of a system, and the safeguarding and security measures to those threats, including both technical and organizational solutions. The starting point for risk management is an analysis of the risks, which is commonly based on the risk impact and probability of occurrence showing the likelihood that a risk will occur. Based on this assessment, the risk map is formed and the following responses for risk management should be implemented as the table 3 [198]:

Risk characteristics	Low probability	High probability
Low Impact	Risk acceptance	Risk mitigation by taking preventive actions for risk reduction and risk curing (treatment)
High Impact	Risk transfer that usually implies risk insurance activities, outsourcing	Risk avoidance by eliminating exposure to the risk, or even the resources related to that risk

Table 5.3: Risk assessment matrix

Several cybersecurity standards and framework have been established. NIST Internal Report

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

(NISTIR) 8183 provides the Cybersecurity Framework implementation details developed for the manufacturing environment in which risk assessment and risk management strategies were provided [199]. The risk assessment detailed by NISTIR 8183 is ranked in levels, including low, moderate and high risks associated with corresponding actions of identification, prioritization and dissemination risk assessment results among relevant stakeholders while risk management strategy defines risk tolerance, establish a risk management process to ensure the risk tolerance for manufacturing systems. Additionally, European Cyber Security Organization summarizes a state-of-the-art syllabus on existing cybersecurity standards and certification schemes applied on different levels and sectors [200]. For smart manufacturing, the reference can be taken on ISA/IEC 62433 (Security for Industrial Automation and Control Systems) and IACS Cybersecurity Certification Framework, or NIST SP 800-82 (Guide to Industrial Control Systems Security).

Human factors

Human roles are considered as potential sources of risk, even if computers or other autonomous systems close the control loops, humans could still perform complementary and monitoring roles in smart manufacturing, such as data inputs, intermittent modifications, and parameter controls, among others [201, 202, 203, 204, 205]. In the context of cybersecurity, two types of people are the major targets: customers and workers [192]. The customers here can be end-users or external stakeholders across the supply chain in which they can be exposed to cyber attacks, such as losing personal information, and even endangered by defective or malfunction products due to cyber-physical attack. The workers are more concerned on safety and environmental risks in work space in which the cyber attacker may take over the control on manufacturing process or emission treatment and even manipulate endangering modifications on the user interface to cause human safety risks [206].

According to National Agency for the Security of Information Systems (ANSSI), the cybersecurity analysis on system vulnerabilities need take into account human factors, beyond to hardware, software, procedures, in order to implement measures to limit and be in a position to safeguard the continuity of core business functions to an acceptable extent [200]. The standards and the guidelines need give some directions on staff awareness and training on cyber-risks and emphasize that security has to consider human issue as equally as technical one [198, 207, 208]. However, despite the awareness and training programs, users continue to become victims of social engineering methods: they regularly fall for phishing attacks. The human factors in security management at the plant level and on shop floors have not been addressed yet and the issue of this will grow with the increase in attacks [208]. That is also a potential future research area in the context of human-centered cybersecurity.

5.3 Solutions

Integrating Cyber security into manufacturing

The massive amount of raw data available from factory floor creates opportunities to add intelligence to the manufacturing process. McKinsey Report indicated that manufacturing has the largest amount of data stored annually[209]. Meanwhile, the volume, velocity, and variety of the generated data have provided industries with a noticeable challenge: how to extract actionable information from this big data. To address this issue, machine health analytics need to be effectively integrated with factory operation analytics (Figure 5.4). In addition, technologies such as Hadoop and Spark have been proposed to provide more powerful computational powers through cloud-based and distributed computing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

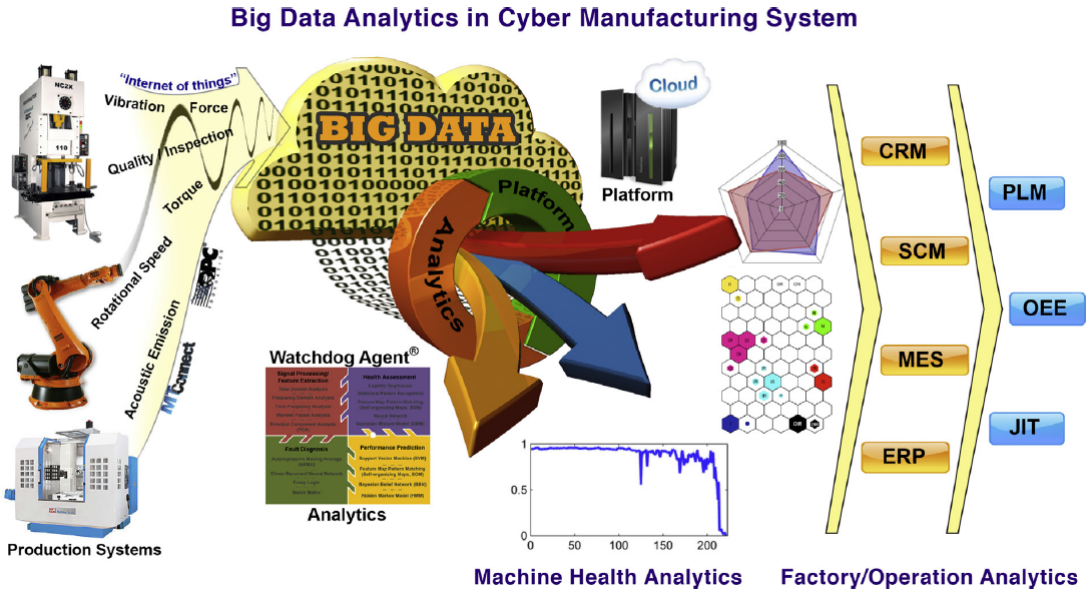


Figure 5.4: Big data analytics in cyber manufacturing systems, reprinted from [210]

Cyber security is one of the major hurdles in implementing cyber manufacturing as it is critical to have resilient capabilities for connected machines and systems in a cloud environment. One approach is to develop a smart cyber-machine interface (CPI) with a time-machine monitoring function so a virtual testing algorithm can be implemented for any control action as input to the physical machine or system. Cyber attacks can be categorized as general and targeted, the latter of which has increased in recent years. Targeted attacks use customized payloads and have higher impacts on the targeted enterprise. Cyber security requires incorporating intelligence-driven approaches instead of solely depending on tools. For example, Defence in Depth is a traditional cyber security strategy that relies on various tools in each layer to ensure protection against attacks. An intelligence-driven use of Defence in Depth[211] requires continuous monitoring of the network and proactively response to potential attacks. Such strategy results in continuous improvement of the defence-intelligence. In addition, developing strict guidelines, technical standards, and educating personnel to avoid social engineering attacks also play a significant role in supporting cyber-security efforts[212]

Block-chain in cyber security

As a cryptographic-based distributed ledger, blockchain technology [213][214] enables trusted transactions among untrusted participants in the network. Since the introduction of the first Bitcoin blockchain in 2008 [215], various blockchain systems, such as Ethereum and Hyperledger Fabric [216], have emerged with public and private accessibility outside of existing fiat currencies and electronic voucher systems. Recently, blockchain technology has also been the subject of an increasing number of scientific researches [217][218][219] [220], and has raised significant interest among researchers, developers, and industry practitioners due to its unique trust and security characteristics.

The opportunities to improve the security of IoT are clearly abundant when consideration is given to the fact that almost half of all published cyber security blockchain applications concerned IoT. This may be because of the proliferation of IoT in our homes, military and healthcare, and the ever increasing demand for IoT solutions. Similarly, demand for solutions to security threats to IoT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

may be spawned from well covered media reports of attacks orchestrated through exploiting such devices. The latest studies suggested that the most security-focused blockchain applications were as follows:

- **IoT:** Authentication of devices to the network and authentication of end users to the devices.
- **Data storage and sharing:** Ensuring that data stored in the cloud remains resistant to unauthorized change, that hash lists allow for searching of data which can be maintained and stored securely, and that data exchanged can be verified as being the same from dispatch to receipt.
- **Network security:** Due to increasingly utilized visualized machines,software-defined networks and the use of containers for application deployment, blockchain allows for authentication critical data to be stored in a decentralized and robust manner
- **Private user data:** Including end user settings for wearable Bluetooth devices and the protection of personal identifiable information being exchanged with other parties

Based on the most security-focused blockchain applications identified so far, blockchain was applied to improve cyber security in IoT, data storage and sharing, network security, private user data, navigation and utility of World Wide Web :

IoT: Main private blockchains (such as Hyperledger Fabric) are applied to implement permitted access control for devices (nodes) in the network [221][222] to securely track data management and prevent any malicious access. In another class of work, blockchain is used to improve the security of firmware deployment through peer-to-peer propagation of updates [223][224][225] to provide IoT device identification, authentication and seamless secure data transfer.

Data storage and sharing: Both public and private distributed ledgers are used to eliminate a single source of failure within a given storage ecosystem, protecting its data from tampering. That is, blockchain helps to ensure that data stored in the cloud remains resistant to unauthorized changes, hash lists allow for searching of data that can be maintained and stored securely, and data exchanged can be verified as being the same from dispatch to receipt [226][227][228].

Network security: The majority of works in this category use blockchains to improve Software Defined Networks (SDNs) and use containers for authentication critical data to be stored in a decentralized and robust manner [229]. In such works,blockchain enabled architecture of SDN controllers using a cluster structure is used. The architecture uses public and private blockchains for P2P communication between nodes in the network and SDN controllers to make the blockchain appropriate for addressing network security issues.

Private user data: Comparing with other categories, the application of blockchain for improving data privacy has been less discussed in the literature. The reason could be due to the irreversibility nature of blockchain (everybody has a copy of the ledger), which makes it hard to be used for privacy purposes, particularly in data protection. In current approaches, typical user device preferences are encrypted and stored on the blockchain to be retrieved only by that user. Also, they explore differences between blockchain PoW and proof-of-credibility consensus mechanisms, where nodes are given a score to determine their credibility dependent on the number of connections to other trusted nodes.[230]

Navigation and utility of the World Wide Web: Blockchain is used to improve the validity of the wireless Internet access points connected to [231], by storing and monitoring the access control data on a local ledger. Also, blockchain is used to help navigating to the correct web page through accurate DNS records, safely utilizing web applications [232], and communicating with others through secure, encrypted methods [233]. To implement these solutions, the idea of

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

consortium blockchain has been used, in which the consensus process is controlled by a pre-selected set of nodes in the network.

5.4 Challenges in cybersecurity

Cyber-attacks have drastically increased since their infancy in the early 1980's with operations such as the suspected 'Logic Bomb' that exploded the Trans-Siberian Pipeline [234]. As the number of attacks grows, their visibility decreases and maliciousness increases (Figure 5.5). Over the past decades, this has been seen in aerospace, control systems, financial systems, and presidential campaign offices Attackers have repeatedly shown that no system is off-limits or out-of-reach. In addition, opportunities for attacks are increasing with the IoT [235], where the number of networked devices is rapidly expanding across every sector, including manufacturing.

While enhanced manufacturing system connectivity provides significant analytical and supply-chain management capabilities, it also opens the door for attacks against cyber-physical components. An attack can alter design files or process parameters (e.g. tool paths) to bring a part out of specification. In addition, this attack could also modify the Quality Control (QC) system to avoid proper quality assessment. Such attacks can disrupt the product/system design process and/or adversely affect a product's design intent, performance, or quality. The results of which could delay a product's launch, ruin equipment, increase warranty costs, or reduce customer trust. More importantly, these attacks pose a risk to human safety for operators and consumers.

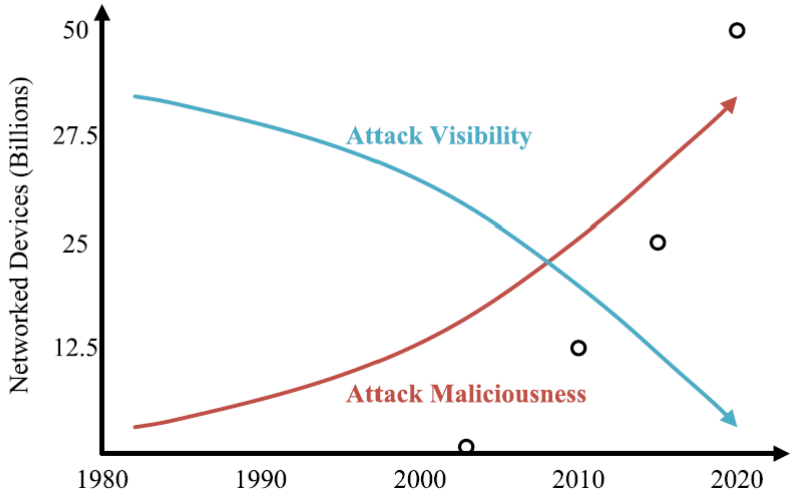


Figure 5.5: Growth of networked devices and cyber-attack visibility and maliciousness trends, reprinted from [236]

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Chapter 6

Conclusions

The aim of this work is to summarize and address key points of the state-of-the-art of interoperability and integration of CPPS in industry 4.0 and their cyber-security requirements. A further research can bring novel approaches by combining different concepts, methodologies, standards and technologies introduced in each section and some of their use cases.

The work includes an alternative definition of interoperability, which considers different levels, types, technologies and standards and the provision of several constraints that should be carried out to achieve a seamless integration of manufacturing processes.

This discussion is extended by identifying an organized collection of information regarding types and levels of interoperability and their respective role in the data transfer and data communication.

Emerging technologies and paradigms in manufacturing like CPPS, cloud manufacturing, smart manufacturing, Internet of Things etc. follow a highly interoperable, hierarchy-free structure. This arises a need for both vertical interoperability between shop-floor automation devices and services as well as horizontal interoperability between enterprises and cloud service platforms. The chapter also explains in detail the emerging technologies like MAS, SOA, Cloud and Edge/Fog for achieving interoperability and what main characteristics, and benefits each of these technologies represent.

Certainly, in the industry 4.0 era, the concept of digitalization implies high data transfer from heterogeneous devices and from different locations and resources. It is, therefore, imperative to take into account the role of cybersecurity and data protection as well as the provision of necessary strategies that provide enough data safety.

Thanks to the wider perspective of this document by establishing a strong baseline of concepts and approaches it is tried to generalise current solutions to make them applicable and simply available in different levels making future manufacturing systems and enterprises, researchers and industrial stakeholders as main beneficiaries.

Undoubtedly, the strong research effort in various manufacturing fields e.g. cybersecurity, emerging technologies, standards and protocols have left a lot of opportunities to achieve high interoperable CPPS. There are, however, some challenges that still have to be taken into account and that certainly can contribute to improve the performance of smart manufacturing. To finalize, this work presents a short survey of the state-of-the-art of various domains identified as possible challenges and considerations. Briefly summarized conclusions related to the areas investigated are presented in the following Table.

Table 6.1: Summarized challenges

State-of-the-art topic	Identified approach	Identified challenge and requirement
	Technological development	Majority of agent-based state of the art approaches for distributed manufacturing are based on the JADE framework, which implies the division between the real time control and the agent abstraction (normally made over the network). This division might cause real time constraints since the rapid response of devices and machines can be dependent on the network latency. In device interoperability, the real time communication is imperative because field devices need to respond rapidly, robust and in an agile way, especially in presence of dynamic events. Therefore, an improved tool and technological development for agent-deviced interoperability approaches is required and can reduce potential communication risks.
Agent based technology	Standarized methodologies	Standardized methodologies: A strong effort has been developed to standardize the utilization of agent technologies and to create patterns for agent communication in industry 4.0 by [59] specially in the hierarchy and axis layers in the rami 4.0 reference architecture. However, a standardization of agent technologies in the production life cycle of the rami 4.0 reference architecture is still missing. This axis provides standards and norms of how to manage the life cycle of a product. In terms of interoperability and integration this standardization will ease the implementation of agent technologies for industrial stakeholders inside and outside the value chain.
	Security and trust	Since a high interoperability is expected in future manufacturing environments, these tools should also enable high security and safety. This is very important considering current security polices and very high risks in industrial scenarios. Future protocols and standards should allow the integration of agent technologies with legacy systems and its connection to the network, higher scalability and more efficient discovery mechanisms that allow a more agile communication

Continued on next page

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Table 6.1 – continued from previous page

State-of-the-art topic	Identified approach	Identified challenge and requirement
Cloud based technology	Challenges in cloud manufacturing	The major challenges in cloud technology is related to data security and transport. Major research is being carried out to develop framework for security and privacy concerns of manufacturers. Demand uncertainity, variability in manufacturing systems,unwillingness to adapt, legal concerns and unavailability of infrastructure are major challenges.
Fog computing	Challenges in fog computing	Major challenges revolve around processing capability of fog nodes.
	Reference architecture models	There is still a need to validate the reference architecture models that have been in the conceptual phase with lack of documented implementation of SOA-based cases [26], which is also recognized by the Table 4.2 showing some case studies in need of implementation validation.
Service oriented technology	Human-centered design	Service interfaces should be designed and easily understood by humans and can be used by reasoning systems to understand and functionality for added-values [237]. This is linked to the SOA principle of business values.
	Granularity	It is often difficult to define the fittest granularity for a service to adapt to a specific application, which is also one of key points to distinguish the differences in approaching SOA-based applications developed by different companies [237, 238]. The service granularity indicates the overall quantity of functionality encapsulated by the service. For instance, an application releases a request to retrieve a complex machine status will have a coarser level of granularity than another application that simply needs status of an engine on the same machine. This is also linked to the SOA principle of business values.
Cyber security	Human factors	The human factors in security management at the plant level and on shop floors have not been addressed yet and the issue of this will grow with the increase in attacks. That is also a potential future research area in the context of human-centered cybersecurity

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

Bibliography

[1] A. Lechler and A. Verl, "Software defined manufacturing extends cloud-based control," in *International Manufacturing Science and Engineering Conference*, vol. 50749. American Society of Mechanical Engineers, 2017, p. V003T04A025.

[2] L. Monostori, B. Kádár, T. Bauernhansl, S. Kondoh, S. Kumara, G. Reinhart, O. Sauer, G. Schuh, W. Sihn, and K. Ueda, "Cyber-physical systems in manufacturing," *Cirp Annals*, vol. 65, no. 2, pp. 621–641, 2016.

[3] O. Cardin, "Classification of cyber-physical production systems applications: Proposition of an analysis framework," *Computers in Industry*, vol. 104, pp. 11–21, 2019.

[4] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *Journal of industrial information integration*, vol. 6, pp. 1–10, 2017.

[5] P. Leitão, A. W. Colombo, and S. Karnouskos, "Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges," *Computers in industry*, vol. 81, pp. 11–25, 2016.

[6] A. Kusiak, "Smart manufacturing," *International Journal of Production Research*, vol. 56, no. 1-2, pp. 508–517, 2018. [Online]. Available: https://doi.org/10.1080/00207543.2017.1351644

[7] Q. Li, Q. Tang, I. Chan, H. Wei, Y. Pu, H. Jiang, J. Li, and J. Zhou, "Smart manufacturing standardization: Architectures, reference models and standards framework," *Computers in Industry*, vol. 101, no. July, pp. 91–106, 2018. [Online]. Available: https://doi.org/10.1016/j.compind.2018.06.005

[8] M. Hankel and B. Rexroth, "The reference architectural model industrie 4.0 (rami 4.0)," *ZVEI, April*, vol. 410, 2015.

[9] V. Alcácer and V. Cruz-Machado, "Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing Systems," *Engineering Science and Technology, an International Journal*, vol. 22, no. 3, pp. 899–919, 2019.

[10] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[11] O. Givehchi, H. Trsek, and J. Jasperneite, "Cloud computing for industrial automation systems — a comprehensive overview," in *2013 IEEE 18th Conference on Emerging Technologies Factory Automation (ETFA)*, 2013, pp. 1–4.

[12] Q. Qi and F. Tao, "A smart manufacturing service system based on edge computing, fog computing, and cloud computing," *IEEE Access*, vol. 7, pp. 86 769–86 777, 2019.

[13] F. Tao, Q. Qi, A. Liu, and A. Kusiak, "Data-driven smart manufacturing," *Journal of Manufacturing Systems*, vol. 48, pp. 157–169, 2018.

[14] G. Shao, S. Shin, and S. Jain, "Data analytics using simulation for smart manufacturing," in *Proceedings of the Winter Simulation Conference 2014*, 2014, pp. 2192–2203.

[15] B. Rodič, "Industry 4.0 and the new simulation modelling paradigm," *Organizacija*, vol. 50, no. 3, pp. 193–207, 2017.

[16] T. Masood and J. Egger, "Augmented reality in support of industry 4.0—implementation challenges and success factors," *Robotics and Computer-Integrated Manufacturing*, vol. 58, pp. 181–195, 2019.

[17] S. A. Tofail, E. P. Koumoulos, A. Bandyopadhyay, S. Bose, L. O'Donoghue, and C. Charitidis, "Additive manufacturing: scientific and technological challenges, market uptake and opportunities," *Materials today*, vol. 21, no. 1, pp. 22–37, 2018.

[18] S. Nahavandi, "Trusted Autonomy Between Humans and Robots: Toward Human-on-the-Loop in Robotics and Autonomous Systems," *IEEE Systems, Man, and Cybernetics Magazine*, vol. 3, no. 1, pp. 10–17, 2017.

[19] T. Samad and D. Cofer, "Autonomy in automation: trends, technologies, tools," *Computer Aided Chemical Engineering*, vol. 9, no. C, pp. 1–13, 1 2001.

[20] M. Gil, M. Albert, J. Fons, and V. Pelechano, "Designing human-in-the-loop autonomous Cyber-Physical Systems," *International Journal of Human Computer Studies*, vol. 130, no. June 2018, pp. 21–39, 2019. [Online]. Available: https://doi.org/10.1016/j.ijhcs.2019.04.006

[21] M. A. Goodrich and A. C. Schultz, "Human-robot interaction: A survey," *Foundations and Trends in Human-Computer Interaction*, vol. 1, no. 3, pp. 203–275, 2007.

[22] U. P. D. Ani, H. He, and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective," *Journal of Cyber Security Technology*, vol. 1, no. 1, pp. 32–74, 2017.

[23] Anonymous, "Ieee standard computer dictionary: a compilation of ieee standard computer glossaries," *IEEE Press*, 1990.

[24] H. Van Der Veer and A. Wiles, "Achieving Technical Interoperability: the ETSI Approach," *European Telecommunications Standards Institute*, no. 3, p. 29, 2008. [Online]. Available: https://portal.etsi.org/CTI/Downloads/ETSIApproach/IOP whitepaper Edition 3 final.pdf

[25] R. A. Rojas and E. Rauch, "From a literature review to a conceptual framework of enablers for smart manufacturing control," *International Journal of Advanced Manufacturing Technology*, vol. 104, no. 1-4, pp. 517–533, 2019.

[26] A. Zeid, S. Sundaram, M. Moghaddam, S. Kamarthi, and T. Marion, "Interoperability in smart manufacturing: Research challenges," *Machines*, vol. 7, no. 2, pp. 1–17, 2019.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[27] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in Internet of Things: Taxonomies and Open Challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, 2019.

[28] A. Napoleone, M. Macchi, and A. Pozzetti, "A review on the characteristics of cyber-physical systems for the future smart factories," *Journal of Manufacturing Systems*, vol. 54, no. August 2019, pp. 305–335, 2020. [Online]. Available: https://doi.org/10.1016/j.jmsy.2020.01.007

[29] J. C. Chaplin, O. J. Bakker, L. De Silva, D. Sanderson, E. Kelly, B. Logan, and S. M. Ratchev, "Evolvable assembly systems: A distributed architecture for intelligent manufacturing," *IFAC-PapersOnLine*, vol. 28, no. 3, pp. 2065–2070, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.ifacol.2015.06.393

[30] P. B. J. Leitao, "Modular and Self-organized Conveyor System Using Multi-agent Systems," vol. 11523, pp. 97–109, 2019. [Online]. Available: https://link.springer.com/article/10.1007/s10514-016-9598-5

[31] M. V. Garcia, E. Irisarri, F. Perez, E. Estevez, D. Orive, and M. Marcos, "Plant floor communications integration using a low cost CPPS architecture," *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, vol. 2016-Novem, no. Iec 62541, pp. 2–5, 2016.

[32] M. Mosley, M. Brackett, S. Earley, and D. Henderson, "DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK Guide)," Data Administration Management Association, Tech. Rep., 2009.

[33] T. Bray, J. Paoli, and M. Sperberg-McQueen, "Extensible Markup Language (XML) 1.0 : W3C Recommendation 10-Feb-98," *Language*, 1998.

[34] S. Decker, S. Melnik, F. Van Harmelen, D. Fensel, M. Klein, J. Broekstra, M. Erdmann, and I. Horrocks, "Semantic Web: The roles of XML and RDF," *IEEE Internet Computing*, vol. 4, no. 5, pp. 63–74, 2000.

[35] S. Heiler, "Semantics," *ACM Computing Surveys (CSUR)*, vol. 27, no. 2, pp. 271–273, 1995.

[36] A. Perzylo, J. Grothoff, L. Lucio, M. Weser, S. Malakuti, P. Venet, V. Aravantinos, and T. Deppe, "Capability-based semantic interoperability of manufacturing resources: A BaSys 4.0 perspective," *IFAC-PapersOnLine*, vol. 52, no. 13, pp. 1590–1596, 2019. [Online]. Available: https://doi.org/10.1016/j.ifacol.2019.11.427

[37] H. Panetto and A. Molina, "Enterprise integration and interoperability in manufacturing systems: Trends and issues," *Computers in Industry*, vol. 59, no. 7, pp. 641–646, 2008.

[38] C. Bettini, O. Brdiczka, K. Henricksen, J. Indulska, D. Nicklas, A. Ranganathan, and D. Riboni, "A survey of context modelling and reasoning techniques," *Pervasive and Mobile Computing*, vol. 6, no. 2, pp. 161–180, 2010. [Online]. Available: http://dx.doi.org/10.1016/j.pmcj.2009.06.002

[39] F. Giustozzi, J. Saunier, and C. Zanni-Merk, "Context Modeling for Industry 4.0: An Ontology-Based Proposal," *Procedia Computer Science*, vol. 126, pp. 675–684, 2018. [Online]. Available: https://doi.org/10.1016/j.procs.2018.08.001

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[40] V. R. Sampath Kumar, A. Khamis, S. Fiorini, J. L. Carbonera, A. O. Alarcos, M. Habib, P. Goncalves, L. I. Howard, and J. I. Olszewska, "Ontologies for industry 4.0," *Knowledge Engineering Review*, vol. 34, pp. 1–14, 2019.

[41] M. K. Uddin, J. Puttonen, S. Scholze, A. Dvoryanchikova, and J. L. Martinez Lastra, "Ontology-Dased context-Sensitive computing for FMS optimization," *Assembly Automation*, vol. 32, no. 2, pp. 163–174, 2012.

[42] K. Alexopoulos, S. Makris, V. Xanthakis, K. Sipsas, A. Liapis, and G. Chryssolouris, "Towards a role-centric and context-aware information distribution system for manufacturing," *Procedia CIRP*, vol. 25, no. C, pp. 377–384, 2014.

[43] H. K. Lin, J. A. Harding, and M. Shahbaz, "Manufacturing system engineering ontology for semantic interoperability across extended project teams," *International Journal of Production Research*, vol. 42, no. 24, pp. 5099–5118, 2004.

[44] N. Chungoora and R. I. Young, "Enterprise Interoperability III," *Enterprise Interoperability III*, no. May, pp. 0–12, 2008.

[45] A. P. Sage and W. B. Rouse, *Handbook of systems engineering and management*. John Wiley & Sons, 2014.

[46] D. SPEC, "91345: 2016-04 reference architecture model industrie 4.0 (rami4. 0)," 2019.

[47] S.-W. Lin, B. Murphy, E. Clauer, U. Loewen, R. Neubert, G. Bachmann, M. Pai, and M. Hankel, "Architecture alignment and interoperability: An industrial internet consortium and plattform industrie 4.0 joint whitepaper," *White Paper, Industrial Internet Consortium*, 2017.

[48] M. Moghaddam, M. N. Cadavid, C. R. Kenley, and A. V. Deshmukh, "Reference architectures for smart manufacturing: A critical review," *Journal of manufacturing systems*, vol. 49, pp. 215–225, 2018.

[49] R. B. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, "Nist cloud computing reference architecture," in *2011 IEEE World Congress on Services*. IEEE, 2011, pp. 594–596.

[50] X. V. Wang and X. W. Xu, "Icms: a cloud-based manufacturing system," in *Cloud manufacturing*. Springer, 2013, pp. 1–22.

[51] G. S. Roadmap, "D I N a n d D K E R O A D M A P German Standardization Roadmap Industrie 4.0." [Online]. Available: www.din.de

[52] M. Wooldridge, *An introduction to multiagent systems*. John Wiley & Sons., 2009.

[53] L. M. Camarinha-Matos and W. Vieira, "Intelligent mobile agents in elderly care," *Robotics and Autonomous Systems*, vol. 27, no. 1, pp. 59–75, 1999.

[54] D. Mourtzis and M. Doukas, "Decentralized manufacturing systems review: Challenges and outlook," *Logistics Research*, vol. 5, no. 3-4, pp. 113–121, 2012.

[55] P. Leitão, "Agent-based distributed manufacturing control: A state-of-the-art survey," *Engineering Applications of Artificial Intelligence*, vol. 22, no. 7, pp. 979–991, 2009.

[56] A. Colombo, "Industrial agents: towards collaborative production-auto- mation, -management and -organization," *IEEE Industrial Electronics Society Newsletter*, 2005.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[57] P. Leitão, S. Karnouskos, L. Ribeiro, J. Lee, T. Strasser, and A. W. Colombo, "Smart Agents in Industrial Cyber-Physical Systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1086–1101, 2016.

[58] L. Ribeiro, "Cyber-physical production systems' design challenges," in *IEEE International Symposium on Industrial Electronics*, 2017, pp. 1189–1194. [Online]. Available: https://www.scopus.com

[59] L. A. Cruz Salazar, D. Ryashentseva, A. Luder, and B. Vogel-Heuser, "Cyber-physical production systems architecture based on multi-agent's design pattern—comparison of selected approaches mapping four agent patterns," *International Journal of Advanced Manufacturing Technology*, vol. 105, no. 9, pp. 4005–4034, 2019. [Online]. Available: https://www.scopus.com

[60] P. Leitão, A. W. Colombo, and S. Karnouskos, "Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges," *Computers in Industry*, vol. 81, pp. 11–25, 2016.

[61] A. Colombo, S. Karnouskos, J. Mendes, and P. Leitao, "Industrial Agents in the Era of Service-Oriented Architectures and Cloud-Based Industrial Infrastructures," in *Industrial Agents*. Morgan Kaufmann, 2015, pp. 67–87.

[62] M. Onori, N. Lohse, J. Barata, and C. Hanisch, "The IDEAS project: Plug & produce at shop-floor level," *Assembly Automation*, vol. 32, no. 2, pp. 124–134, 2012.

[63] B. Vogel-Heuser, C. Diedrich, D. Pantförder, and P. Göhner, "Coupling heterogeneous production systems by a multi-agent based cyber-physical production system," *Proceedings - 2014 12th IEEE International Conference on Industrial Informatics, INDIN 2014*, pp. 713–719, 2014.

[64] A. W. Colombo, T. Bangemann, and S. Karnouskos, "IMC-AESOP outcomes: Paving the way to collaborative manufacturing systems," *Proceedings - 2014 12th IEEE International Conference on Industrial Informatics, INDIN 2014*, no. July, pp. 255–260, 2014.

[65] F. Pauker, I. Ayatollahi, and B. Kittl, "Service Orchestration for Flexible Manufacturing Systems using Sequential Functional Charts and OPC UA," *Dubrovnik*, vol. 9, no. September, pp. 9–11, 2015.

[66] S. Azaiez, M. Boc, L. Cudennec, M. Da Silva Simoes, J. Haupert, S. Kchir, X. Klinge, W. Labidi, K. Nahhal, J. Pfrommer, M. Schleipen, C. Schulz, and T. Tortech, "Towards Flexibility in Future Industrial Manufacturing: A Global Framework for Self-organization of Production Cells," *Procedia Computer Science*, vol. 83, no. Ramcom, pp. 1268–1273, 2016.

[67] F. Fraile, R. Sanchis, R. Poler, and A. Ortiz, "Reference models for digital manufacturing platforms," *Applied Sciences (Switzerland)*, vol. 9, no. 20, 2019.

[68] R. A.Dias, I. T. M. Mendonça, and A. Regis, "Integrated Manufacturing Management using Internet of Things," *International Journal of Computer Applications*, vol. 51, no. 11, pp. 20–25, 2012.

[69] H. Demirkan, R. J. Kauffman, J. A. Vayghan, H. G. Fill, D. Karagiannis, and P. P. Maglio, "Service-oriented technology and management: Perspectives on research and practice for the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

coming decade," *Electronic Commerce Research and Applications*, vol. 7, no. 4, pp. 356–376, 2008. [Online]. Available: http://dx.doi.org/10.1016/j.elerap.2008.07.002

[70] S. Hachani, H. Verjus, and L. Gzara, "Service-Oriented Approach for Agile Support," pp. 103–112.

[71] A. J. Redelinghuys, A. H. Basson, and K. Kruger, "A six-layer architecture for the digital twin: a manufacturing case study implementation," *Journal of Intelligent Manufacturing*, vol. 31, no. 6, pp. 1383–1402, 2020. [Online]. Available: https://doi.org/10.1007/s10845-019-01516-6

[72] V. Tountopoulos, E. Kavakli, and R. Sakellariou, "Towards a cloud-based controller for data-driven service orchestration in smart manufacturing," *Proceedings - 2018 6th International Conference on Enterprise Systems, ES 2018*, pp. 96–99, 2018.

[73] X. Ye, T. Y. Park, S. H. Hong, Y. Ding, and A. Xu, "Implementation of a Production-Control System Using Integrated Automation ML and OPC UA," *2018 Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2018 - Proceedings*, no. April, pp. 242–247, 2018.

[74] H. Zhang, Q. Yan, and Z. Wen, "Information modeling for cyber-physical production system based on digital twin and AutomationML," *International Journal of Advanced Manufacturing Technology*, vol. 107, no. 3-4, pp. 1927–1945, 2020.

[75] G. Cândido, J. Barata, A. W. Colombo, and F. Jammes, "SOA in reconfigurable supply chains: A research roadmap," *Engineering Applications of Artificial Intelligence*, vol. 22, no. 6, pp. 939–949, 2009.

[76] Y. Lu and F. Ju, "Smart Manufacturing Systems based on Cyber-physical Manufacturing Services (CPMS)," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 15 883–15 889, 2017.

[77] J. Morgan and G. E. O'Donnell, "Enabling a ubiquitous and cloud manufacturing foundation with field-level service-oriented architecture," *International Journal of Computer Integrated Manufacturing*, vol. 30, no. 4-5, pp. 442–458, 2017.

[78] H. O. Unver, "An ISA-95-based manufacturing intelligence system in support of lean initiatives," *International Journal of Advanced Manufacturing Technology*, vol. 65, no. 5-8, pp. 853–866, 2013.

[79] F. Jammes, H. Smit, J. L. Martinez Lastra, and I. M. Delamer, "Orchestration of service-oriented manufacturing processes," *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, vol. 1 2 VOLS, no. January, pp. 617–624, 2005.

[80] f. . C. i. . . j. . I. n. . . p. . . t. . O. v. . . y. . . Luder, A., Schleipen, M., Schmidt, N., Pfrommer, J., Hensen, R., doi = 0.1109/COASE.2017.8256275.

[81] E. Cardoso Moraes and H. Augusto Lepikson, "Service-oriented framework for oil fields automation," *Applied Mechanics and Materials*, vol. 496-500, pp. 1438–1441, 2014.

[82] C. Legner and R. Heutschi, "SOA adoption in practice-Findings from early SOA implementations," *Proceedings of the 15th European Conference on Information Systems, ECIS 2007*, pp. 1643–1654, 2007.

[83] M. P. Papazoglou and W. J. Van Den Heuvel, "Service oriented architectures: Approaches, technologies and research issues," *VLDB Journal*, vol. 16, no. 3, pp. 389–415, 2007.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[84] J. Bean, *SOA and Web services interface design : principles, techniques, and standards*. Calif. Oxford: Morgan Kaufmann Elsevier Science distributor, 2009.

[85] T. Lojka, M. Bundzel, and I. Zolotová, "Service-oriented architecture and cloud manufacturing," *Acta Polytechnica Hungarica*, vol. 13, no. 6, pp. 25–44, 2016.

[86] A. Ismail and W. Kastner, "Surveying the features of industrial SOAs," *Proceedings of the IEEE International Conference on Industrial Technology*, pp. 1199–1204, 2017.

[87] S. Pakari, E. Kheirkhah, and M. Jalali, "Web Service Discovery Methods and Techniques: A Review," *International Journal of Computer Science, Engineering and Information Technology*, vol. 4, no. 1, pp. 01–14, 2014.

[88] A. Zeid, S. Sundaram, M. Moghaddam, S. Kamarthi, and T. Marion, "Interoperability in smart manufacturing: Research challenges," *Machines*, vol. 7, no. 2, pp. 1–17, 2019.

[89] M. Moghaddam, M. N. Cadavid, C. R. Kenley, and A. V. Deshmukh, "Reference architectures for smart manufacturing: A critical review," *Journal of Manufacturing Systems*, vol. 49, no. September, pp. 215–225, 2018.

[90] C. Tuck and R. Hague, "The pivotal role of rapid manufacturing in the production of cost-effective customised products," *International Journal of Mass Customisation*, 2006.

[91] A. Charro and D. Schaefer, "Cloud Manufacturing as a new type of Product-Service System," *International Journal of Computer Integrated Manufacturing*, vol. 31, no. 10, pp. 1018–1033, 10 2018. [Online]. Available: https://doi.org/10.1080/0951192X.2018.1493228

[92] X. Vincent Wang and X. W. Xu, "An interoperable solution for Cloud manufacturing," *Robotics and Computer-Integrated Manufacturing*, vol. 29, no. 4, pp. 232–247, 2013.

[93] X. Xu, "From cloud computing to cloud manufacturing," *Robotics and Computer-Integrated Manufacturing*, 2012.

[94] D. Tai and F. Xu, "Cloud manufacturing based on cooperative concept of SDN," in *Advanced Materials Research*, 2012.

[95] Z. Jin, "Research on solutions of cloud manufacturing in automotive industry," in *Lecture Notes in Electrical Engineering*, 2013.

[96] F. Tao, Y. Cheng, L. D. Xu, L. Zhang, and B. H. Li, "CCIoT-CMfg: Cloud computing and internet of things-based cloud manufacturing service system," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1435–1442, 2014.

[97] H. Y. Jeong and B. H. Hong, "The cloud manufacturing system in factory automation," *Applied Mechanics and Materials*, vol. 271, no. PART 1, pp. 528–532, 2013.

[98] F. Tao, Y. Cheng, L. Zhang, Y. L. Luo, and L. Ren, "Cloud manufacturing," *Advanced Materials Research*, vol. 201-203, pp. 672–676, 2011.

[99] I. Liu and H. Jiang, "Research on key technologies for design services collaboration in cloud manufacturing," *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2012*, pp. 824–829, 2012.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[100] M. Bohlouli, A. Holland, and M. Fathi, "Knowledge integration of collaborative product design using cloud computing infrastructure," in *IEEE International Conference on Electro Information Technology*, 2011.

[101] A. L. Kuan, U. Rauschecker, M. Meier, R. Muckenhirn, A. Yip, A. Jagadeesan, and J. Corney, "Cloud-based manufacturing-as-a-service environment for customized products," *eChallenges e-2011 Conference Proceedings*, 2011.

[102] A. L. K. Yip, A. P. Jagadeesan, J. R. Corney, Y. Qin, and U. Rauschecker, "A FRONT-END SYSTEM TO SUPPORT CLOUD-BASED MANUFACTURING OF CUSTOMIZED PRODUCTS," in *9th International Conference on Manufacturing Research (ICMR)*, 2011.

[103] P. S. Huang, X. He, J. Gao, L. Deng, A. Acero, and L. Heck, "Learning deep structured semantic models for web search using clickthrough data," in *International Conference on Information and Knowledge Management, Proceedings*, 2013.

[104] F. Jrad, J. Tao, and A. Streit, "SLA based service brokering in intercloud environments," in *CLOSER 2012 - Proceedings of the 2nd International Conference on Cloud Computing and Services Science*, 2012.

[105] F. Xiang and Y. Hu, "Cloud manufacturing resource access system based on Internet of Things," *Applied Mechanics and Materials*, vol. 121-126, pp. 2421–2425, 2012.

[106] L. Zhang, H. Guo, F. Tao, Y. L. Luo, and N. Si, "Flexible management of resource service composition in cloud manufacturing," in *IEEM2010 - IEEE International Conference on Industrial Engineering and Engineering Management*, 2010.

[107] B. Lv, "A multi-view model study for the architecture of cloud manufacturing," in *Proceedings - 2012 3rd International Conference on Digital Manufacturing and Automation, ICDMA 2012*, 2012.

[108] F. Ning, W. Zhou, F. Zhang, Q. Yin, and X. Ni, "The architecture of cloud maufacturing and its key technologies research," in *CCIS2011 - Proceedings: 2011 IEEE International Conference on Cloud Computing and Intelligence Systems*, 2011.

[109] Z. Zhang and P. Zhong, "Key issues for cloud manufacturing platform," *Advanced Materials Research*, vol. 472-475, pp. 2621–2625, 2012.

[110] F. Zhang and H. f. Xue, "Cloud manufacturing-based enterprise platform architecture and implementation," *Applied Mechanics and Materials*, vol. 190-191, pp. 60–63, 2012.

[111] Q. Ai, K. Mo, Y. Wang, and L. Zhao, "Research of product information sharing system based on cloud manufacturing," *Applied Mechanics and Materials*, vol. 248, pp. 533–538, 2013.

[112] Y. Zhang and Y. Jin, "Research on knowledge management for group enterprise in cloud manufacturing," in *Proceedings - 2012 International Conference on Computer Science and Service System, CSSS 2012*, 2012.

[113] X. V. Wang and X. W. Xu, "An interoperable solution for Cloud manufacturing," *Robotics and Computer-Integrated Manufacturing*, 2013.

[114] N. Liu and X. Li, "A resource virtualization mechanism for cloud manufacturing systems," in *Lecture Notes in Business Information Processing*, 2012.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[115] L. Ferreira, G. Putnik, M. Cunha, Z. Putnik, H. Castro, C. Alves, V. Shah, and M. L. R. Varela, "Cloudlet architecture for dashboard in cloud and ubiquitous manufacturing," in *Procedia CIRP*, 2013.

[116] L. Zhang, Y. Luo, F. Tao, B. H. Li, L. Ren, X. Zhang, H. Guo, Y. Cheng, A. Hu, and Y. Liu, "Cloud manufacturing: a new manufacturing paradigm," *Enterprise Information Systems*, 2014.

[117] S. Wang, J. Wan, M. Imran, D. Li, and C. Zhang, "Cloud-based smart manufacturing for personalized candy packing application," *Journal of Supercomputing*, vol. 74, no. 9, pp. 4339–4357, 2018.

[118] D. Wu, J. L. Thames, D. W. Rosen, and D. Schaefer, "Towards a cloud-based design and manufacturing paradigm: Looking backward, looking forward," in *Proceedings of the ASME Design Engineering Technical Conference*, vol. 2, no. PARTS A AND B, 2012, pp. 315–328.

[119] D. Schaefer, J. Lane Thames, R. D. Wellman, D. Wu, and D. W. Rosen, "Distributed collaborative design and manufacture in the cloud-motivation, infrastructure, and education," *Computers in Education Journal*, vol. 22, no. 4, pp. 1–16, 2012.

[120] Y. Cheng, D. Zhao, A. R. Hu, Y. L. Luo, F. Tao, and L. Zhang, "Multi-view models for cost constitution of cloud service in cloud manufacturing system," in *Communications in Computer and Information Science*, vol. 202 CCIS, no. PART 2, 2011, pp. 225–233.

[121] Y. L. Luo, L. Zhang, D. J. He, L. Ren, and F. Tao, "Study on multi-view model for cloud manufacturing," in *Advanced Materials Research*, vol. 201-203, 2011, pp. 685–688.

[122] J. Lartigau, L. Nie, X. Xu, D. Zhan, and T. Mou, "Scheduling methodology for production services in cloud manufacturing," in *Proceedings - 2012 International Joint Conference on Service Sciences, Service Innovation in Emerging Economy: Cross-Disciplinary and Cross-Cultural Perspective, IJCSS 2012*, 2012, pp. 34–39.

[123] Y. Luo, L. Zhang, K. Zhang, and F. Tao, "Research on the knowledge-based multi-dimensional information model of manufacturing capability in CMfg," in *Advanced Materials Research*, vol. 472-475, 2012, pp. 2592–2595.

[124] C. Hu, C. Xu, X. Cao, and J. Fu, "Study of classification and modeling of virtual resources in Cloud Manufacturing," in *Applied Mechanics and Materials*, vol. 121-126, 2012, pp. 2274–2280.

[125] B. Ding, X. Y. Yu, and L. J. Sun, "A cloud-based collaborative manufacturing resource sharing services," *Information Technology Journal*, 2012.

[126] W. Wang and F. Liu, "The research of cloud manufacturing resource discovery mechanism," in *ICCSE 2012 - Proceedings of 2012 7th International Conference on Computer Science and Education*, 2012, pp. 188–191.

[127] H. Guo, L. Zhang, and F. Tao, "A framework for correlation relationship mining of cloud service in cloud manufacturing system," *Advanced Materials Research*, vol. 314-316, pp. 2259–2262, 2011.

[128] C. Li, P. Yang, Y. Shang, C. Hu, and P. Zhu, "Research on cloud manufacturing resource scheduling and performance analysis," *Advanced Science Letters*, vol. 12, pp. 240–243, 2012.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[129] Y. Laili, F. Tao, L. Zhang, and L. Ren, "The optimal allocation model of computing resources in cloud manufacturing system," *Proceedings - 2011 7th International Conference on Natural Computation, ICNC 2011*, vol. 4, pp. 2322–2326, 2011.

[130] L. Wang, "Wise-ShopFloor: An integrated approach for web-based collaborative manufacturing," *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, vol. 38, no. 4, pp. 562–573, 2008.

[131] Y. K. Lu, C. Y. Liu, and B. C. Ju, "Cloud manufacturing collaboration: An initial exploration," in *Proceedings of the 2012 3rd World Congress on Software Engineering, WCSE 2012*, 2012, pp. 163–166.

[132] A. Hu and L. Zhang, "MSEC2013-1133 LIFECYCLE MANAGEMENT OF KNOWLEDGE IN A CLOUD MANUFACTURING," pp. 1–9, 2017.

[133] F. Tao, Y. Cheng, L. D. Xu, L. Zhang, and B. H. Li, "CCIoT-CMfg: Cloud computing and internet of things-based cloud manufacturing service system," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1435–1442, 2014.

[134] O. F. Valilai and M. Houshmand, "A collaborative and integrated platform to support distributed manufacturing system using a service-oriented approach based on cloud computing paradigm," *Robotics and Computer-Integrated Manufacturing*, 2013.

[135] W. Jiang, J. Ma, X. Zhang, and H. Xie, "Research on cloud manufacturing resource integrating service modeling based on cloud-Agent," in *ICSESS 2012 - Proceedings of 2012 IEEE 3rd International Conference on Software Engineering and Service Science*, 2012.

[136] X. Y. Yang and W. J. Li, "Research and application of the management and control platform oriented the cloud manufacturing services," in *2011 International Conference on System Science, Engineering Design and Manufacturing Informatization, ICSEM 2011*, 2011.

[137] L. Ferreira, G. Putnik, M. M. Cruz-Cunha, Z. Putnik, H. Castro, C. Alves, and V. Shah, "Dashboard services for pragmatics-based interoperability in cloud and ubiquitous manufacturing," *International Journal of Web Portals*, 2014.

[138] U. Rauschecker and M. Stöhr, "Using manufacturing service descriptions for flexible integration of production facilities to manufacturing clouds," in *2012 18th International Conference on Engineering, Technology and Innovation, ICE 2012 - Conference Proceedings*, 2012.

[139] I. Sittón and S. Rodríguez, "Pattern extraction for the design of predictive models in industry 4.0," in *Advances in Intelligent Systems and Computing*, 2017.

[140] O. García, P. Chamoso, J. Prieto, S. Rodríguez, and F. De La Prieta, "A serious game to reduce consumption in smart buildings," in *Communications in Computer and Information Science*, 2017.

[141] P. CHAMOSO and F. DE LA PRIETA, "Swarm-Based Smart City Platform: A Traffic Application," *ADCAIJ: ADVANCES IN DISTRIBUTED COMPUTING AND ARTIFICIAL INTELLIGENCE JOURNAL*, 2015.

[142] A. R. Biswas and R. Giaffreda, "IoT and cloud convergence: Opportunities and challenges," in *2014 IEEE World Forum on Internet of Things, WF-IoT 2014*, 2014.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[143] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[144] F. Ganz, D. Puschmann, P. Barnaghi, and F. Carrez, "A Practical Evaluation of Information Processing and Abstraction Techniques for the Internet of Things," *IEEE Internet of Things Journal*, 2015.

[145] R. S. Alonso, D. I. Tapia, J. Bajo, García, J. F. De Paz, and J. M. Corchado, "Implementing a hardware-embedded reactive agents platform based on a service-oriented architecture over heterogeneous wireless sensor networks," *Ad Hoc Networks*, 2013.

[146] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Cla, "Middleware for internet of things: A survey," *IEEE Internet of Things Journal*, 2016.

[147] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, 2014.

[148] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[149] W. Shi and S. Dustdar, "The Promise of Edge Computing," *Computer*, 2016.

[150] M. Satyanarayanan, "The emergence of edge computing," *Computer*, 2017.

[151] M. Isaja, J. Soldatos, and V. Gezer, "Combining Edge Computing and Blockchains for Flexibility and Performance in Industrial Automation," 2017.

[152] N. K. Giang, S. Kim, D. Kim, M. Jung, and W. Kastner, "Extending the EPCIS with building automation systems: A new information system for the internet of things," in *Proceedings - 2014 8th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2014*, 2014.

[153] H. F. Atlam, A. Alenezi, R. Khalid Hussein, and G. B. Wills, "Validation of an Adaptive Risk-based Access Control Model for the Internet of Things," *International Journal of Computer Network and Information Security*, 2018.

[154] Y. Ai, M. Peng, and K. Zhang, "Edge computing technologies for Internet of Things: a primer," *Digital Communications and Networks*, 2018.

[155] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *MCC'12 - Proceedings of the 1st ACM Mobile Cloud Computing Workshop*, 2012.

[156] F. Haouari, R. Faraj, and J. M. Alja'Am, "Fog Computing Potentials, Applications, and Challenges," in *2018 International Conference on Computer and Applications, ICCA 2018*, 2018.

[157] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," 2016.

[158] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, "Developing an adaptive risk-based access control model for the internet of things," in *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017*, 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[159] Z. Wen, R. Yang, P. Garraghan, T. Lin, J. Xu, and M. Rovatsos, "Fog orchestration for internet of things services," *IEEE Internet Computing*, 2017.

[160] M. Verma, N. Bhardwaj, and A. K. Yadav, "Real Time Efficient Scheduling Algorithm for Load Balancing in Fog Computing Environment," *International Journal of Information Technology and Computer Science*, 2016.

[161] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog computing: Platform and applications," in *Proceedings - 3rd Workshop on Hot Topics in Web Systems and Technologies, HotWeb 2015*, 2016.

[162] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," *Computer Communication Review*, vol. 44, no. 5, pp. 27–32, 2014.

[163] Y. Shi, G. Ding, H. Wang, H. Eduardo Roman, and S. Lu, "The fog computing service for healthcare," in *2015 2nd International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare, Ubi-HealthTech 2015*, 2015.

[164] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: Fundamental, network applications, and research challenges," *IEEE Communications Surveys and Tutorials*, 2018.

[165] M. Aazam and E. N. Huh, "Fog computing and smart gateway based communication for cloud of things," in *Proceedings - 2014 International Conference on Future Internet of Things and Cloud, FiCloud 2014*, 2014.

[166] ——, "Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT," in *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 2015.

[167] H. F. Atlam, R. J. Walters, and G. B. Wills, "Fog computing and the internet of things: A review," 2018.

[168] Y. Liu, J. E. Fieldsend, and G. Min, "A framework of fog computing: Architecture, challenges, and optimization," *IEEE Access*, 2017.

[169] M. Aazam, P. P. Hung, and E. N. Huh, "Smart gateway based communication for cloud of things," in *IEEE ISSNIP 2014 - 2014 IEEE 9th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Conference Proceedings*, 2014.

[170] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Koldehofe, "Mobile fog: A programming model for large-scale applications on the internet of things," in *MCC 2013 - Proceedings of the 2nd, 2013 ACM SIGCOMM Workshop on Mobile Cloud Computing*, 2013.

[171] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: A platform for internet of things and analytics," *Studies in Computational Intelligence*, 2014.

[172] I. Stojmenovic and S. Wen, "The Fog computing paradigm: Scenarios and security issues," in *2014 Federated Conference on Computer Science and Information Systems, FedCSIS 2014*, 2014.

[173] K. P.Saharan and A. Kumar, "Fog in Comparison to Cloud: A Survey," *International Journal of Computer Applications*, 2015.

[174] N. Peter, "Fog computing and its real time applications," *textit{International Journal of Emerging Technology and Advanced Engineering*}, 2015.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[175] S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing," 2015.

[176] V. Gazis, A. Leonardi, K. Mathioudakis, K. Sasloglou, P. Kikiras, and R. Sudhaakar, "Components of fog computing in an industrial internet of things context," in *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking - Workshops, SECON Workshops 2015*, 2015.

[177] A. V. Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh, and R. Buyya, "Fog Computing: Principles, architectures, and applications," in *Internet of Things: Principles and Paradigms*, 2016.

[178] O. Skarlat, S. Schulte, M. Borkowski, and P. Leitner, "Resource provisioning for IoT services in the fog," in *Proceedings - 2016 IEEE 9th International Conference on Service-Oriented Computing and Applications, SOCA 2016*, 2016.

[179] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, "Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures," *IEEE Transactions on Vehicular Technology*, 2016.

[180] M. Sookhak, F. R. Yu, Y. He, H. Talebian, N. Sohrabi Safa, N. Zhao, M. K. Khan, and N. Kumar, "Fog Vehicular Computing: Augmentation of Fog Computing Using Vehicular Cloud Computing," *IEEE Vehicular Technology Magazine*, 2017.

[181] A. Yousefpour, G. Ishigaki, and J. P. Jue, "Fog Computing: Towards Minimizing Delay in the Internet of Things," in *Proceedings - 2017 IEEE 1st International Conference on Edge Computing, EDGE 2017*, 2017.

[182] C. Puliafito, E. Mingozzi, and G. Anastasi, "Fog Computing for the Internet of Mobile Things: Issues and Challenges," in *2017 IEEE International Conference on Smart Computing, SMARTCOMP 2017*, 2017.

[183] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog Computing: A taxonomy, survey and future directions," in *Internet of Things*, 2018.

[184] S. S. Adhatarao, M. Arumaithurai, and X. Fu, "FOGG: A Fog Computing Based Gateway to Integrate Sensor Networks to Internet," in *Proceedings of the 29th International Teletraffic Congress, ITC 2017*, 2017.

[185] M. Billinghurst, A. Clark, and G. Lee, "A survey of augmented reality," 2014.

[186] J. K. Zao, T. T. Gan, C. K. You, S. J. R. Mendez, C. E. Chung, Y. T. Wang, T. Mullen, and T. P. Jung, "Augmented brain computer interaction based on fog computing and linked data," in *Proceedings - 2014 International Conference on Intelligent Environments, IE 2014*, 2014.

[187] D. Schatz, R. Bashroush, and J. Wall, "Towards a more representative definition of cyber security," *Journal of Digital Forensics, Security and Law*, vol. 12, no. 2, pp. 53–74, 2017.

[188] Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems," *Journal of Manufacturing Systems*, vol. 43, pp. 339–351, 2017.

[189] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, nov 2011, pp. 4490–4494. [Online]. Available: http://ieeexplore.ieee.org/document/6120048/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[190] R. M. Lee, M. J. Assante, and T. Conway, "ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper - German Steel Mill Cyber Attack," ICS Defense Use Case (DUC), Tech. Rep.

[191] A. Zarreh, H. D. Wan, Y. Lee, C. Saygin, and R. A. Janahi, *Procedia Manufacturing*, no. 2019, pp. 532–539.

[192] M. Wu and Y. B. Moon, "Taxonomy for secure cybermanufacturing systems," *ASME International Mechanical Engineering Congress and Exposition, Proceedings (IMECE)*, vol. 2, pp. 1–10, 2018.

[193] M. Wu and Y. Moon, "Taxonomy of Cross-Domain Attacks on CyberManufacturing System," *Procedia Computer Science*, vol. 114, pp. 367–374, 2017. [Online]. Available: https://doi.org/10.1016/j.procs.2017.09.050

[194] W. Yakowicz, "Honda Factory Shuts Down After WannaCry Virus Infects Computers." [Online]. Available: https://www.inc.com/will-yakowicz/wannacry-virus-hits-honda-factory-japan.html

[195] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework," *Computers in Industry*, vol. 103, pp. 97–110, 2018.

[196] H. Bauer, G. Scherf, and V. von der Tann, "Six Ways CEOs Can Promote Cybersecurity in the IoT Age," *McKinsey&Company*, 2017.

[197] H. Orojloo and M. A. Azgomi, "A method for evaluating the consequence propagation of security attacks in cyber–physical systems," *Future Generation Computer Systems*, vol. 67, pp. 57–71, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.future.2016.07.016

[198] T. V. Šibalija, "Cyber-security in digital manufacturing: assessment and testing," *2nd International Conference on "Modern Methods of Testing and Evaluation in Science"*, no. December, 2015.

[199] K. Stouffer, T. Zimmerman, C. Tang, J. Lubell, J. Cichonski, and J. McCarthy, "Cybersecurity framework manufacturing profile," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep., sep 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

[200] ECSO, "State-of-the-Art Syllabus Overview of existing cybersecurity standards and certification schemes," no. June, pp. 1–228, 2017. [Online]. Available: https://www.ecs-org.eu/documents/publications/5a31129ea8e97.pdf

[201] N. H. Carreras Guzman, M. Wied, I. Kozine, and M. A. Lundteigen, "Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis," *Systems Engineering*, vol. 23, no. 2, pp. 189–210, 2020.

[202] S. Nahavandi, "Trusted Autonomy Between Humans and Robots: Toward Human-on-the-Loop in Robotics and Autonomous Systems," *IEEE Systems, Man, and Cybernetics Magazine*, vol. 3, no. 1, pp. 10–17, jan 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7815473/

[203] F. Santoni de Sio and J. van den Hoven, "Meaningful Human Control over Autonomous Systems: A Philosophical Account," *Frontiers in Robotics and AI*, vol. 5, feb 2018. [Online]. Available: http://journal.frontiersin.org/article/10.3389/frobt.2018.00015/full

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[204] M. Gil, M. Albert, J. Fons, and V. Pelechano, "Designing human-in-the-loop autonomous Cyber-Physical Systems," *International Journal of Human-Computer Studies*, vol. 130, pp. 21–39, oct 2019. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1071581919300461

[205] S. Malatji, Masike; Marnewick, Annlize; von Solms, "The Impact of Artificial Intelligence on the Human Aspects of Information and Cybersecurity," no. Haisa, pp. 158–169, 2018.

[206] D. Quarta, M. Pogliani, M. Polino, F. Maggi, A. M. Zanchettin, and S. Zanero, "An Experimental Security Analysis of an Industrial Robot Controller," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, may 2017, pp. 268–286. [Online]. Available: http://ieeexplore.ieee.org/document/7958582/

[207] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *Journal of Manufacturing Systems*, vol. 47, no. February, pp. 93–106, 2018.

[208] R. Torten, C. Reaiche, and S. Boyle, "The impact of security awarness on information technology professionals' behavior," *Computers and Security*, vol. 79, pp. 68–79, 2018. [Online]. Available: https://doi.org/10.1016/j.cose.2018.08.007

[209] B. B. J. B. R. D. C. R. A. H. B. James Manyika, Michael Chui, "Big data: The next frontier for innovation, competition, and productivity," *McKinsey Global Institute May*, vol. 156, pp. 339–351, 2011.

[210] J. Lee, B. Bagheri, and C. Jin, "Introduction to cyber manufacturing," *Manufacturing Letters*, vol. 8, pp. 11–15, 2016.

[211] C. systems security program, "Recommended practice:improving industrial control systems cybersecurity with defense-in-depth strategies," *Control systems security program*, vol. 156, 2009.

[212] J. Butt, "A conceptual framework to support digital transformation in manufacturing using an integrated business process management approach," *Designs*, vol. 4, no. 3, p. 17, 2020.

[213] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *computer*, vol. 50, no. 9, pp. 18–28, 2017.

[214] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*. IEEE, 2017, pp. 557–564.

[215] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[216] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[217] L. Kan, Y. Wei, A. H. Muhammad, W. Siyuan, G. Linchao, and H. Kai, "A multiple blockchains architecture on inter-blockchain communication," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. IEEE, 2018, pp. 139–145.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[218] D. Miller, "Blockchain and the internet of things in the industrial sector," *IT professional*, vol. 20, no. 3, pp. 15–18, 2018.

[219] M. Samaniego, U. Jamsrandorj, and R. Deters, "Blockchain as a service for iot," in *2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2016, pp. 433–436.

[220] J. Fiaidhi, S. Mohammed, and S. Mohammed, "Edi with blockchain as an enabler for extreme automation," *IT Professional*, vol. 20, no. 4, pp. 66–72, 2018.

[221] O. J. A. Pinno, A. R. A. Gregio, and L. C. De Bona, "Controlchain: Blockchain as a central enabler for access control authorizations in the iot," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.

[222] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE, 2017, pp. 618–623.

[223] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.

[224] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[225] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018.

[226] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in *2016 {USENIX} annual technical conference ({USENIX}{ATC} 16)*, 2016, pp. 181–194.

[227] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," in *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*. IEEE, 2017, pp. 117–121.

[228] K.-K. R. Choo, "Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks?" in *Handbook of digital currency*. Elsevier, 2015, pp. 283–307.

[229] S. R. Basnet and S. Shakya, "Bss: Blockchain security over software defined network," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*. IEEE, 2017, pp. 720–725.

[230] D. Fu and L. Fang, "Blockchain-based trusted computing in social network," in *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*. IEEE, 2016, pp. 19–22.

[231] Y. Niu, L. Wei, C. Zhang, J. Liu, and Y. Fang, "An anonymous and accountable authentication scheme for wi-fi hotspot access with the bitcoin blockchain," in *2017 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE, 2017, pp. 1–6.

[232] L. Xu, L. Chen, N. Shah, Z. Gao, Y. Lu, and W. Shi, "Dl-bac: Distributed ledger based access control for web applications," in *Proceedings of the 26th International Conference on World Wide Web Companion*, 2017, pp. 1445–1450.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078

[233] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli, "Iotchain: A blockchain security architecture for the internet of things," in *2018 IEEE wireless communications and networking conference (WCNC)*. IEEE, 2018, pp. 1–6.

[234] J. Rost and R. L. Glass, *The dark side of software engineering: evil on computing projects*. John Wiley & Sons, 2011.

[235] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," *CISCO white paper*, vol. 1, no. 2011, pp. 1–11, 2011.

[236] L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-physical security challenges in manufacturing systems," *Manufacturing Letters*, vol. 2, no. 2, pp. 74–77, 2014.

[237] G. Cândido, J. Barata, A. W. Colombo, and F. Jammes, "SOA in reconfigurable supply chains: A research roadmap," *Engineering Applications of Artificial Intelligence*, vol. 22, no. 6, pp. 939–949, 9 2009.

[238] C. Legner and R. Heutschi, "SOA adoption in practice-Findings from early SOA implementations," *Proceedings of the 15th European Conference on Information Systems, ECIS 2007*, pp. 1643–1654, 2007.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant No. 814078