UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

TIBA: A trustworthy interoperability architecture for Industry 4.0

Ana Paula Allian

Tese de Doutorado do Programa de Pós-Graduação em Ciências de Computação e Matemática Computacional (PPG-CCMC)

ICMC USP SÃO CARLOS

Ana Paula Allian

TIBA: A trustworthy interoperability architecture for Industry 4.0

Thesis submitted to the Instituto de Ciências Matemáticas e de Computação – ICMC-USP – in accordance with the requirements of the Computer and Mathematical Sciences Graduate Program, for the degree of Doctor in Science. *FINAL VERSION*

Concentration Area: Computer Science and Computational Mathematics

Advisor: Prof. Dr. Elisa Yumi Nakagawa

USP – São Carlos
March 2021

Ana Paula Allian

TIBA: Uma arquitetura de interoperabilidade confiável para Indústria 4.0

Tese apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Doutora em Ciências – Ciências de Computação e Matemática Computacional. *VERSÃO REVISADA*

Área de Concentração: Ciências de Computação e Matemática Computacional

Orientadora: Prof. Dr. Elisa Yumi Nakagawa

USP – São Carlos
Março de 2021

ACKNOWLEDGEMENTS

This thesis is not only the result of the last five years of work, but yes was a consequence of cumulative learning, experiences, and collaborations, on both personal and professional levels. I remember a friend when I was 12 years old. He asked me what I would like to be in the future. At that time I had no idea and replied that I would like to be a successful person. He asked me - "are there many successful people in your family?" - I answered - "As far as I know, no". He said - "So, be the first one!". His words made me realize I had a long journey ahead. I am glad I have met many extraordinary people who guided me to be who I am now. So, I am thankful to all those wonderful people who were and still are part of my life. I thank God for guiding me and giving me strength and hope through all these years. I thank my family, my mom Odete, my brothers Ju and Gui for being supportive and giving words of strength. I thank all my school friends, who gave me the first words of motivation, and all the other colleagues from school and from university who made part of my academic growth. Special thanks go to my great friends from USP Bruno, Pedro, Leo, Dió, MLydia, and many other great friends from LABES, who I will never forget. I thank all my professors from primary and high school who helped me shape who I am. I thank the professors from my bachelor's, master's, and doctorate degrees, who showed me the tools for me to start learning by myself. I am deeply grateful to Prof. Elisa for all the "good tanoshimis". For believing in me and accepting to oriented me during this journey. For being a person who has brought many possibilities in my life. Thank you so much for the great moments shared and for the good vibes! I thank all professionals and friends from Fraunhofer, in special Dr. Pablo Antonino, Prof. Dr. Dieter Rombach, Christian, Frank, Tagline, Zai, Alex, Thomas, Markus, Yasmin, and many other colleagues who support me during my stay in Kaiserslautern. In special, I want to thank Sonnhild for being my German mon during my staying in Kaiserslautern. I also have to give many thanks to Aisha and Florian for being my first great friends in KL. I want to thank Bea and her family for being my family here in Germany "Muchas Gracias! Dankeschön!". I am grateful to my best friends, in special I want to thank Vlad for being my inspiration and motivation for resilience and persistence. Joca for the great words of motivation. Gil, Ota, Ze Elias, Xandy, Alex, Paulo, Rogerio, Renato, and Evilin for the great moments of fun and support during this phase of my life. Results obtained with this thesis were possible to the financial support from the Brazilian funding agencies FAPESP (Research Support Foundation of the State of São Paulo) through the Grants No: 2016/05919-0, 2018/20882-1, and CAPES (Coordination for higher Education Staff Development).

LISTS OF ACRONYMS

ABAC	Attribute-Based Access Control
ACL	Access Control Lists
ATHENA	Advanced Technologies for Interoperability of Heterogeneous Enterprise Networks and their Applications
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CNBC	Consumer News and Business Channel
CPS	Cyber-Physical Systems
CPPS	Cyber-Physical Production Systems
CRM	Customer Relationship Management
EI	Enterprise Integration
ERP	Enterprise Resource Planning
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens
IESE	Institute for Experimental Software Engineering
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IIRA	Industrial Internet Reference Architecture
IIS	Industrial Internet Systems
IoT	Internet of Things
MaaS	Manufacturing-as-a-Service
MES	Manufacturing Execution System
NIF	National Interoperability Framework
PaaS	Production-as-a-Service
PDCS	Process Distributed Control System
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
RAMI 4.0	Reference Architectural Model Industrie 4.0

RBAC	Access Rules, or coverage by a Role-Based Access Control
RBAC-ABAC	Role-Based Access Control and Attribute-Based Access Control
SAML	Security Assertion Markup Language
SCADA	Supervisory Control and Data Acquisition
SLR	Systematic Literature Review
SoS	Systems-of-Systems
SQuaRE	Systems and software Quality Requirements and Evaluation
TIBA	Trustworthy Interoperability Architecture
VAB	Virtual Automation Bus
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie (German Electrical and Electronic Manufacturers' Association)

RESUMO

ALLIAN, A. P. **TIBA: Uma arquitetura de interoperabilidade confiável para Indústria 4.0**. 2021. 160 p. Tese (Doutorado em Ciências – Ciências de Computação e Matemática Computacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2021.

A Indústria 4.0 tem chamado a atenção de empresas ao alavancar fábricas inteligentes interconectadas e complexos processos de fabricação. A busca por uma interoperabilidade confiável entre diversas entidades heterogêneas no contexto da Indústria 4.0 é um grande desafio; por isso, diversas initiavas para padronizar a interoperabilidade têm sido implementadas com objetivo de padronizar e adaptar diferentes soluções. No entanto, as empresas interessadas no Industry 4.0 não têm deparado com orientações sobre quais soluções ou requisitos devem ser considerados para arquitetar sistemas para a Industria 4.0 e garantir uma interoperabilidade confiável. Este trabalho contribui com uma arquitetura de interoperabilidade confiável para a Indústria 4.0 (TIBA), combinando blockchain com soluções tradicionais de interoperabilidade. A primeira etapa constituiu da identificação dos principais desafios em relação à interoperabilidade em projetos reais da Industria 4.0. Em seguida, projetamos um conjunto de drivers arquiteturais combinando tais desafios com aspectos de qualidade extraídos da literatura por meio de uma revisão sistemática. Refinamos esses drivers ao com especialistas da indústria 40 por meio de pesquisas online. Posteriormente definimos soluções para os drivers arquiteturais e conduzimos uma pesquisa com especialistas da Indústria 4.0 por meio de entrevistas. As respostas dos especialistas foram analisadas com estudos qualitativos baseado em Grounded-theory. O projeto do TIBA leva em consideração a tecnologia blockchain combinada com sistemas tradicionais que, juntos, cobrem as principais preocupações relacionadas a uma interoperabilidade confiável. Para avaliar o TIBA, nós o instanciamos em um cenário real da Indústria 4.0, observando como uma empresa de manufatura pode conceder contratos automaticamente a fim de incorporar capacidades de empresas externas em seu próprio sistema de produção. Cada etapa deste cenário foi cuidadosamente projetada de acordo com os drivers arquiteturais e representada por meio de visões arquiteturais. TIBA pode apoiar o projeto para desenolver soluções de interoperabilidade confiável, fornecendo drivers arquiteturais e soluções arquiteturais. TIBA compreende do primeiro conjunto de decisões arquiteturais relacionadas à combinação de blockchain com tecnologias tradicionais e pode contribuir para a realização de projetos da Indústria 4.0.

Palavras-chave: Interoperabilidade, Arquitetura, Confiabilidade, Indústria 4.0.

ABSTRACT

ALLIAN, A. P. **TIBA: A trustworthy interoperability architecture for Industry 4.0**. 2021. 160 p. Tese (Doutorado em Ciências – Ciências de Computação e Matemática Computacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2021.

Industry 4.0 has called the attention of companies by leading to highly networked smart factories and leveraging the complex manufacturing processes. The achievement of trustworthy interoperability among several heterogeneous entities and also companies is still a challenge; hence, research, standardization initiatives, and adaptation of solutions from other areas were already conducted. However, companies interested in Industry 4.0 do not have direction about what solutions or concerns/requirements should be considered to architect Industry 4.0 systems that assure trustworthy interoperability. This work contributes with a Trustworthy Interoperability Architecture (TIBA) for Industry 4.0, by combining blockchain with traditional solutions for interoperability. We firstly identified the main challenges regarding interoperability in real-world Industry 4.0 projects. Following, we designed a set of architecture drivers combining such challenges with quality aspects extracted through a systematic literature review. We refined these drivers through a survey with experts from Industry 4.0, and we defined the main architecture solution through the conduction of interviews with experts from Industry 4.0. The design of TIBA takes into account blockchain technology combined with traditional technologies used in Industry 4.0 that together cover the main concerns related to trustworthy interoperability. To evaluate TIBA, we instantiated it in a real-world scenario of Industry 4.0 and observed how a manufacturing company can automatically award contracts to incorporate capacities of outside companies into its production system. TIBA can support the design of a trustworthy interoperability solution by providing architecture drivers and architectural solutions. TIBA comprises the first set of architectural decisions regarding the combination of blockchain with traditional technologies and could contribute to realizing Industry 4.0 projects.

Keywords: Interoperability, Trustworthy, Architecture, Industry 4.0.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

ABAC	Attribute Based Control
ACL	Access Control Lists
ATHENA	Advanced Technologies for Interoperability of Heterogeneous Enterprise Networks and their Applications
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CNBC	Consumer News and Business Channel
CPPS	Cyber-Physical Production Systems
CPS	Cyber-Physical Systems
CRM	Customer Relationship Management
EI	Enterprise Integration
ERP	Enterprise Resource Planning
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens
IESE	Fraunhofer Institute for Experimental Software Engineering
IIC	Industrial Internet Consortium
IIOT	Industrial Internet of Things
IIRA	Industrial Internet Reference Architecture
IIS	Industrial Internet Systems
IoT	Internet-of-Things
Maas	Manufacturing as a service
MES	Manufacturing Execution Systems
NIF	National Interoperability Framework
PaaS	Production-as-a-Service
PDCS	Process Distributed Control Systems
PKI	Public Key Infrastructure
PLC	Programmable Logic Controllers
RAMI 4.0	Reference Architectural Model Industrie 4.0
RBAC	Access Rules, or coverage by a Role-Based Access Control
RBAC-ABAC	Role-Based Access Control and Attribute-Based Access Control

SAML	Security Assertion Markup Language
SCADA	Supervisory Control and Data Acquisition
SLR	Systematic Literature Review
SoS	Systems-of-Systems
SQuaRE	Systems and software Quality Requirements and Evaluation
TIBA	Trustworthy Interoperability Architecture
VAB	Virtual Automation Bus
ZVEI	German Electrical and Electronic Manufacturers' Association

CONTENTS

CHAPTER

1

INTRODUCTION

"Interoperability comes
at the speed of trust"

The Forcare

1.1 Context

Industry 4.0 has been proclaimed as the fourth industrial revolution and aims to completely transform the manufacturing processes towards to be faster and more efficient as well as to discover new business opportunities (ANTONINO *et al.*, 2019; HEADAYETULLAH; PRADHAN, 2010). Industry 4.0 implies several interconnected virtual and physical entities within smart factories, such as software systems, Cyber-Physical Systems (CPS), computer network, equipment (like robots, machines, Internet-of-Things (IoT) devices, and Programmable Logic Controllers (PLC)), and also processes and services (XU; XU; LI, 2018). Also, Industry 4.0 usually involves many companies, such as producers, suppliers, vendors, transportation companies, distribution centers, and retailers, through complex supply chain networks. In this scenario, the interoperability among all these entities (i.e., virtual/physical entities within smart factories and also companies) is not only crucial to the success of Industry 4.0 but also a big challenge. According to Ponemon Institute[1], more than 90% of industries faced at least one major malicious attack in the past two years, including in systems that adopt IP-based connectivity as Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and PLC. Besides that, Garnet IT[2] states communication is one of the most vulnerable targets in the fourth industrial revolution.

[1] <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-the-iiot-attack-surface-threats-and-security-solutions>

[2] <https://www.rambus.com/iot/industrial-iot/>

Interoperability is the ability of two or more different information systems, applications, or devices to connect in a trustworthy and coordinated agreed manner, across and within organizational borders to exchange data towards mutually common goals (BASS; CLEMENTS; KAZMAN, 2012; EIF, 2017; TOGAF, 2018). Interoperability encompasses a shared understanding and agreement with expectations of data exchanged. It is considered a quality attribute of systems incorporating the reliability, security, and trustworthiness of information (GRIDWISE, 2008). Additionally, it is also a major architecture concern of many software systems, including Systems-of-Systems (SoS), Industry 4.0, and IoT, for becoming strategically globally competitive.

Systems interoperate successfully as long as the trustworthiness and reliability of data involved are sufficiently guaranteed (HEADAYETULLAH; PRADHAN, 2010). Considering the large-scale and number of systems and organizations involved, the importance of trusting in the information and means to communicate becomes essential not only for the protection of fundamental rights but also for the effectiveness of interoperability as an information surveillance tool (LI; PING, 2009). The main benefits of promoting trustworthy interoperability are:

- *"Interoperability comes at the speed of trust"* (FORECARE, 2018). Trust in the information being exchange increase security, data integrity, and reliability, resulting in more productivity across a range of organizations and bringing new ways in which business can operate (HEADAYETULLAH; PRADHAN, 2010).

- Strategic and tactical goals shared among businesses. Trustworthy communication enables alignment of organizations goals and the understanding of their mutual business process (GRIDWISE, 2008).

- Support evolution and decision-making regarding the information available. Trust in communication add more value for the companies and organizations, enabling them to identify opportunities to evolve their business (GRILO; JARDIM-GONCALVES, 2010).

- High level of trust in the interoperability increase company reputation. There can be no business without trust and, for this reason, there is a major shift of big organizations concerned about the reliability of data being exchanged. (SARTOR, 2006).

The potential for companies to guarantee trustworthy interoperability raises concerns about data privacy, confidentiality, security, and the conflicting interest to spontaneously cooperate into the adoption of a common communication infrastructure, even with the benefits standards may bring. The problem becomes even more challenging when each of these systems and organizations is heterogeneous, independent, and must guarantee trust considering not just technical aspects of interoperability, but also semantic, organizational, and legal. The challenge related to enabling trust in interoperability is a matter widely discussed in the Software Engi-

neering community and also by the social and economic business society (UM; LEE; CHOI, 2016).

The hyper-connected nature of the current digital world brings a large scale collection of data from many sources, including sensors and devices. This imposes the risks of users to unanticipated consume inaccurate information, causing irreparable damage for their business (UM; LEE; CHOI, 2016). These have increased the debate around trust considerations related to data, and some of the main concerns are (SARTOR, 2006) *i) Privacy and transparency* challenges regarding how the Industry 4.0 companies are protecting the more vulnerable data; *ii) Ethical concerns* on how information has been used by business and the way companies deal with intellectual property rights, and *iii) Fraud protection* regarding information being exchanged.

Privacy and transparency of information have become predominant issues in the context of Industry 4.0. Privacy of data imposed by smart things, services, business, and personal information requires awareness of data protection (ZIEGELDORF; GARCÍA-MORCHÓN; WEHRLE, 2014). The definition of privacy in this work takes the idea of data self-determination by enabling the companies and employees to protect sensitive information and assure they have control of it (ZIEGELDORF; GARCÍA-MORCHÓN; WEHRLE, 2014; Sadeghi; Wachsmann; Waidner, 2015). Transparency about what information will be shared and with whom is another crucial concern of industry 4.0 (Castelluccia *et al.*, 2018). On one hand, transparency provides confidence to companies and demonstrate they are acting with responsibility. On the other hand, full transparency can compromise the security of Industry 4.0 and make them attractive targets for cyber attacks (Sadeghi; Wachsmann; Waidner, 2015). Finding and maintaining a sustainable balance to protect both privacy and transparency of data represents a significant challenge in the context of the new industrial era (Castelluccia *et al.*, 2018).

Ethics is the principle of right and wrong that people use to make a choice to guide their behaviors (KIZZA, 2013). In the context of Industry 4.0, information is distributed on a very large scale and integrated digitally unleashing new concerns about ethics regarding the protection of intellectual property (MARTIN, 2015). Identify and define the owner of data retrieved by sensors, devices connected to Industry 4.0, or the product being made with the participation of many partners might results in many conflicts of interests (ALLHOFF; HENSCHKE, 2018). Intellectual property must be subject to a variety of protections in Industry 4.0, including a statutory grant that protects developers rights from having their work copied for another purpose, and patent registration to grant the owner an exclusive monopoly of ideas (KIZZA, 2013).

The current increasingly connected world of Industry 4.0 has introduced an additional issue for business, the risk of fraud in the information being exchanged by "trusted" parties (DYCK; MORSE; ZINGALES, 2014). Fraudsters can employ several tactics to steal important information from a business or even propagate fake data. Fraud is an expensive problem for business, and can cause a cost of 16 billion dollars for consumers according to the Consumer

News and Business Channel (CNBC)[3]. For this reason, organizations usually rely on internal and external audit reviews system to mitigate the risk of fraud in their data (BURNABY; HOWE; MUEHLMANN, 2011).

With the increasing need to exchange data in the context of Industry 4.0, the responsibility to keep information safe and trustworthy is not only from employees or organizational parties. The responsibility must be also shared through the software systems, sensors, and devices connected to the network.

Establishing trust interoperability in Industry 4.0 represents a primary security milestone to have reliable systems communicating and exchanging data. It aims to create a relationship based on trustworthiness between all industrial parties. Thus, each participant within the network must interoperate only with other trusted parties, increasing the reliability of the information being exchanged. The lack of trust in data communication results in uncertainties about the outcome of others' actions, failures in projects, an increase of costs, unsafe and insecure industrial scenarios, and a negative impact to work performance and reputation of companies involved.

There is also some initiatives and solutions to deal with trustworthy interoperability in Industry 4.0, including trust end-to-end communication protocol for Cyber-Physical Production Systems (CPPS) (Bicaku *et al.*, 2017), trust access control (KJERSGAARD; ERIKSENA; HARLAMOVA, 2018; KJERSGAARD; ERIKSENA, 2018), trustworthy communication among gateways and physical devices (Fraile *et al.*, 2018), middleware solution based on blockchain to promote trust in the integration of resources and services (Mohamed; Al-Jaroodi, 2019), and solutions related to trustworthy contracts to support privacy and security (AL-ALI *et al.*, 2018b). Although these and other many punctual solutions can promote trust in the interoperability in Industry 4.0, covering only some aspects is not enough for companies to avoid disruptions and breaches in the production lines (AL-ALI *et al.*, 2018b; Bicaku *et al.*, 2017; KJERSGAARD; ERIKSENA; HARLAMOVA, 2018) and, therefore, a set of complementary aspects should be jointly considered.

In particular, in the context of this work, *trustworthy interoperability in Industry 4.0* is understood as the ability to exchange data in a trusted way within the Industry 4.0 ecosystem (which involves diverse virtual and physical entities of a smart factory and also several companies). Besides that, based on other works that discuss trustworthy interoperability in Industry 4.0 (JUNGO, 2015; HEADAYETULLAH; PRADHAN, 2010; LI; PING, 2009; ALLIAN, 2019), this interoperability can be also understood as the balance among quality aspects (e.g., data privacy and transparency, ethical concerns, and data protection) in the communication among known entities connected in a transparent and coordinated infrastructure, allowing the data exchange according to predefined rules for achieving common goals.

[3] https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html

1.2 Problem and motivation

In the strongly dynamic context of Industry 4.0, the increasing automation and geographically distributed industrial ecosystems are raising concerns related to trustworthy interoperability of data, things, and services undertaken by fine-grained (humans, machines, robots, sensors) to coarse-grained decentralized entities (enterprises, business). This infrastructure relies on many intermediaries, which increases the risk of non-authorized access to data and intrusions in the production process, affecting different areas, such as modification of operation process, interruption in the manufacturing process, sabotage and manipulation of data and services causing injury or even loss of life (Bicaku *et al.*, 2017).

Current solutions are focused on specific concerns related to trust, such as security and privacy of data (Bicaku *et al.*, 2017; KJERSGAARD; ERIKSENA; HARLAMOVA, 2018; KJERSGAARD; ERIKSENA, 2018; Fraile *et al.*, 2018; AL-ALI *et al.*, 2018b), but the trust gap in current solution is exponentially expanding unnecessary burden to always trust in intermediaries to control data. At the same time, blockchain has been widely considered as new promising technology to solve trust concerns in the interoperability of systems by mainly reducing or avoiding the need for intermediaries (Christidis; Devetsikiotis, 2016; Wang *et al.*, 2018). In turn, blockchain is a distributed database of transactions used to share and replicate data and synchronized across all blockchain partners (PERERA *et al.*, 2020). Commonly associated with cryptocurrencies, e.g., Bitcoin (NAKAMOTO, 2009), in recent years, blockchain have been applied across a wide variety of industry sectors, including healthcare (Wang *et al.*, 2018), financial (PAZAITIS; FILIPPI; KOSTAKIS, 2017), automotive (Yang *et al.*, 2019), Internet of Things (Christidis; Devetsikiotis, 2016), and government sectors (EUBLOCKCHAIN, 2018). Blockchain has also increasingly gained space in Industry 4.0 projects as a solution that could assure trust (Anjum; Sporny; Sill, 2017; HAWLITSCHEK; NOTHEISEN; TEUBNER, 2018; Yang *et al.*, 2019), security (Fernandez-Carames; Fraga-Lamas, 2019; LIN *et al.*, 2018), transparency (Ahram *et al.*, 2017; Golosova; Romanovs, 2018), and reliability of data (Mohamed; Al-Jaroodi, 2019; Tama *et al.*, 2017). The Industry 4.0 community has believed blockchain could provide the so necessary infrastructure to promote trust, but there is no guidance on how blockchain could be combined with Industry 4.0 solutions to assure such trustworthy interoperability.

1.3 Objectives

Therefore, to deal with the unreliable current Industry 4.0 scenarios, there is the need to investigate whether blockchain can really assure trustworthy interoperability in Industry 4.0 and propose means to enable such trustworthy interoperability at architecture level. Thus, the main objective of this work is to propose a Trustworthy Interoperability Architecture (TIBA). TIBA provides guidelines for designing services that combine concepts of blockchain with traditional interoperability solutions. TIBA encompasses: i) the main architecture drivers centered on

compatibility (referred to as Compatibility of Data and Services in this work), Reliability (Availability of Physical Devices and Data Availability), Security (Authentication to the System, Data Access Control, Data Privacy to Protect Sensitive Information, Traceability and Auditability of Data) (ISO/IEC, 2011). Besides, ii) architecture solutions for these drivers that are adequate for a wide range of Industry 4.0 contexts; iii) architecture views that represent the elements, interactions, and flow of messages among each element from the architecture; iv) instantiation of TIBA in the context of Production-as-a-Service (PaaS) business model. The intention of TIBA is:

- To promote trust and support the delivery of services by fostering cross-border and cross-sectoral interoperability in Industry 4.0.
- To guide organizations in their work to provide trust data and services for different businesses, partners and people;
- To complement and tie together the various organizations and partners at the same level trust in the interoperability of Industry 4.0.

This doctoral project also intends to consolidate the research collaboration among the ICMC/USP and Fraunhofer Institute for Experimental Software Engineering (IESE), Germany. This institution has contributed to the architecting industrial software-intensive systems that meet quality standards by carrying out joint research projects with industrial partners and other research institutes, combining academic know-how with industrial practice.

1.4 Research methodology

The development of this project follows the design science in information systems and software engineering research (WIERINGA, 2014; HEVNER *et al.*, 2004). This guideline proposes a systematic way to build an artifact (i.e., methods, techniques, notations, and algorithms used in software systems) that improves something for stakeholders and empirically investigate the performance of such artifact in a context (i.e., design, development, maintenance, and use), as illustrated in Figure 1. The evaluation of the artifacts is a continuing process in design science and it encompasses the Design Cycle with constant, relevant, and rigor feedback from the real world (i.e. Environment) and from knowledge questions (i.e. Knowledge Base) (HEVNER *et al.*, 2004; WIERINGA, 2014). The artifact produced as a result of our project is an enterprise architecture based on blockchain technology. These results are later evaluated using interviews, surveys, case studies, and refined based on the evaluation results.

The research and design process can be divided into three major stages:

1. **Investigation of the Literature**: identification of the existing problem, related works, environment and available resources about trust in interoperability of Industry 4.0;

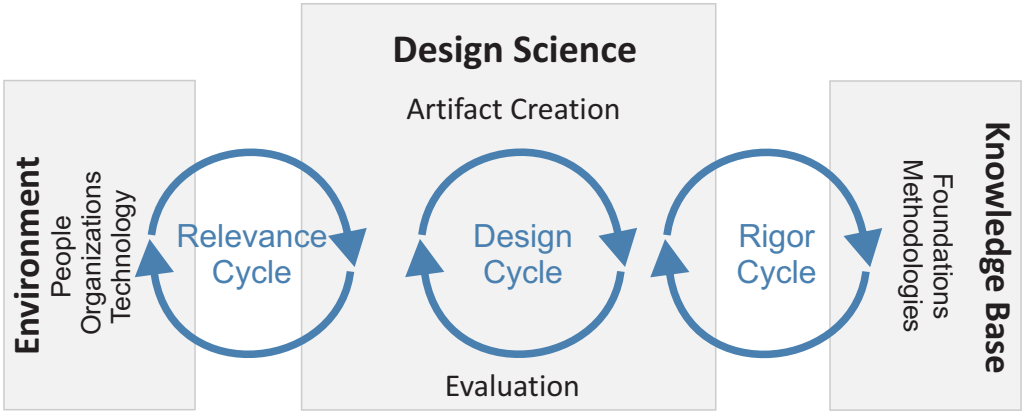

Figure 1 – Design science research

2. **Development of the Project**: the establishment of the architecture drivers; definition of architecture solutions; and designing and modeling the architecture; and

3. **Evaluation of the Project**: execution of surveys, interviews, and instantiation of the architecture based on a real-world Industry 4.0 scenario for evaluating the feasibility and effectiveness of TIBA.

1.4.1 Investigation of the literature

To systematize the definition of TIBA, we first observed the main challenges related to trust in the interoperability in Industry 4.0 in the context of BaSys 4.0 project, the German reference project for Industry 4.0[4], whose consortium complies with several research institutions and companies, such as Bosch, a German multinational company for engineering and electronics solutions; Kuka, a German company for automation solutions; Fortiss GMBH, Software-intensive systems and services research institute; SYSGO and Kontron, a company related to critical application and security solutions; SMS Group, the leading global partner for the metallurgical industry in Germany; ITQ, independent engineering, and consulting firm; ABB, a multinational in the areas of robotics, energy, heavy electrical equipment, and automation technology. To complement the evidence collected from this observation, we also conducted a Systematic Literature Review (SLR) (KITCHENHAM; CHARTERS, 2007) to gather the main quality aspects related to trust in Industry 4.0.

1.4.2 Development of the project

The establishment of TIBA was divided into four activities:

1. **Establishment of the architecture drivers:** Results from the observations of real-world Industry 4.0 projects in the context of BaSys 4.0[5] and results of the SLR guided us in

[4] https://www.basys40.de/
[5] <https://www.iese.fraunhofer.de/en/innovation_trends/industrie40.html>

the first definition of the architecture drivers for promoting trustworthy interoperability in Industry 4.0. Seven architectural drivers for promoting trustworthy interoperability in Industry 4.0 were defined based on results from the observations of real-world Industry 4.0 projects in the context of BaSys 4.0[6] and results of the SLR. The seven architecture drivers were centered on security (cf. Authentication to the System, Data Access Control, Data Privacy to Protect Sensitive Information, Traceability and Auditability of Data, Availability of Data, Availability of Physical Devices, and Compatibility of Data and Services.

2. **Definition of architecture solutions:** Seven directions for architecture solutions based on experts of Industry 4.0, such as project managers, engineers, and IT analysts, to solve the architecture drivers were defined. This is not about models documenting the solution, but rather about claims that can be further represented with any model-driven approaches or more formal representations.

3. **Designing and modeling the architecture:** This activity is related to document architecture solution decisions in architecture views. To systematize the design of TIBA, we followed the modeling profile from the C4 model, which proposes four levels of abstraction to represent the architecture: i) context, ii) containers, iii) components, and iv) code (Vazquez-Ingelmo; Garcia-Holgado; Garcia-Penalvo, 2020; LEANPUB, 2017). The motivation for adopting the C4 Model is the opportunity to translate the architecture drivers previously defined, which encompass quality attributes, functional requirements, and constraints into a technical view, creating the overall structure of the system. Besides that, it is also about communicating the views to the stakeholders and systems involved (Vazquez-Ingelmo; Garcia-Holgado; Garcia-Penalvo, 2020; LEANPUB, 2017).

4. **Instantiation of TIBA:** TIBA was instantiated considering a real-world Industry 4.0 project. This instantiation is used to define the design specification of the architecture and serves as solution pattern for the conception of modern production plants.

1.4.3 Evaluation of the project

When conducting research, it is crucial to make sure the entire research process is set up and performed rigorously and validly (WIERINGA, 2014). In this project, different types of evaluation were performed. Surveys, interviews with experts, and instantiation of TIBA in the context of digitalization of an automated transport system based on a real-world project from one of the partners of the BaSyS 4.0 project.

[6] <https://www.iese.fraunhofer.de/en/innovation_trends/industrie40.html>

1.5 Organization

This chapter presented an overview of the context and motivation for developing this doctoral project, including its main objectives and research methodology to conduct this work.

Chapter 2 describes the overall concepts related to Industry 4.0, blockchain, interoperability, and trust related to interoperability in Industry 4.0. It also describes concepts related to architecture drivers and solutions and architecture concerns.

Chapter 3 describes the main architecture drivers defined to promote trust in interoperability of Industry 4.0 and evaluation through a survey with experts from Industry 4.0.

Chapter 4 describes the architecture solution and decisions for the architecture drivers and the conduction of interviews with experts from Industry 4.0 aiming to evaluate the architecture solutions.

Chapter 5 describes TIBA that combines blockchain with traditional interoperability solutions. This section also provides the architectural views, and the steps for the evaluation through an instantiation in a real-world Industry 4.0 scenario.

Chapter 6 describes the instantiation of TIBA based on a real-world Industry 4.0 project. This section also provides the description of the use scenario, the architectural drivers and solutions for the scenario proposed and the architectural views of TIBA.

Chapter 7 describes the conclusions and future directions for this work.

CHAPTER

2

BACKGROUND

"I don't want the
trust that can be bought
My kind of trust is shareware"

The Ark

2.1 Initial considerations

Industry 4.0 has been the focus of attention of companies and researchers by bringing the opportunity to highly networked smart factories and by leveraging the complex production processes towards the fourth industrial revolution. Requirements related to interoperability apply to most Industry 4.0 systems independent of the application domain. Enabling trustworthy interoperability among manufacturers is one of the most important concerns for the success of Industry 4.0. The existing literature on architecture proposals for interoperability in Industry 4.0 focuses on standards and reference models, detailing how the high level of abstractions shall be considered for systems and machinery to interoperate securely and efficiently. Several research initiatives and technical solutions, including blockchain, have tried to solve the problems related to trustworthy interoperability. Thus, specific requirements shall be considered to achieve trustworthy interoperability. These set of particular requirements classified as new, risky, or expensive to implement or to maintain and therefore significantly affect the architecture are known as architecture drivers. The specification of architecture drivers must be precise enough to enable the software architect to properly reason about adequate architecture solutions. This chapter gives an overview regarding concepts related to Industry 4.0, interoperability, blockchain, and definition related to architecture drivers, architecture solutions, and architecture views for a proper understanding of this work.

2.2 Industry 4.0

Industry 4.0 refers to a new industrial revolution focused on integration and automation of production lines with the connectivity of different machinery, humans, and systems (ANTONINO *et al.*, 2019; XU; XU; LI, 2018). The concept of Industry 4.0 was first introduced in Germany's manufacturing sector and it is widely used across Europe and worldwide. In the United States, it is also used the term "Industrial Internet of Things (IIOT)" or IOT to refer to Industry 4.0 (KAGERMANN *et al.*, 2013). Industry 4.0 or IOT or IIOT are concepts that recognize that traditional manufacturing is in the process of a digital transformation. To understand the current state of manufacturing, it is vital to understand the history of the previous industrial revolutions (cf. Figure 2).

The first industrial revolution occurred in Britain over the 18th century and was characterized by the mechanization of the industrial process through water power and steam power. The second industrial revolution starts in the 20th century incorporating inventions, such as airplanes and Henry Ford's product line model (VAIDYA; AMBAD; BHOSLE, 2018; KAGERMANN *et al.*, 2013). The next period, the third industrial revolution, started in the 1970s and was known as the period of computer electronics, supply chain, and logistic. The fourth industrial revolution, also known as Industry 4.0, started in the year 2000 paving the way for the systematical deployment of CPS, which integrates network, physical devices, embedded computers with the internet (VAIDYA; AMBAD; BHOSLE, 2018; KAGERMANN *et al.*, 2013; ANTONINO *et al.*, 2019; KUHN *et al.*, 2018; UHLEMANN; LEHMANN; STEINHILPER, 2017).

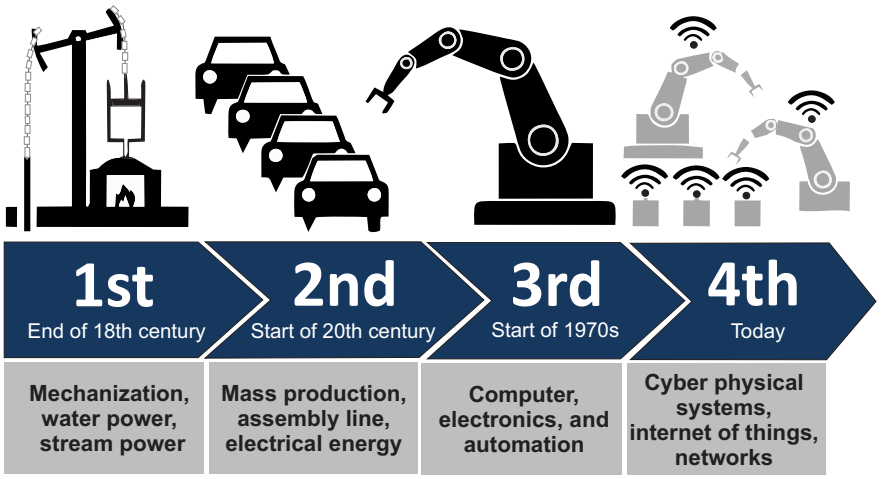

Figure 2 – Industrial revolution. Based on (KAGERMANN *et al.*, 2013)

Industry 4.0 has called the attention of companies by leading to highly networked smart factories (ANTONINO *et al.*, 2019; HEADAYETULLAH; PRADHAN, 2010; XU; XU; LI, 2018). It aims to completely transform the manufacturing processes from traditional hierarchical industrial automation to a cross-layer entity-to-entity communication (ANTONINO *et al.*, 2019). This entity-to-entity communication within smart factories must imply concerns related to

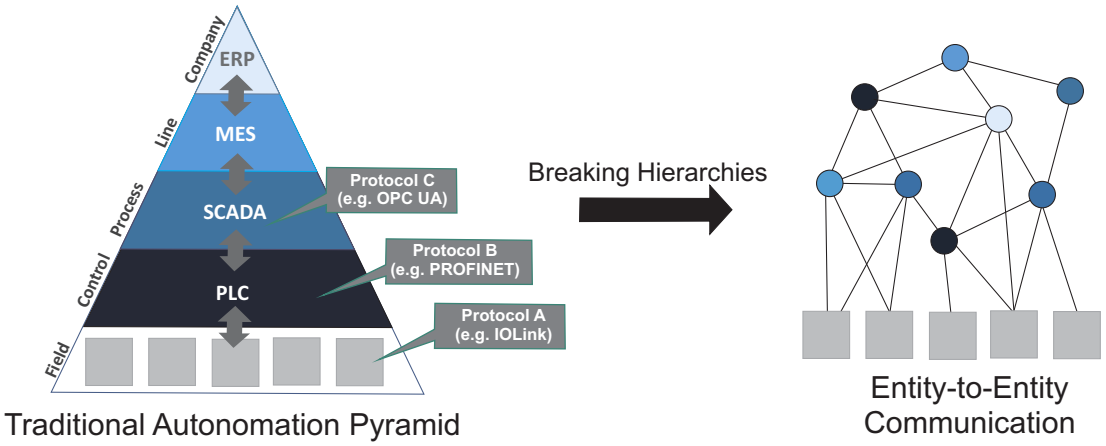

Figure 3 – Transitioning from traditional automation pyramid to entity-to-entity communication (ANTONINO *et al.*, 2019)

trustworthy interoperability among parties in different hierarchical levels from the production line. Figure 3 depicts the main layers of the automation pyramid (ANTONINO *et al.*, 2019). The Enterprise Resource Planning (ERP) is presented at the top of the automation pyramid. ERP manages the resource planning of the company, including human and material resources. ERP is primarily used for long-term planning in the process chain (ANTONINO *et al.*, 2019). The next level of the pyramid includes Manufacturing Execution Systems (MES) responsible for mid-term production planning and execution. SCADA and Process Distributed Control Systems (PDCS) control the system state during operation to avoid critical problems or failures in the production line. The digital computers known as PLC controls signals of sensors devices and machinery from the field level. The field level describes the machinery hardware, devices, and sensors responsible for execution of productive operations (KUHN *et al.*, 2018; ANTONINO *et al.*, 2019). The main transition from the hierarchical level to entity-to-entity communication encompasses the communication of a diverse of protocols into a homogeneous integration system instead of the creation of news patterns or standards. This entity-to-entity communication can be enabled by the Virtual Automation Bus (VAB), which bridges the communication between digital twins and different entities from the production line process (KUHN *et al.*, 2018; ANTONINO *et al.*, 2019).

Digital twins are the digital representation of a physical asset (TAO *et al.*, 2019). Digital twins enable simulation of future scenarios that can help with planning and preventive maintenance (UHLEMANN; LEHMANN; STEINHILPER, 2017; KUHN *et al.*, 2018; ANTONINO *et al.*, 2019). It also allows easier integration of data analysis, machine learning, and monitoring that can be directly tied to the physical asset. This includes horizontal integration that refers to integration of process at the production floor level and vertical integration that refers to integration of entities from production floor to higher-level business process such as quality control (KUHN *et al.*, 2018; ANTONINO *et al.*, 2019).

2.3 Interoperability

Interoperability can be roughly understood as the ability of two or more entities/-companies to exchange meaningful data and use this data to achieve common goals (BASS; CLEMENTS; KAZMAN, 2012; ISO/IEC, 2011). Interoperability addresses concerns regarding the connectivity among software systems, exchange of data and files, networking infrastructure, and other communications scenarios. Some challenges of interoperability address the ability to adapt in ever-changing environments, handle new technologies, transfer data in a secure manner, and connected legacy systems while new standards and technologies are being released.

To comprehend the main challenges of interoperability in Industry 4.0, we first investigated for frameworks considered different countries based on the studies (CHARALABIDIS; LAMPATHAKI; ASKOUNIS, 2009; BOSCH, 2016). The objective of this investigation was to gather a variety of versions of interoperability that have been created by different countries around the world. We compared 39 countries (Table 1) that have addressed the problem of implementation of interoperability by creating a National Interoperability Framework (NIF). These NIFs provide a set of recommendations, guidelines, and technical structure by which the e-Government services are developed to ensure the flow of information among their systems. As a national standard, many organizations follow the NIF to create their specific interoperability models. In general, interoperability solutions must be implemented following some principles. These principles guide the process of developing interoperability solutions and become the basis for the selection of interoperability standards. Many of the NIFs are designed by the principles of the European Commission and they describe the context in which European public services are designed and implemented as follows:

- **Security:** Citizens and businesses must be confident that when they interact with public authorities they are doing so in a secure and trustworthy environment and full compliance with relevant regulations, e.g., the Regulation and Directive on data protection, and the Regulation on electronic identification and trust services.

- **Privacy:** Public administrations must guarantee the citizens' privacy and the confidentiality, authenticity, integrity, and non-repudiation of information provided by citizens and businesses.

- **Openness:** It refers to the idea that all public data should be freely available for use and reuse by others unless restrictions apply e.g. for protection of personal data, confidentiality, or intellectual property rights.

- **Reusability:** Reuse means that public administrations confronted with a specific problem seek to benefit from the work of others by looking at what is available, assessing its usefulness or relevance to the problem.

Table 1 – Interoperability principles

N	Country	Reusability	Openness	Market Support	Security	Privacy
NIF1	Australia	✓	✓	✓	✓	
NIF2	Austria	✓	✓	✓	✓	✓
NIF3	Brazil		✓	✓		✓
NIF4	Bulgaria	✓	✓		✓	
NIF5	Canada	✓				
NIF6	China	✓	✓		✓	✓
NIF7	Croatia		✓		✓	✓
NIF8	Cyprus	✓	✓		✓	✓
NIF9	Czech-Republic		✓		✓	✓
NIF10	Denmarck	✓	✓		✓	
NIF11	Estonia	✓	✓		✓	✓
NIF12	Europe	✓	✓	✓	✓	✓
NIF13	Finland	✓	✓	✓	✓	✓
NIF14	Finland/Estonia	✓	✓	✓	✓	✓
NIF15	France	✓	✓	✓	✓	✓
NIF16	Germany	✓	✓		✓	✓
NIF17	ICEland	✓	✓	✓	✓	✓
NIF18	INDIA		✓		✓	✓
NIF19	Italy	✓	✓	✓	✓	✓
NIF20	Japan		✓		✓	✓
NIF21	Latvia	✓	✓	✓	✓	✓
NIF22	Lithuania	✓	✓	✓	✓	✓
NIF23	Luxembourg	✓	✓	✓	✓	✓
NIF24	Malaysian	✓	✓	✓		
NIF25	Malta			✓	✓	✓
NIF26	Mexico		✓	✓	✓	✓
NIF27	New Zealand				✓	✓
NIF28	Norway	✓	✓	✓	✓	✓
NIF29	Poland	✓	✓	✓	✓	✓
NIF30	Portugal	✓			✓	✓
NIF31	Slovakia	✓	✓	✓	✓	✓
NIF32	Slovenia	✓	✓	✓	✓	✓
NIF33	Spain		✓		✓	✓
NIF34	Swenden	✓	✓	✓	✓	✓
NIF35	Thailand	✓	✓	✓		
NIF36	The Netherlands	✓	✓	✓	✓	✓
NIF37	UK		✓	✓		
NIF38	USA	✓	✓	✓	✓	✓
NIF39	USA	✓			✓	✓

- **Market support:** Standards and specifications should be supported by the dominant technology platforms, software, business applications.

The NIFs facilitates the alignment of the organizational procedures with the technical systems. The result is the alignment of interoperability at the organizational level between different administrations. Technical standards are particularly important for the interoperability of systems. Eventually in the industry, standards increase the levels of quality, reliability, safety, and efficiency of interoperability, providing benefits at an economical cost.

2.3.1 Interoperability in Industry 4.0

While interoperability in traditional industry deals with repetitive tasks for standardization encompassing automation of single machines and processes sometimes controlled by a central authority, interoperability in Industry 4.0 encompasses an end-to-end implies collab-

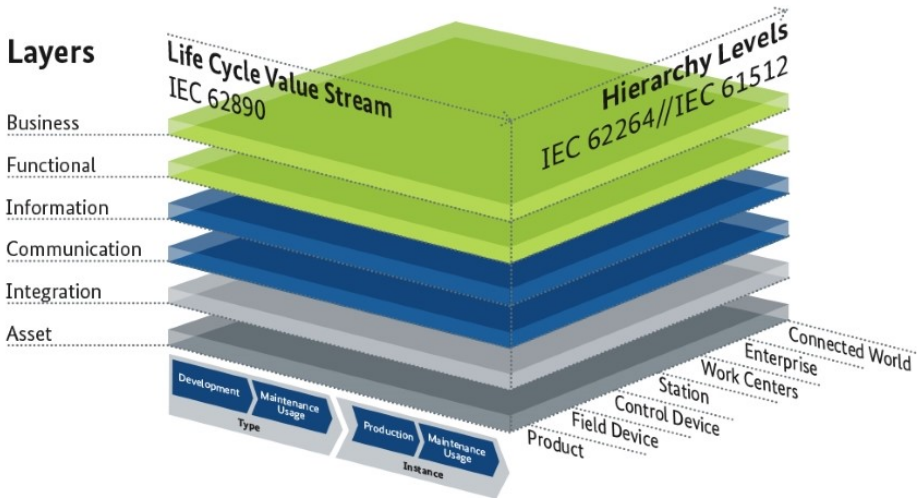

Figure 4 – The reference architecture model Industry 4.0 (ZVEI-ELEKTROINDUSTRIE, 2015)

oration of several interconnected virtual and physical entities within smart factories, such as software systems, CPS, networks, equipment (e.g., robots, machines, IoT devices, and PLC), as well as processes and services (XU; XU; LI, 2018; Qiu *et al.*, 2020). Besides, Industry 4.0 usually involves some companies, such as producers, suppliers, vendors, distribution centers, and retailers, across complex supply chain networks. In this scenario, interoperability among all these entities (i.e., virtual/physical entities within smart factories and companies) is not only crucial to the success of Industry 4.0 but also a great challenge. According to the Ponemon Institute[1], more than 90% of industries faced at least one major attack in the past two years, including denial of service attacks, man-in-the-middle attacks, malicious actions, espionage and data theft. Most systems attacked adopt IP-based connectivity as ICS, SCADA, and PLC. Besides, GarnetIT[2] reports communication is one of the most vulnerable targets in the 4th industrial revolution.

Several consortia have been working towards the definition and goals of interoperability in Industry 4.0 by providing reference models from different perspectives. The most known reference architecture used by Industry 4.0 is the Reference Architectural Model Industrie 4.0 (RAMI 4.0) and the Industrial Internet Reference Architecture (IIRA). They incorporate industrial requirements, such as integration, communication, and interoperability, which derive capabilities of middlewares regarding harmonized interfaces and communication protocols.

The RAMI 4.0 (Figure 4) was developed by the German Electrical and Electronic Manufacturers' Association (ZVEI) to support Industry 4.0 initiatives. It consists of a three-dimensional coordinate system that contains the essential aspects of Industry 4.0. Complex relationships can thus be broken down into smaller, more manageable packages.

The "Hierarchy Levels" are based on the IEC 62264, the international series of standards

[1] <https://www.trendmicro.com/vinfo/us/security/news>
[2] <https://www.rambus.com/iot/industrial-iot/>

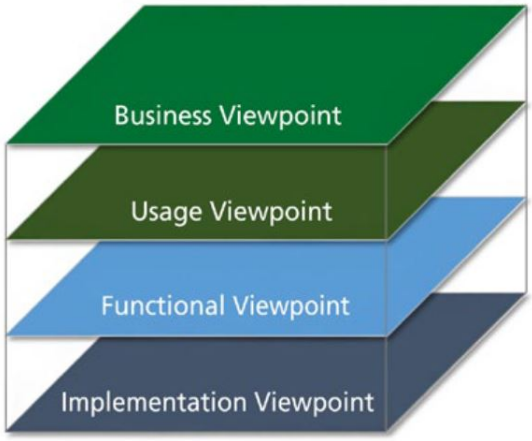

Figure 5 – The industrial internet reference architecture (LIN *et al.*, 2017)

on the integration of corporate IT and control systems. These levels represent the different functionalities within the industry or the plant. The functionalities were supplemented by the workpiece, "Product", and the access to the Internet of Things and Services, "Connected World" to map the Industry 4.0 environment. The "Life Cycle and Value Stream" levels represent the life cycle of systems and products. The basis for this is IEC 62890 for life cycle management. A distinction is also made between type and instance. A “type” becomes an “instance” when the development and prototype production has been completed and the actual product is manufactured in production. The "Layers" represents the IT, i.e. the virtual mapping of machines, for example, is described in a structured layer by layer. The representation in layers comes from information and communication technology. The three axes map all essential aspects of Industry 4.0. They make it possible to classify an object such as a machine into a model. RAMI 4.0 provides a highly flexible Industry 4.0 concepts that shall be described and implemented. The reference architecture model allows for the gradual migration from today to Industry 4.0.

The IIRA (Figure 5) (LIN *et al.*, 2017) is a standard-based open architecture under the Industrial Internet Consortium (IIC) for designing Industrial Internet Systems (IIS). Based on ISO/IEC 42010, IIRA defines what are the most important industrial internet architecture components, their connections and categorize the IIS concerns on four viewpoints: implementation, functional, usage, and business viewpoint.

- Business viewpoint: includes all business concerns when setting up an IIS as well as the regulatory framework. Basic system properties are defined and oriented towards business goals. The stakeholders with this viewpoint are usually executives, product managers, and systems engineers.

- Usage viewpoint: includes all concerns for using an IIS. A typical representation is the description of operating procedures.

- Functional viewpoint: focused on the functional components of an IIS. Their relationships, structure, interfaces, and interactions play a role. The interactions of an IIS with its environment are also relevant at this level.
- Implementation Viewpoint: covers the technologies required to implement an IIS. The focus is on functional components, their networking and communication interfaces as well as their product life cycles. The concerns summarized here are of particular relevance for component designers, system developers, and integrators.

In the second part of the description, IIRA describes key system concerns, such as:

- Safety: functional safety;
- Security, Trust, and Privacy: IT security and data protection;
- Resilience: Reliability;
- Integrability, Interoperability, and Composability: Scalable integrability and interoperability;
- Connectivity: networking;
- Data Management: Integrated data management;
- Analytics and Advanced Data Processing: Advanced data analysis capabilities;
- Intelligent and Resilient Control: Robust controls;
- Dynamic Composition and Automated Interoperability: ad hoc capabilities and plug and play.

The reference architectures RAMI 4.0 and IIRA describe the logical structure of overall systems and processes in the Industry 4.0 and IIoT environment. The main focus is on the standardization of terms, representation of functionalities and concerns in higher abstract levels, and the definitions of semantic relationships. However, IIRA addresses interoperability differently in comparison to RAMI 4.0. The central concept of the IIRA is the use of Digital Twins that can continually record the measurements and create a profile to be used to provide insights regarding systems performance and possible future changes in product design or the manufacturing process. RAMI 4.0 relies on different protocols and standards for each component to communicate independently using Industry 4.0 communication protocols. In summary, Industry 4.0 may benefit from the cross implementation of both architectures.

2.3.2 Trustworthy interoperability in Industry 4.0

The existing literature regarding interoperability in Industry 4.0 encompass approaches focusing mainly on *security* to enable trustworthy communication among devices, systems, manufacturers, and the production line. Confidentiality, integrity, and availability are the classical model to guide the creation of security policies within organizations that enable trustworthiness interoperability among the systems (Fraile *et al.*, 2018). According to (SCHRECKER; SOROUSH; MOLINA, 2016), the main requirements for trustworthy interoperability in Industry IoT systems shall encompass:

- **Security**: it ensures that the system is protected from unauthorized access, change, or disruption.
- **Resilience**: it provides means to dynamically avoid misuse, attacks, accidents, and rapidly recover from changing failure conditions.
- **Reliability**: it ensures the system's operation is error-free for the specified time.
- **Availability**: it is related to reliability and planned operation stops.
- **Privacy**: it provides authorization control over the data and storage of information and defines how the information can be shared by systems or by organizations.
- **Safety**: it ensures that the stakeholders and environment are free of any unacceptable risk during the system's operation.

Trustworthy interoperability in Industry 4.0 involves a range of activities and technologies that encompass the entire lifecycle of its entities and systems. The state-of-the-art highlights some of the scientific works that contribute with solutions to provide more trust in the communication of Industry 4.0 systems. The works of (Fraile *et al.*, 2018) and (Bicaku *et al.*, 2017) focused on trust related to cybersecurity during the design of gateways for different system's layers. The mechanisms to ensure trustworthiness are based on standards that provide technical security using certificate authorities and role-attribute-based access control to ensure proper data access. Other two examples of works are (KJERSGAARD; ERIKSENA, 2018; KJERSGAARD; ERIKSENA; HARLAMOVA, 2018) that proposed to enhance trust in the access control using public and private keys to check CPS identity. They proposed a solution based on blockchain to manage authentication identities. Trust is placed in CPS ownership and the system uses its currency to protect data against non-authorized users. Besides security, trustworthy interoperability in Industry 4.0 has been also addressed by *privacy* through, for instance, encryption techniques that encode proven dependencies among smart objects (Petroulakis *et al.*, 2019), and trustworthy policies to increase data privacy by using contracts and security mechanism (AL-ALI *et al.*, 2018a). All these and other related works are examples of punctual solutions that could promote

to some extent trustworthy interoperability in Industry 4.0. However, such interoperability could encompass not only a subset of aspects, but also a broader spectrum involving, for instance, reliability, fault tolerance, compatibility, availability, and scalability, some of them pointed out still as challenges and research opportunities to improve the Industry 4.0 interoperability (Habib; Chimsom, 2019), (IWANICKI, 2018), (Sisinni *et al.*, 2018), (Delsing, 2017), (Schulte; Colombo, 2017).

Other related works conducted surveys and SLR on interoperability of Industry 4.0. LU (2017) presents a comprehensive review of architectures and frameworks for interoperability in Industry 4.0 detailing the three frameworks Advanced Technologies for Interoperability of Heterogeneous Enterprise Networks and their Applications (ATHENA); Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR); and Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens (IDABC)). These frameworks specify different levels of abstractions including operational, technical, semantic to covering standards, models, and protocols necessary to make Industry 4.0 more productive and less expensive. Study (HOFER, 2018) also presented an SLR on main technologies and architectures for Industry 4.0, including CPS, IoT, enterprise architecture, Information and Communications Technology (ICT), and Enterprise Integration (EI). This study outlined interoperability related to data transparency and decentralized decisions and highlighted the main challenges for interoperability in Industry 4.0. Considering the related work, we observed there were still many open issues to achieve trustworthy interoperability in Industry 4.0, which motivated us to conduct our work.

2.4 Software architecture

When discussing architecture it is important to present a proper definition. IEEE defines architecture as “the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution” (IEEE. . . , 2000). This definition addresses several aspects that are of interest in the context of interoperability. First, it addresses how a system is organized concerning its environment. Next, the principles governing the design of the system are addressed. The current design goes hand-in-hand with evolution principles. And finally, how the system implements the provided functionality is addressed.

Architectures are therefore needed for the conceptualization part of systems and enterprises as well as the implementation part, latest particularly for systems. They have to provide structured documentation of who is doing what, where, when, why, and how. This information must be provided in the machine-understandable form to allow support of identifying solutions for potential reuse, selecting the best systems in case of alternative solutions, compose the solutions into a system of systems providing the required functionality, and orchestrate the

execution.

Designing architecture is the creative activity of software engineers making principal design decisions about a software system to be built or to be evolved. It translates concerns and drivers in the problem space into design decisions and solution concepts in the solution space (cf. Figure 6). Software architects have to know how to accomplish business goals, how to achieve key functional and quality requirements, and how to handle given constraints. To support software architects during this decision process, architecture drivers can be used (KNODEL; NAAB, 2016). They capture the important and significant unknown requirements regarding stakeholders' concerns. The design decisions must define solution concepts that satisfy the architecture drivers considering the given context factors. The arrows represents the architecture concerns that spans in each architecture area of interests and represent explicit information being exchange and communicated in each architecture stage (KNODEL; NAAB, 2016).

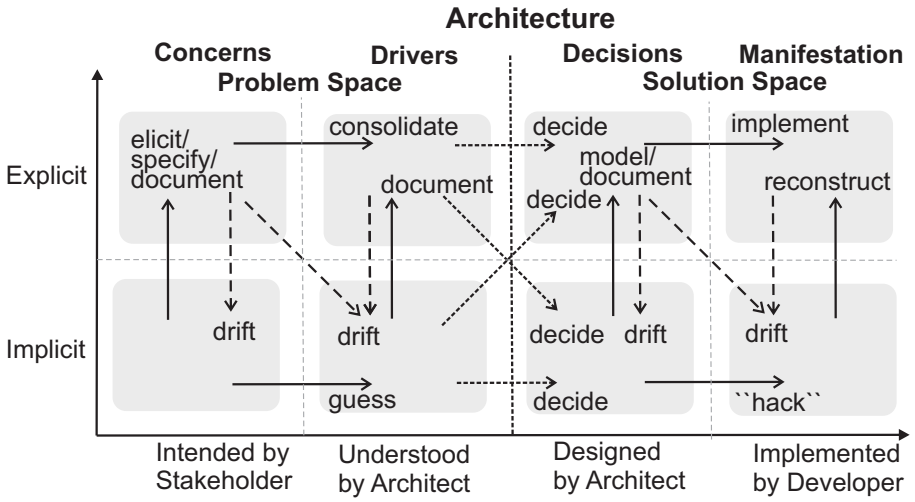

Figure 6 – Architecting design process. Extracted from (KNODEL; NAAB, 2016)

Architecture drivers

Architecture drivers are a particular set of requirements classified as new, risky, or expensive to implement or to maintain (KNODEL; NAAB, 2016) and therefore significantly affect the architecture. The specification of architecture drivers must be precise enough to enable the architecture to properly reason about adequate architecture solutions to address them. In this regard, we adopted the approach proposed by Knodel and Naab (2016), who claim that architecture drivers must be specified in terms of (i) the environment or condition in which this driver occurs; (ii) the event that stimulates the occurrence of the driver; (iii) the expected response of the system to the driver event; and (iv) the quantifications associated with the three previous aspects. Each of these measurable effects indicates whether the driver is addressed by the architecture.

The systematic specification of the architecture drivers must indicate what quality aspects characterize the system functions described in each architecture driver specification. For instance, instead of claiming that the light barrier sensors shall transmit signals to the roller conveyor of the production plant, we might characterize the system function by the degree of security of the signal transmission (e.g., the maximum tolerable delay). In this way, the architecture drivers specify not only the what but also the how well (i.e., with what degree of quality), thereby providing proper information for the selection of an adequate architecture solution for each architecture driver. To this end, we adopted the quality characteristics described in ISO/IEC 25010 Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality model to characterize the I4.0 architecture drivers described in this thesis. ISO/IEC 25010 comprises the following quality characteristics: Functional Suitability, Performance Efficiency, Compatibility, Usability, Reliability, Security, Maintainability, and Portability. Each quality aspect is further refined into sub-aspects.

Architecture solutions

The architecture solutions are regarding the designing of a solution that properly fits to satisfy the architecture driver. It describes the rationale for designing a solution and discarding the others. The solution needs iterations of revisions and updating the documentation of the respective solution. The solution shall describe the advantages, drawbacks, and trade-offs of a solution concept (or alternative solution concepts) for satisfying the architecture driver previously defined.

Architecture describes the solution space of a system and therefore traditionally is thought of as an early part of the design phase (KNODEL; NAAB, 2016). Design decisions must define solutions to satisfy architecture drivers considering a given context and stakeholders' concerns. Each architecture driver has one or more associated architecture solution specifications. The approach proposed by Knodel and Naab (2016) describes architecture solution in terms of (i) an overview description of the design decision(s) that comprise the architecture solution; (ii) pros and opportunities, i.e., the positive aspects of the architecture solution that contribute to achieving the architecture driver; (iii) assumptions and quantifications; (iv) cons and risks, i.e., the aspects that might impose challenges regarding the achievement of the driver; and (v) trade-offs. i.e., other quality attributes, drivers, and decisions that might be negatively impacted by the architecture solution (ANTONINO *et al.*, 2019).

2.5 Blockchain

Blockchain is a digital technology that provides a decentralized digital database of transactions commonly associated with cryptocurrencies e.g., Bitcoin (NAKAMOTO, 2009). During recent years, blockchain have been applied across a wide variety of industry sectors, including

healthcare (Wang *et al.*, 2018), financial (PAZAITIS; FILIPPI; KOSTAKIS, 2017), automotive (Yang *et al.*, 2019), Internet of Things (Christidis; Devetsikiotis, 2016), and government sectors (EUBLOCKCHAIN, 2018).

Blockchain works under three main concerns: decentralization, transparency, and immutability (WEBER *et al.*, 2016). Decentralization means information is not stored in a unique single entity, instead, everyone in the blockchain network owns the information. Transparency in blockchain provides a fully auditable and valid ledger of transactions. Immutability means data are once written is hard to be changed, which brings more trust and integrity to the data being transferred (WEBER *et al.*, 2016). Some blockchain also provides a computation infrastructure to execute autonomous code called smart contracts.

Smart contracts are automatically executable codes that run when predetermined conditions and rules are met (MORKUNAS; PASCHEN; BOON, 2019). They allow parties to trade information without an intermediary (middleman), which provides a trustworthy and secure environment (PAZAITIS; FILIPPI; KOSTAKIS, 2017). Smart contracts are designed to work when monetary or other conditions are agreed upon, and these transactions can be viewed by the involved parties in real-time.

It is possible to use smart contracts in many situations with bitcoin; however, the use of bitcoins in a smart contract is very limited in contrasts to Etherum[3] (PAZAITIS; FILIPPI; KOSTAKIS, 2017). The main advantages of the smart contract is automation, time-saving, safety, and reliability of data being transferred. However, redundancy is one of the main problems as transactions must be processed independently in every node of the blockchain network.

Many blockchain solutions have been proposed to deal with security concerns in the interoperability of systems. Guerreiro et al. (GUERREIRO *et al.*, 2017) propose a security risk-based metamodel using blockchain concepts for the execution of business transactions. Their proposal focuses on the technical interoperability level of enterprise business by controlling the access to transaction state data objects. Other studies (ZAMYATIN *et al.*, 2019; KWON; ETHANBUCHMAN, 2019; SPOKE; NUCO, 2017) go in the same direction by using blockchain for enabling trust and security communication at a technical level. From a medical domain perspective, researchers developed various techniques targeting interoperability between systems using blockchain concepts. The work (GORDON; CATALINI, 2018) explores potential ways blockchain can facilitate communication from institution to patient. Studies (ZHANG *et al.*, 2017; EKBLAW *et al.*, 2016; YANG; YANG, 2017; NICHOL; BRANDT, 2016; PETERSON *et al.*, 2016) also explore the applicability of blockchain to exchange health information in a secure and fast manner at the technical communication level. From the IoT application domain, blockchain concepts were also explored as a solution for in the interoperability of IoT systems. Study (Li *et al.*, 2018) explores the use of blockchain to enable secure energy interoperability in microgrids, vehicle-to-grids, and energy harvesting networks. They use the concept of credit-based payment

[3] <https://www.ethereum.org>

to allow the transaction between IoT systems. Study (DURAND; GREMAUD; PASQUIER, 2017) proposed a decentralized public key infrastructure to improve security and transparency of data being transferred. (Jin; Dai; Xiao, 2018) proposes an architecture to reduce the overhead while maintaining the timeliness of communication between blockchain. They organize the architecture in five blockchain architecture layers, including *Data Layer* that contains transaction format, *Network Layer* ensures consistency of blockchain states, *Contract Layer* coordinates the smart contracts, and *Application Layer* supports API applications. (KJERSGAARD; ERIKSENA, 2018; KJERSGAARD; ERIKSENA; HARLAMOVA, 2018) proposed an access control protocol for Industry 4.0 using blockchain to avoid central authority controlling authentication. (Mohamed; Al-Jaroodi, 2019) proposed a middleware solution based on blockchain to promote trust in the integration of resources and services, by enabling secure and traceable data among smart manufacturing applications. This middleware abstracts devices and systems functionalities as services and assure traceability of data among smart manufacturing applications. Interoperability is a fundamental architecture concern for the interaction of Industry 4.0 systems, and many efforts have been applied towards providing architectural solutions and standards to support high levels of interoperability at early development stages. However, communication between parties relies on common agreements made by intermediaries in many levels of interoperability concerns, which increases the cost and barriers of collaboration, as it usually involves unpredictable behavior of operations made by humans. Besides, these studies describe important initiatives to assure trustworthy interoperability in smart factories, but they are focused on punctual solutions and do not encompasses at the same time a balance among the main quality aspects regarding trustworthy interoperability (i.e., authentication to the system, data access control, privacy control to protected sensitive information, data traceability and auditability, physical devices availability, data availability, and data and services compatibility) (HEADAYETULLAH; PRADHAN, 2010; JUNGO, 2015; LI; PING, 2009).

2.6 Final considerations

Interoperability is the ability of complex software systems to interact and share information and knowledge towards mutually common goals. Many models and standards for interoperability already exist and they are used to determine the degree of communication among information technology systems. The increased importance of integration of companies and the increased market needs are placing high demands on all areas of industry, including technology, security, organization process, and laws. In this context, interoperability in Industry 4.0 highlights the importance of proper agreements and collaboration contracts to support future demands of services and products. However, the main challenge of these models is the centralization of data and many middlemen to intermediate the access of information. Consequently, information consumer has no way to ensure data reliability, which facilitates the misuse or even fraud of data being transferred. Blockchain makes a good fit for solving interoperability problems related to

the reliability of data being transferred and could be used to design a trustworthy solution for interoperability in Industry 4.0.

CHAPTER

3

ARCHITECTURE DRIVERS

"Time waits for nobody
We've got to trust one another
Or we'd have no more future at all"

Freddie Mercury

3.1 Initial consideration

Industry 4.0 has come to the attention of companies as it enables highly networked smart factories and leveraging of complex manufacturing processes. How to achieve trustworthy interoperability among several heterogeneous entities and also among companies is still a challenge, however; hence, there is a strong focus on research, standardization initiatives, and adaptation of solutions from other areas. Yet, companies interested in Industry 4.0 do not have any guidance on what solutions or concerns should be considered to architect Industry 4.0 systems that assure trustworthy interoperability. This chapter contributes with a set of essential requirements for assuring trustworthy interoperability in Industry 4.0 known as architecture drivers. These architecture drivers are a set of key main requirements to promote trustworthy interoperability. This chapter presents the process to identify and define them based on the main challenges regarding interoperability in real-case Industry 4.0 projects. The drivers were designed by combining such challenges with quality aspects extracted from a systematic literature review. These drivers were then refined based on a survey with experts from Industry 4.0. As a result, seven architecture drivers were defined: Authentication to the System, Data Access Control, Data Privacy to Protect Sensitive Information, Traceability and Auditability of Data, Availability of Physical Devices, Availability of Data, and Compatibility of Data and Services.

3.2 Architecture drivers design

Architecture drivers are a set of key main requirements classified as risky, new, and costly to be maintained, which can seriously affect the architecture design and implementation. Thus, the research method used to define the architecture drivers to promote trustworthy interoperability of Industry 4.0 encompassed five activities, as follows:

- *Observations from industry projects:* Our analysis started by observing real-world industrial projects in the context of BaSys 4.0[1]. These observations were summarized as the current challenges and concerns faced by the projects concerning trustworthy interoperability in Industry 4.0;
- *Systematic Literature Review:* To complement the previous observations, we conducted an SLR to gather evidence from literature about the quality aspects related to trust in the interoperability in Industry 4.0;
- *First definition of architecture drivers:* The quality aspects found in the SLR were used as basis of the first version of the architecture drivers. In that moment, we defined six drivers (Appendix A), namely *Authentication*, *Data Consistency*, *Data Privacy*, *Traceability*, *Availability*, and *Scalability*. It is worth highlighting the finding of these drivers was grounded on real use case scenarios from our research group working with BaSys 4.0;
- *Refinement of architecture drivers:* Architecture drivers were systematically refined and improved through the conduction of a survey with experts from Industry 4.0; and
- *Final definition of architecture drivers:* Results of this refinement resulted in seven drivers, namely *Authentication to the system*, *Data access control*, *Privacy control to protected sensitive information*, *Traceability and auditability of data*, *Availability of physical devices*, *Availability of data*, and *Compatibility of data and services* (whose final version is presented in Section 3.3).

The following sections details the activities: (i) Section 3.2.1 presents the SLR planning and synthesis of results; and (ii) Section 3.2.2 presents the refinement of architectural drivers through the survey.

3.2.1 Systematic literature review

We conducted an SLR based on the guidelines proposed by Kitchenham and Charters (2007) to understand and gather studies regarding trustworthy interoperability in Industry 4.0. The main steps for the conduction of this SLR and its results are presented as follows.

[1] <https://www.iese.fraunhofer.de/en/innovation_trends/industrie40.html>

Planning and Conduction

An SLR protocol was created to reduce the possibility of biases, and herein we present the main parts of its protocol that were established and followed to reduce the possibility of biases. This protocol contains: (i) research questions; (ii) search strategy; (iii) inclusion/exclusion criteria; (iv) selection of studies; and (v) synthesis of SMS results.

i) Research question: The specific objective of this SLR is to identify existing studies that describe quality concerns to promote trustworthy interoperability in Industry 4.0. For this, we established the following research questions (RQ):

RQ: *How has trust in the interoperability in Industry 4.0 been promoted?*

i) Search strategy: It supports the identification and retrieval of as many relevant studies as possible. The search string was defined using terms that entail the most appropriate keywords on the scope of this SLR, as follows:

(("Industry 4.0" OR "I4.0" OR "I4" OR "industrial revolution" OR "Industrial Internet of Things" OR "IIOT") AND ("interoperability")).

Following, the most important electronic databases for computing was selected to rung the search string: ACM DL[2], IEEE Xplore[3], Science Direct[4], and Scopus[5]. The search string was used against the metadata (titles, keywords, and/or abstracts) of selected databases. The search string was used against the metadata (titles, keywords, abstracts) in the selected databases. We considered studies from the lasts 20 years. After running the search queries, 400 studies were recovered (18 from ACM DL, 106 from IEEE Xplore, 37 from Science Direct, and 239 from Scopus) and, after removing repetitive studies, 277 studies remained.

iii) Inclusion/exclusion criteria: Selection of primary studies was based on predefined inclusion and exclusion criteria:

Inclusion Criteria:

- IC1. Quality attributes to promote trust in interoperability of Industry 4.0.
- IC2. Requirements to promote trust in interoperability of Industry 4.0.

Exclusion Criteria:

- EC1. Study not related to Industry 4.0 context.
- EC2. Study not describe trust requirements for Industry 4.0.

[2] http://dl.acm.org
[3] http://ieeexplore.ieee.org
[4] http://www.sciencedirect.com
[5] http://www.scopus.com

- EC3. Duplicated studies.
- EC4. Study containing an editorial, abstract, or introduction.
- EC5. Study not written in English.

iv) Selection of Studies: Inclusion and exclusion criteria were applied in two rounds of selection. In the first one, the reading of the title and abstract of each study was conducted, and, in cases where they were not enough to decide whether the study should be included or excluded, introduction and conclusion sections were also read. In this activity, 240 studies were removed and 37 potential studies were selected. In the second round, the full text of all selected studies was read to find out whether they meet the inclusion and exclusion criteria. This activity ended with a selection of 18 studies. The complete list of studies can be seen in Appendix A. Figure 7 presents the main process of this SLR.

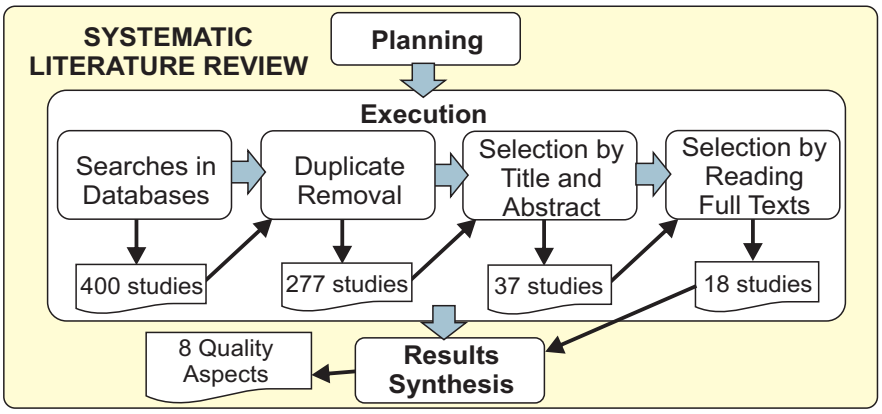

Figure 7 – SLR process

Synthesis of results

This section summarizes the content of the 18 studies found. Figure 8 shows the number of studies that address each quality aspect that could promote trust in interoperability in Industry 4.0 grouped by research topics. As can be seen in Figure 8, most studies are describing specific solutions for interoperability, which encompasses some quality aspects to enable trustworthy interoperability. For instance: i) Authorization, Authentication, Data Privacy are quality aspects related to security. These quality aspects are described as solutions to access control and authentication to the system (Kolluru *et al.*, 2018; XU; XU; LI, 2018; Delsing, 2017), end-to-end communication describing security protocols for communication (Polonia; Melgarejo; de Queiroz, 2015), meta-data for security semantic interoperability (Petroulakis *et al.*, 2019), security IoT gateways for providing secure connectivity between devices (Condry; Nelson, 2016); ii) Availability is presented in some studies that describe solutions to increase the redundancy of devices and reduce failures with safety mechanisms to increase availability (IWANICKI, 2018), (Urbina *et al.*, 2019); iii) Scalability is described in some studies that present

solutions for reconfiguration of devices to increase the ability to change the production structure and increase the productivity, and scalability in the machine level that could be tailored according to manufacturing demands (Imtiaz; Jasperneite, 2013). These quality concerns have been the focus during the design of architectures, metamodels, and security mechanism for providing more reliable interoperability, but also have been considered big challenges as described in (IWANICKI, 2018; Sisinni *et al.*, 2018; XU; XU; LI, 2018; Habib; Chimsom, 2019; Delsing, 2017; Schulte; Colombo, 2017). The most challenges highlighted by these studies are that most techniques and solutions developed for interoperability in Industry 4.0 cannot be adapted or used in an industrial context due to many restricted requirements regarding many other quality aspects, such as fault-tolerance, safety, reliability, compatibility, and integrity of data (DOBAJ *et al.*, 2018). The main reason is that these solutions, even using web technologies, are not designed according to architectural design principles, which requires a deep analysis of the main quality requirements that can further affect the whole design of an architecture (Polonia; Melgarejo; de Queiroz, 2015).

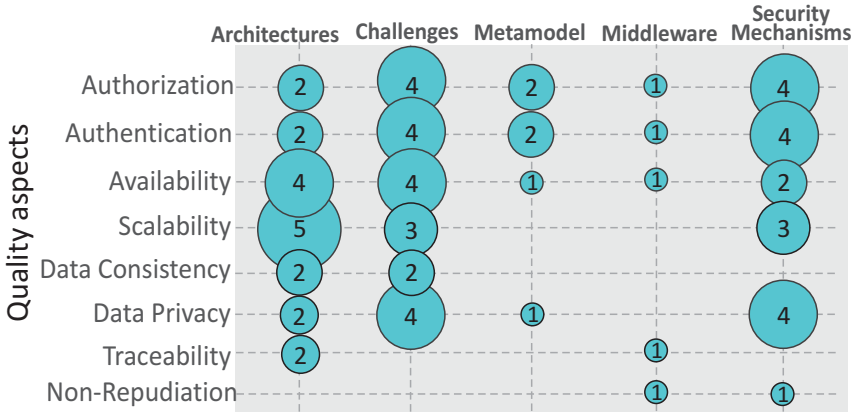

Figure 8 – Number of studies addressing the quality aspects for trust in interoperability in Industry 4.0 classified into research topics

The analysis of the SLR provided us evidence of the lack of studies that encompass these main quality aspects that can further affect the whole architecture. Architectural solutions for interoperability in Industry 4.0 must be first designed by identifying the main quality aspects that can interfere with the whole project. To support this identification, use case scenarios and specific requirements for Industry 4.0 must be analyzed (Polonia; Melgarejo; de Queiroz, 2015; Sisinni *et al.*, 2018; XU; XU; LI, 2018; Habib; Chimsom, 2019). Details of each quality aspect together with possible technical solutions are presented below:

Authentication: Its main role is to support the assignment of applications and users with their respective tokens who have access to a system (Petroulakis *et al.*, 2019). To enable trustworthy interoperability, Industry 4.0 requires assurance that each user and device has a unique identity when attempting to make a connection (Sisinni *et al.*, 2018; Habib; Chimsom, 2019; Polonia; Melgarejo; de Queiroz, 2015); this includes security manager and accounting services to exchange/publish data (Petroulakis *et al.*, 2019). ***Technical solution:*** Protocol-level

security measures, such as homomorphic signature scheme (PERALTA *et al.*, 2019), and a combination of multi-factor authentication (id, password, PIN, email account, token device, fingerprint) (Schulte; Colombo, 2017; Schulz, 2015) could promote trust.

Authorization: This determines the privileges and permissions of authenticated users or devices to use a resource in the system (Petroulakis *et al.*, 2019; Sisinni *et al.*, 2018). Industry 4.0 needs assurance that authorization should rely on peer devices to enable decentralized access rules verification to authorize users and objects to access the network. To enhance trust in authorization, an authority mechanism should certify a user's access according to security rules and entitlement policies based on particular attributes or roles (Fraile *et al.*, 2018). ***Technical solution:*** Access Control Lists (ACL), Access Rules, or coverage by a Role-Based Access Control (RBAC) model, which all control individuals' access to a system (Polonia; Melgarejo; de Queiroz, 2015; Habib; Chimsom, 2019; Schulte; Colombo, 2017; PERALTA *et al.*, 2019; Condry; Nelson, 2016). A certification authority is another mechanism to enable trust and protect data confidentiality (Fraile *et al.*, 2018; Delsing, 2017; Bicaku *et al.*, 2017).

Data Privacy: This often related to two main concerns: (i) an anonymous data process to ensure confidentiality of information through cryptography protection (PERALTA *et al.*, 2019); and (ii) a data collection process to ensure data will be collected for authorized personnel only (Sisinni *et al.*, 2018; Petroulakis *et al.*, 2019; Polonia; Melgarejo; de Queiroz, 2015). Data privacy should obey legislative requirements to bring trustworthy interoperability in Industry 4.0, protecting and monitoring data, and avoiding that production process secrets are betrayed (Schulz, 2015; Fraile *et al.*, 2018). ***Technical solution:*** Technologies guided by laws and regulations aimed at addressing privacy issues throughout the data lifecycle must be implemented and combined with authorization security approaches to only give access to authorized users (Fraile *et al.*, 2018). Besides, information must be classified into sensitive and public data to ensure that each authorized device may collect data (Schulz, 2015).

Traceability: This is defined as the ability to track digital information and data transactions along their full life cycle (KAUR *et al.*, 2018). In Industry 4.0, traceability allows decision-makers to come up with resolutions of issues, or to work out solutions instantly. Implementing traceability increases the transparency of companies across their end-to-end value chain. Traceability also improves control over production quality. ***Technical solution:*** Dobaj et al. (DOBAJ *et al.*, 2018) used patterns to trace external service requests by assigning a unique ID to each external service request. Mohamed and Jaroodi (Mohamed; Al-Jaroodi, 2019) used blockchain to allow traceable audit trails to detailed information regarding transaction records in the chain.

Non-Repudiation: This refers to the inability of a system or a person to deny the validity of their authorship actions (Fraile *et al.*, 2018; Mohamed; Al-Jaroodi, 2019). To ensure this, all transactions must be logged and trail data must be created and stored for further audit. Traditional centralized non-repudiation solutions fail to bring trust into Industry 4.0 because they rely

on third parties to control the information. Decentralized solutions can improve Industry 4.0 scenarios in which the service publisher is delivered separately and mandatorily recorded in a hash ledger. ***Technical solution:*** Study (Fraile *et al.*, 2018) used a centralized security center that implements Role-Based Access Control and Attribute-Based Access Control (RBAC-ABAC). The advantage of this approach is that it reduces errors in the implementation of device drivers (Fraile *et al.*, 2018; Mohamed; Al-Jaroodi, 2019).

Scalability: The need for scalability imposes some concerns related to authorization, service exchanges, flexibility, and orchestration across protective boundaries (Delsing, 2017; XU; XU; LI, 2018; Sisinni *et al.*, 2018; Habib; Chimsom, 2019; DOBAJ *et al.*, 2018; IWANICKI, 2018; Petroulakis *et al.*, 2019). An Industry 4.0 system needs to connect a huge number of devices and must have the means to collect and analyze data. ***Technical solution:*** A stable data network is necessary to implement trust in scalability in Industry 4.0 to enable devices to share information and manufacturers to quickly identify risk and avoid major performance outages (Delsing, 2017; XU; XU; LI, 2018).

Data Consistency: It must be ensured that data will not be changed during transactions or processing. A proper consistency checking mechanism must ensure the same data for each node in the network (IWANICKI, 2018; DOBAJ *et al.*, 2018). Digital twins can be used in Industry 4.0 to reduce the time needed for reconfiguration by detecting sequence errors of the system (ANTONINO *et al.*, 2019). ***Technical solution:*** Constrains rules and consistency check mechanisms can enforce verification of data from different enterprises localized in distinct locations (IWANICKI, 2018; DOBAJ *et al.*, 2018).

Availability: Availability demands that all relevant information must be accessible in real-time through the interconnection of all components of an Industry 4.0 system, regardless of physical damage of devices or malicious user faults (Fraile *et al.*, 2018). ***Technical solution:*** Clusters, redundancy mechanisms, RAID, and fail-over techniques can mitigate serious consequences when hardware issues occur (IWANICKI, 2018; Petroulakis *et al.*, 2019). However, replication brings data conflicts, resulting in the inconsistency of information along the industrial chain (Schulte; Colombo, 2017). Availability also raises questions regarding data integrity, as information must be globally available across company and systems boundaries. Cloud computing publishes data and guarantees data availability globally, but raises concerns related to security and control to safeguard data (Sisinni *et al.*, 2018; GAZQUEZ; BUENO-DELGADO, 2018).

3.2.2 Refinement of architecture drivers

This section presents the steps conducted to refine the first version of the architecture drives as follows.

Survey design and execution

Surveys are widely applied as a valuable means for gathering human opinion via questionnaires or interviews (WOHLIN *et al.*, 2012); hence, we adopted this instrument to collect evidence about the quality and effectiveness of the proposed drivers. We strictly followed the three-step process for surveys defined in (WOHLIN *et al.*, 2012): survey design, execution, and analysis of results. Concerning the survey design, we paid particular attention to its protocol to ensure repeatability. Specifically, this protocol established three questions regarding the experience of experts, such as:

- *QE1: What role describes you best?*
- *QE2: How would you rate your experience with reference/enterprise architectures?*
- *QE3: How would you rate your experience with Industry 4.0?*

and three questions regarding the architecture drivers:

- *Q1: Is the architecture driver properly defined according to the Industry 4.0 context?*;
- *Q2: What must be improved in the architecture driver?*
- *Q3: Which architecture drivers are still missing?*

We adopted a self-administered, cross-sectional, exploratory survey (MOLLÉRI; PETERSEN; MENDES, 2016). As it was self-administered, the respondents answered in writing a set of questions; as it was cross-sectional, we gathered a snapshot in time, as this survey gave us an idea of how things were for our respondents at present; and finally, it was exploratory, we focused on taking advantage of the respondents' experience.

Regarding the survey execution, we invited eleven high-qualified experts who were carefully selected according to their experience and direct involvement in projects of Industry 4.0, in particular, from international companies related to electronics, automation, robotics, energy, heavy electrical, and automation technology. We contacted them with an email that contained information about the survey itself. The complete survey sent to the experts is available in Appendix B. The survey contained three questions related to the experts' professional profile, two questions (Q1 to Q2) for each architecture driver, totaling 12 questions, as well as question Q3.

Analysis and synthesis of results

We analyzed the answers of the eleven respondents, who took an average of 22 minutes to answer the questionnaire. Concerning the *Roles and experience of the respondents in projects*

regarding Industry 4.0, most participants (8) had at least three years of experience with projects related to Industry 4.0, in roles, such as software architect (3), software engineer (6), project manager (2), researcher (2), and quality manager (1). Therefore, our respondents are well experienced in different roles in software projects and even as researchers in the area.

Regarding **Q1**, the respondents used a scale for each driver: (i) *FULL Driver Integrity*[6]: The driver is approved and properly well defined; (ii) *LARGE Driver Integrity*: The driver is approved, but requires refinement or elaboration; (iii) *PARTIAL Driver Integrity*: The driver can be approved to some extent, but there are parts of the driver that need further refinement; and (iv) *NO Driver Integrity*: The driver is not well represented and must be redone.

Figure 9 summarizes the answers from the experts and shows that most drivers were approved concerning their structure and context. In particular, *Authentication*, *Data Privacy*, *Traceability*, and *Availability* were approved by the experts, who added only some remarks to improve them. On the other hand, *Scalability* and *Data Consistency* required further refinement about the environment, stimulus, responses, quantification, and specific details related to real-world use case scenarios of Industry 4.0.

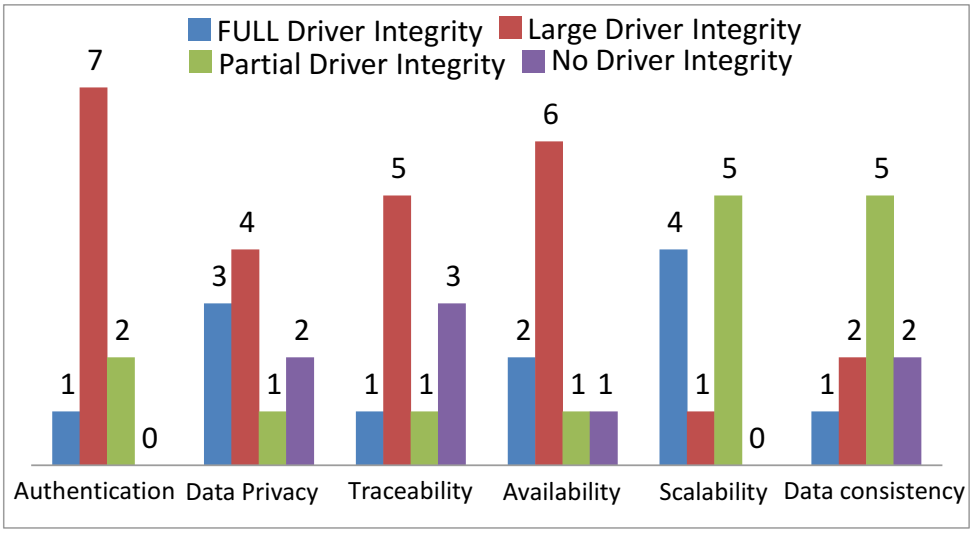

Figure 9 – Number of respondents that graded each architecture drive

For **Q2**, the respondents included important input (in textual format) for improving each driver. To analyze these texts, we conducted a qualitative analysis based on coding, which is a technique for preparing data to be analyzed quantitatively (SEAMAN, 2008). Coding makes it possible to systematically review data collected in textual-format and tag it with codes grouped into categories. Using this technique, 17 codes and four categories were collected[7], as shown in Table 2. Improvements related to the driver definition resulted in the following categories: *Driver inconsistent* (meaning it must be redone), *Environment*, *New driver* (meaning a new driver must

[6] We kept the term "Driver Integrity" as originally proposed (KNODEL; NAAB, 2016).
[7] We performed the coding using (http://www.maxqda.com).

be created), and *Quantification*. This qualitative analysis enabled a systematic analysis regarding the improvement of each driver as discussed below:

Table 2 – Categories and codes for improving the architecture drivers

Category	**Code**
Driver inconsistent	(C1) Driver does not represent the concept of consistency (C2) Driver does not represent the quality aspect concern
Environment	(C3) Details about scalability are missing (C4) Be more specific on the status of the application (C5) Give more specific details about Industry 4.0 (C6) Describe better how users/objects are logged into system (C7) Traceability needs more details related to the environment
New driver	(C8) New driver for Privacy must be regarding laws
Quantification	(C9) Be more specific on the quantification of connections (C10) Be more specific about quantification related to time (C11)Be more specific about the number of sessions per object (C12) Be more specific about quantification in authentication (C13) Give more details about who can change the production (C14) Give more details about the availability of system (C15) Be more specific regarding quantification for traceability (C16) Use dedicated metrics like availability in % (C17) User can login without restrictions in performance

- **Authentication:** This driver was approved by 8 (of 11) experts, and they suggested some improvements regarding the field *Environment*, *Quantification* and *Stimulus*. According to the experts, the *environment* field should be refined with more details to cope with Industry 4.0 concepts. Code C5, literally reported as *"...What is I40 specific here?"* and *"more complete description of the context is missing"*, represents the expert' concerns about the lack of particular information about Industry 4.0. Codes related to category *Quantification* (C10 and C12) suggest using the a metric for a generic authentication scenario.

- **Availability:** This driver was approved by 8 (of 11) experts. In summary, the experts pointed out the need to improve the fields *Environment*, *Stimulus*, *Response*, as well as the description of Industry 4.0 and technical details, such as pointed out in *..." you need to specify the operating conditions which might vary; e.g., desert vs Amazonas rain"* and *... it's missing at least a link with another driver which will describe the approach(es) how to proceed with the restoring of the system..*". The experts recommended defining a metric for the field *Quantification* as identified in code C16. Also, they suggested splitting this driver into *Availability of Physical Devices* and *Availability of Data*, because these two concerns (physical devices and data), although related, should be explicitly treated due to their relevance to together enable trustworthy interoperability.

- **Consistency:** The experts recognized the importance of this driver, but claimed that data consistency could be solved through *Authentication*, *Data Privacy*, and *Traceability* drivers.

For this reason, they suggested removing this driver. Two codes identified for this driver (C1 and C5) codify the main concerns regarding this driver. Some fragments of the experts' comments are *"I'm not sure if I understood the context Consistency of data and who save the data"*, *"This driver does not make sense to me. Why is it named consistency?, ... Save data is not sufficient description"*, and *"...what is the concrete system set-up to keep tracking data"*.

- **Traceability:** The main concerns related to this driver are its description and details about Industry 4.0, as pointed out in code C5. Besides, the respondents also called for better clarification of the field *Response* by providing more details related to traceability (code C15). For the field *Quantification*, they suggested defining many users for changing each procedure/recipe (code C13).

- **Data Privacy:** This driver was approved by 7 (of 11) experts. They pointed out improvements to the driver's name, as in *"In my opinion, it's not about privacy but instead "Data Access Control"* and *"In my understanding, the naming of this driver is not correct."*. They also suggested splitting this driver into two, creating a new one dedicated exclusively to the legal aspect of Data Privacy. Their concerns about this new driver included: *"Data Privacy is about technical aspect, but very important is the legal aspects (laws and so on) are also addressed."* and *"driver content is not only / not directly related to data privacy..."*.

- **Scalability:** The experts stressed the importance of this driver because it makes it possible to scale the production lines in smart factories; however, they claimed scalability is not directly related to data storage or transmission and therefore not related to the promotion of trustworthy interoperability in Industry 4.0. For this reason, they recommended the removal of this driver.

Concerning **Q3**, the experts pointed out that two new drivers should be created:

- Driver *Social Trust*: This driver should describe the trust in human behavior concerning data misuse and corruption by people involved;

- Driver *Compatibility*: This driver was suggested to be created as Industry 4.0 systems should be compatible with and adaptable to new elements (e.g., new products to be built, new production lines, new devices in the production lines, and new software systems). This driver describes the need for the system to be prepared for some extension and should have some intelligent mechanism to change the facilities, according to semantic and syntactic protocols. The implementation of a solution for a compatibility driver must count on the agreement of all partners involved in the production line.

After analysis of both drivers, we decided to create the driver *Compatibility* (later renamed into *Compatibility of Data and Services*) and not to include the driver *Social Trust*. Compatibility is relevant for achieving trustworthy interoperability in Industry 4.0, while social

trust is beyond the scope of this work because we are considering interoperability among entities (virtual and physical entities of a smart factory and companies); hence, social trust should be examined in other research addressing psychological issues. Besides, human operations are also important assets from Industry 4.0, however, they were not considered on this analysis due to the fact we are focusing on qualitative requirements regarding interoperability.

3.3 Architecture drivers for trustworthy interoperability in Industry 4.0

Supported by the results of our SLR and our survey, and with knowledge about Industry 4.0 from our research group, we reached a valuable set of seven architecture drivers to promote trust in interoperability in Industry 4.0.

The first architecture driver – *Authentication to the System*, shown in Table 3 – must be implemented in Industry 4.0 to provide secure access to the whole manufacturing system. This driver describes the process of confirming and ensuring the identification of users and devices. In this case, as described in the field *Environment*, we assume that there are applications installed on the system with an authentication solution already implemented. There are many devices, servers, gateways, and stakeholders that require authentication to the system. The application is an ever-changing system and needs to have an efficient way to support the addition and removal of new devices. Besides, digital twins, which represent a digital copy of the production line including functionality, operational process, and data flow among different objects, exist in the production line and must also authenticate in the system. A central authority for key signing might not be the most appropriate way. Therefore, devices need to authenticate to the application and get credential token keys during authentication. Responses describe the system verifies the credentials preventing unauthenticated access. Server authenticates devices and users by comparing a pair of authentication keys.

Table 3 – Driver *Authentication to the system*

Authentication to the System	**Quantification**
Environment: There is an ever-changing system that needs to efficiently support the addition and removal of new devices. External entities (users and devices) can join or leave the system anytime.	Entities >0
Stimulus: An external entity presents credentials to access the system.	Credential keys !=NULL
Response: The system verifies the credentials preventing unauthenticated access.	Pair of credential keys= TRUE

The driver *Data Access Control* (Table 4) refers to privileges that a user is given over large-scale data, which avoids the situation that sensitive data is shared without appropriate au-

thorization. Many different stakeholders and devices have distinct access rights to the production line that must be managed properly, (i.e., access control based on stakeholders' roles or devices and machinery attributes).

Table 4 – Driver *Data access control*

Data Access Control	**Quantification**
Environment: Multiple devices, users and authorized external entities (users and devices) can access the system. Arbitrary transactions between objects are possible.	Entities >0
Stimulus: An external entity sends a request to the control heating system for granting permission of access to modify the temperature parameters from a sensor.	Permission rights !=NULL
Response: The system verifies the grant permission to grant access to authorized entities to modify data.	If (Permission rights = TRUE) than modify.

The driver *Data Privacy to Protect Sensitive Information* (Table 5) addresses the data anonymization of entities that have contracts to deal with privacy-specific legal regulations to produce products in a production line. In a PaaS scenario, potential customers need to be able to access certain data, e.g., the status of their current product. However, they must not access data of products from other customers.

Table 5 – Driver *Data privacy to protect sensitive information*

Data Privacy to Protect Sensitive Information	**Quantification**
Environment: Internal and external entities (systems, users and devices) are interconnected and communicating in a transparent manner.	Entities >0.
Stimulus: A manufacturer requires the transmission of sensitive data related to the profitable values that is under jurisdiction protection through the system.	Sensitive data != NULL.
Response: The system protects the sensitive data and grants access only for authorized users.	If (grant permission = TRUE AND UserID = TRUE AND end-to-end encryption = TRUE) then access data.

The driver *Traceability and auditability of data* (Table 6) describes the ability to track data and support an audit trail in case of a malicious attack. This driver covers the traceability aspect by tracking what was changed and in what way (i.e., device configuration, tools, etc), and the auditability aspect by recording who initiated the changes, the autonomous decision engine, and the plant engine. This driver provides a response mechanism to record every step in a process chain, from raw material to the final product, improving quality and audit readiness throughout the lifecycle, and allowing managers to make rational decisions to isolate faulty parts. This driver also covers the aspect of data immutability, because it takes the current data and links to the previous data creating a chain of information.

Table 6 – Driver *Traceability and auditability of data*

Traceability and Auditability of Data	Quantification
Environment: Several entities (sensors, systems, devices, users, and industrial plants) are interconnected. Arbitrary transactions between objects are possible.	Transactions != NULL.
Stimulus: The plant engineer and an autonomous decision engine initiate the production of a product.	New timestamp != old timestamp
Response: The system records each step of the product production, including what was changed, in which way, and who made the changes.	Current step of production != previous step of production

The driver *Availability of Physical Devices* (Table 7) deals with all relevant information being accessible in real-time. This is usually achieved through physical data redundancy; when an unexpected event happens, the other replicas can still deliver the information. For Industry 4.0, where many plants are interconnected, replication requires decentralized mechanisms to verify that other devices are available to deliver the required information. In this scenario, a product's workpiece status shall be retrieved from its digital copy, which must calculate the capacity to process the production of the product's workpiece stopped by the failure.

Table 7 – Driver *Availability of physical devices*

Availability of Physical Devices	Quantification
Environment: There is an ever-changing system that needs to efficiently support the addition and removal of new devices. The production line is working with at least one product scheduled.	Devices >0. Products scheduled >0.
Stimulus: An unexpected event happens and turns off the main device.	Error alert >0.
Response: The system emits an alert related to the device with defects. The system send the error by message for the responsible stakeholder.	Complete workpiece=0. Process P=producing. Reschedules= 1

Another driver related to availability is *Availability of Data* (Table 8), which describes that manufacturers shall document production line records and logs for a minimum period according to the current obligations in the manufacturing domain. This data must be available upon request from sponsors or for auditability verification. Therefore, provisions must be made in the system for not deleting original data and for retaining information related to changes made to the original data.

The driver *Compatibility of Data and Services* (Table 9) describes the ability to scale Industry 4.0 production when a new external device is added to the structure of a manufacturing system and some new suppliers provide services, many of which may be legacy or rely on a diverse set of technologies and communication structures. This driver describes the scenario when compatibility is required to connect, translate, and use information across different machines in a

Table 8 – Driver *Availability of data*

Availability of Data	Quantification
Environment: Several entities (sensors, systems, devices, users, and industrial plants) are interconnected. Arbitrary transactions between objects are possible. All data from the production line is stored.	Data !=NULL
Stimulus: External system requests access to the database to collect information from two sensors (i.e. temperature and bomb pressure) at a specific date and time.	Timestamp != NULL.
Response: Data is retrieved from the database according to specific date and time inputs.	If (grant permission = TRUE AND UserID = true AND end-to-end encryption = true) then access data

current Industry 4.0 system. As a response, this system supports these new nodes integrating them into a unified enterprise architecture layer, which allows more compatibility and maximization of Industry 4.0. This maximization is possible due to common protocols for vertical integration (i.e., machine to machine communication on the shop floor) and also horizontal integration(e.g., cloud to device) across all layers. Besides, all entities must be addressable (e.g., via TCP/UDP, IP, MAC address, or IDs) to allow one-to-many and bi-directional communication among them.

Table 9 – Driver *Compatibility of data and services*

Compatibility of Data and Services	Quantification
Environment: The production line is working with at least one product scheduled. Many devices offering several capabilities must exchange data . Digital twins exist for each object	Product scheduled >0. Digital copy = Number of the entity.
Stimulus:An external device is added to the manufacturing system.	Device ID parameter != NULL.
Response: The system integrates the new device in the system with its identification parameter accordingly to common standards and protocols for communication.	New entity value = new digital copy value. Devices are addressable.

3.4 Main findings and limitations

The architecture drivers proposed in this work are the first step towards designing proper solutions to enable trust in interoperability in the context of Industry 4.0. An example of the application of the proposed driving factors can be seen at one of the partners of the BaSyS 4.0 project in the digitalization of an automated transport system to move a workpiece forward and backward (ANTONINO *et al.*, 2019). This transport system includes roller conveyors, shift tables, and turntables. Many sensors are controlling the speed, temperature, position, and shift of the workpiece. Sensors, devices, and applications are interconnected and need

to interoperate with some systems and users inside and outside the production line. These competitive interests from different companies require a trustworthy infrastructure, which can be implemented by considering the seven architecture drivers proposed in this work. Regarding the driver *Authentication to the System*, experts must be aware that innumerable types of devices, machinery, sensors, systems, digital twins, and users must authenticate to the system. The authentication of these objects must be designed in a secure and decentralized way, where the authentication control must recognize the dynamic scenario of ever-changing devices, with systems and components from numerous manufacturers. This specific example also affects the driver *Data Access Control*, which must be implemented transparently to help manufacturers recognize the right access of each component and user. The driver *Data Privacy to Protect Sensitive Information* is closely related to the driver *Data Access Control* and must consider the privacy right of each manufacturer when they mark their data as anonymous or private or accessible for only some devices and users. This characteristic is important in Industry 4.0 to enable manufacturers to schedule a private production plan only for authorized users. Another important architecture driver to be considered is *Traceability and Auditability of Data*, as in the scenario described above, the transport system is arranged into multiple lines to produce specific workpieces according to manufacturers' specifications. The transport control system tracks the status of real-time data and makes it available for all users and devices in the chain. Regarding the drivers *Availability of Data* and *Availability of Physical Devices*, a control system must exist to recognize the status of each workpiece and the real-time data from each sensor and device. The system then automatically calculates any disruption and emits an alert when a failure occurs due to lack of availability of data or devices and calculates a new transport route if the current route is no longer valid. The diver *Compatibility of Data and Service* describes the need for the system to be prepared for some extension, accordingly to semantic and syntactic protocols. The implementation of the solution for compatibility driver must count on a communication channel for Industry 4.0 applications and digital twins of many entities of the production process. The assumption must encompass that each element connected in the communication channel are typed and have well-defined properties for each object.

The main finding of this work is that considering only one quality aspect, such as security or privacy, or even a set of them (without an analysis), cannot assure trustworthy interoperability in Industry 4.0. In fact, it is necessary to jointly consider seven specific quality concerns, or drivers (namely *Authentication to the System*, *Data Access Control*, *Data Privacy to Protect Sensitive Information*, *Traceability and Auditability of Data*, *Availability of Physical Devices*, *Availability of Data*, and *Compatibility of Data and Services*). Hence, for instance, if failures occur in the production line containing several virtual and physical entities interconnected, manufactures can access traced data records if the *Traceability and Auditability of Data* was implemented. This increases trust by empowering the manufacturers and stakeholders involved to have more control over their production line, by clarifying issues, and by preparing them for the further evolution of their production lines.

Another finding is that representing the seven quality concerns using architecture drivers has benefits. This is because by definition: (i) architecture drivers delineate only the significant requirements (and information related to them) needed to implement and maintain software-intensive systems, which in our case refers to Industry 4.0 systems; (ii) a set of architecture drivers for a given purpose must not overlap in terms of content (i.e., there must be no redundant information) and, at the same time, each one must be self-contained (making it also possible for each one to be used independently without the obligation to adopt others); (iii) architecture drivers make it possible to avoid costly and risky decisions; (v) by nature, architecture drivers must be presented at a higher level of abstraction; and (iv) they can often determine the success or failure of projects. Hence, we recommend the adoption of architecture drivers as a first key step for developing large, complex software-intensive systems, such as systems-of-systems and ultra-large-scale systems.

It is worth highlighting that the drivers defined in this work do not consider malicious attacks made by users who are authenticated in Industry 4.0 systems. Besides, the social and cultural aspects of trust in terms of human behavior are not addressed in this work because these must embrace principles regarding human resources management, which encompasses many psychological concerns related to identifying whether a person is reliable or not when it comes to working reliably in a manufacturing environment.

Moreover, as stated above, by nature, architecture drivers are artifacts at a higher level of abstraction in the context of software/systems development processes. Hence, these drivers should be refined for specific cases, for instance, a given production plan of an automotive manufacturer.

Finally, the architecture drivers proposed in this work can be considered a first key step towards designing architectural solutions with trustworthy interoperability in Industry 4.0. Benefiting from the openness of these drivers, different techniques and approaches (many of them already proposed in the literature and/or being used in practice) could be selected, analyzed, and chosen.

For instance, the field *Quantification* of the driver *Authentication to the System* states that the authentication token must not be null. One possible solution for this driver is the use of certification authorities combined with a Public Key Infrastructure (PKI). A certification authority represents a trusted third party that supports multiple security services, such as data access control requests or PKI digital signature. There are also many possibilities for this solution, such as identity verification and increasing the security and confidentiality of online transactions. Another example is the driver *Data Access Control*, which demands that stakeholders must have distinct access rights to the system. One solution for that is to use an ACL to determine the privileges of users or devices. An ACL specifies the access rights allowed, denied, or audited for that trustee's access to a securable object according to roles or specific attributes defined in advance. This solution assumes only one login per user/plant and requires the definition of

a maximum transfer rate according to the application domain. In summary, one advantage of architecture drivers is that they can provide important support for architecture design because they can lead to good design decisions and, as a consequence, the success of industry projects.

This work (in particular, the results of the SLR and the survey) might have been affected by some threats to validity. Concerning **construct validity**, when we conducted our SLR, we minimized the threats to this validity by systematically following the specific guidelines proposed in (KITCHENHAM; CHARTERS, 2007). Besides, the keywords used in the search string were tested in Scopus to make it possible to collect all relevant studies; for instance, using the search string *(“Industry 4.0" AND “Interoperability" AND “trust")*, no relevant studies were found; hence, we adopted a more open string involving terms related to “Industry 4.0" and “Interoperability". For our survey, we minimized threats to this validity by designing a focused, multiple-choice questionnaire with a text field for the respondents to add extra information. We also thoroughly chose representative respondents, which assured us that we got relevant answers from industrial practitioners.

Regarding **internal validity**, to ensure that the SLR was complete and no important study was missed, we used five publication databases, including all those recommended for software engineering. Another threat refers to the selection of primary studies. To minimize this threat, the selection process was carried out by one researcher and continually reviewed by others, together with the application of the inclusion and exclusion criteria. One threat to internal validity in our survey is that the respondents might have misunderstood the questions. Hence, before distributing the survey, each question was reviewed by two experts from Industry 4.0 and the field of software architecture.

The **conclusion validity** is related to the ability to draw correct conclusions. To mitigate threats to this validity during our SLR, we applied a data extraction process based on the specific guidelines found in (KITCHENHAM; CHARTERS, 2007). Concerning the survey, our conclusions are based on information provided by respondents in an online questionnaire, which might reflect beliefs rather than real facts. We mitigated this threat by inviting only experts directly involved in Industry 4.0 projects. Another threat is the small number of respondents of our survey; as we aimed at considering their answers valid for a wider population, we only invited practitioners with deep knowledge of industrial projects, including Industry 4.0 projects.

3.5 Final considerations

Trustworthy interoperability in different levels, from technical to organizational and also vertical and horizontal interoperability, is crucial to set up Industry 4.0. This chapter contributed to the essential requirements that should be considered for the implementation of Industry 4.0 systems with trustworthy interoperability. Represented in the format of architecture drivers, these requirements are regarding seven issues, namely authentication to the system, data access control,

privacy control to protected sensitive information, data traceability and auditability, physical devices availability, data availability, and data and services compatibility. We also recommend all these drivers must be jointly considered to achieve trust in the interoperability in Industry 4.0 systems.

CHAPTER

4

ARCHITECTURE SOLUTIONS

"When electioneering I trust
I can rely on your vote
When I go forwards,
you go backwards
And somewhere we will meet"

Thom Yorke

4.1 Initial consideration

Industry 4.0 is a concept related to the new industrial revolution for improving the way modern factories will work. Trustworthy interoperability among manufacturers is one of the most important concerns for the success of Industry 4.0. Several research initiatives and technical solutions, including blockchain, have tried to solve the problems related to trustworthy interoperability. However, little is known about the actual impact of blockchain technology on regarding provide trust to interoperability. Thus, this chapter presents seven architectural solutions to properly solve the architecture drivers previously established (i.e., Authentication to the System, Data Access Control, Data Privacy to Protect Sensitive Information, Traceability and Auditability of Data, Availability of Physical Devices, Availability of Data, and Compatibility of Data and Services). To define these solutions, we conducted interviews with experts from Industry 4.0 and experts in the blockchain.

4.2 Architecture solution design

The main objective of this chapter is to present the steps performed to define solutions for the architecture drivers previously defined. Thus, we performed a survey by conducting interviews with experts in projects regarding Industry 4.0. It is worth highlighting that this

survey was a type of qualitative research (SEAMAN, 2008) widely applied as a valuable means to methodologically gather opinions (WOHLIN *et al.*, 2012; RUNESON; HÖST, 2009). The planning and execution of the survey as well as the analysis of results are presented in this chapter.

4.2.1 Planning

To conduct our survey, we systematically followed the steps proposed in (WOHLIN *et al.*, 2012; RUNESON; HÖST, 2009) to guarantee the validity of the results. Thus, a survey protocol was created containing: (i) the main objective; (ii) the design decisions; (iii) the procedures for carrying the survey.

i) The main objective: The main objective of this survey was to collect evidence on the capability of blockchain to be a solution for each architecture driver.

ii) The design decisions: To conduct the survey, we decided to use semi-structured interviews (WOHLIN *et al.*, 2012). This type of interview is open in the sense that they allowed new ideas to be brought up during the interview. Besides, we decided to conduct the interviews face to face with each expert and record the data in audio. Besides, we created a package of documentation including two forms: i) a consent term to get authorization for recording the interview in an audio device application, and ii) documentation containing the seven architecture drivers and proposed solutions for each driver. The documentation package is presented in Appendix C. Also, we defined two main questions to be asked during the interviews:

- *Q1: Can blockchain be considered a solution for realizing each architecture driver?*
- *Q2: Which are the solutions combined (or not) with blockchain to solve each architecture driver?*

iii) The procedures for carrying the survey: Considering that the institution (Fraunhofer IESE) where we developed this work is involved in Industry 4.0 projects, we had the opportunity to select and invite eight experts working in Industry 4.0 projects; two of them are also experts in the blockchain. The participants had at least three years of experience with Industry 4.0 projects, in roles like software engineer (5 experts), software architect (2), project manager(2), researcher (2), and quality manager (1). Therefore, our respondents were well-experienced in one or more roles in software projects, which gives confidence to their answers.

4.2.2 Execution

In each interview conducted individually with each expert, an explanation about the research being conducted, including details of each architecture driver, was provided. After we had asked our questions, the interviewees were free to ask, discuss, and share their experience

from real-world Industry 4.0 projects. When an expert did not agree that blockchain could be a proper solution for a given driver, the interviewer asked for other solutions that could cover that driver and how these could be combined with blockchain, if possible. Each interview took around 60 minutes, totaling 9hours and 20 minutes of audio during the step *"Record interviews in audio"*, as shown in Figure 10, which summarizes the steps we took to conduct the execution and analyze the results.

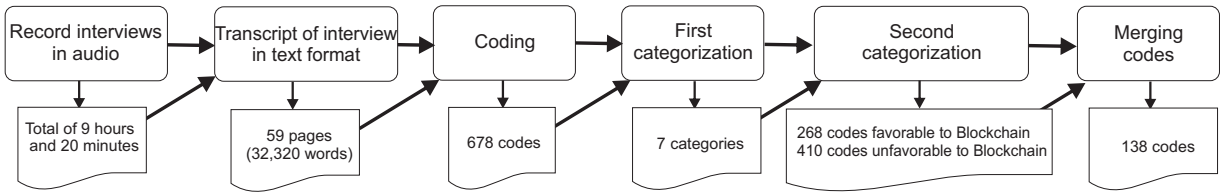

Figure 10 – Process for performing the qualitative analysis

4.2.3 Analysis of results

To systematically analyze the information collected from interviews, we used Grounded Theory (SEAMAN, 2008; STRAUSS; CORBIN, 1998), which encompasses two techniques (STRAUSS; CORBIN, 1998): (i) *open coding* identifies codes that are separated into discrete parts for analysis; and (ii) *axial coding* handles connections between codes and groups them according to their similarities. We used the QDA Miner tool[1] to support the analysis using these techniques. As also showed in Figure 10, we performed the following steps in this analysis:

- **Transcript of interview in text format:** The eight interviews (referred to as I1 to I8) were transcribed into a 59-page text document (32,320 words) for further analysis[2].
- **Coding:** Using *open coding*, we identified codes and assigned them to the pieces of text based on the similarity found in such texts. Figure 11 depicts an example of pieces of text assigned to different codes that were identified using the QDA Miner tool. More specifically, we first looked at the text from interview I1 and identified 24 codes related to the driver *Authentication to the System*. For instance, from the pieces of text *"I am not sure if a blockchain-based concept will have any benefit"* and *"...maybe this majority vote could fix this, but, who will decide"*, which were said in I1, we identified the codes *"Blockchain does not bring benefits"* and *"Majority vote is a drawback"*, respectively. We used these codes as a first set to code the interviews of the other respondents, considering the part of the interviews related to this driver. When new codes were identified, they were included in this set. In the end, we found 125 codes only for this driver. We repeated this same process for each architecture driver, which resulted in a total of 678 codes. Table 10 lists the number of codes found for each interview and each driver.

[1] <https://provalisresearch.com>

[2] Due to the confidentiality that interviewees need to keep when participating in industry projects, the full transcript cannot be available publicly, but we make part of it available when necessary for the comprehension of this work.

- **First categorization of codes:** The next step was to find a categorization for the codes. As our transcript was divided into seven architecture drivers, we used this division to create seven categories: *Authentication to the System* (125 codes), *Data Access Control* (90 codes), *Data Privacy to Protect Sensitive Information* (111 codes), *Traceability and Auditability of Data* (106 codes), *Availability of Data* (97 codes), *Availability of Physical Devices* (74 codes), and *Compatibility of Data and Services* (75 codes).

- **Second categorization of codes:** We also defined two broder categories *("Blockchain may be a good solution" and "Blockchain may not be a good solution")*, which were the main theme of interest during the analysis. Next, we read the entire transcript again, and, considering the 678 codes and the seven categories previously found, we categorized these codes into these two new categories. Due to space limitations, we present only a few examples of the pros and cons of blockchain for the driver *Authentication to the System (AS)*:

  - **Pros of using blockchain:** The experts pointed out benefits of blockchain for this driver; hence, the following codes were classified into the category favorable for blockchain:

    – *"AS.7. Blockchain brings trust because it is a distributed system"*: The experts affirmed that a decentralized infrastructure would bring more security and reliability for dealing with sensitive and critical data;

    – *"AS.1. Blockchain and public-key infrastructure (PKI) can bring security"*: Blockchain relies on cryptography infrastructure such as PKI, which brings more security for exchanging data; and

    – *"AS.12. Blockchain can help to bring transparency in the whole chain"*: We found that blockchain would bring more transparency and freedom for manufacturers to deal with data. Also, it would bring the ability to automatically define and have change-protected smart contracts for production settings.

  - **Cons of using blockchain:** The experts pointed out concerns in adopting blockchain for this driver and provided important feedback, such as:

    – *"AS.5. The blockchain majority vote is difficult to be applied"* and *"AS.19. Blockchain majority vote works if there are rewards"*: These codes describe the concern regarding the use of majority vote, which corresponds to agreed votes from each manufacturer to modify behavior or data inside the blockchain;

    – *"AS.18. Blockchain trade-off is to validate each block in a fast, accurate way with a consensus algorithm"*: The consensus mechanisms describe the agreement among all nodes of the blockchain and can be achieved by implementing a proof of work or proof of stake. In the proof of work, miners are rewarded by solving complex formula equations. In the proof of stake, it is based on the number of coins a person has to mine the block to get a reward (Yang *et al.*, 2019); and

  - *"AS.2. Blockchain is a risk if you lost the identity keys"* and *"AS.8. Blockchain needs to be combined with a central authority"*: These codes describe security concerns in case credential identities are lost. In a blockchain, it is really hard to recover lost IDs.

As a result of this categorization, 268 codes were categorized into *"Blockchain may be a good solution"* and 410 codes into *"Blockchain may not be a good solution"*.

- **Merging codes:** We analyzed the codes found for each driver to find similarities among them and merged those with the same meaning. For instance, once again considering *Authentication to the System*, the codes *"AS.16. Blockchain is not mature for authentication"* and *"AS.27. There is still the need for more evaluation of blockchain"* are similar, so we merged them into the code *"AS.16. Blockchain is not mature technology for authentication"*. Analyzing all 125 codes related to this driver, we found 23 unique codes, of which 12 were in the category "Blockchain may be a good solution", while 11 were in the category "Blockchain may not be a good solution". Table 10 (last column) summarizes the number of unique codes for each driver[3].

Figure 12 shows the number of codes that are favorable, respectively unfavorable, for adopting blockchain for each architecture driver. While blockchain could be beneficial for the drivers *Data Access Control* and *Traceability and Auditability of Data*, it could not support *Availability of Data*, *Availability of Physical Devices* and *Compatibility of Data and Services*. The other two drivers had balanced opinions. For each driver, we also developed an analysis to understand the reasons for these results.

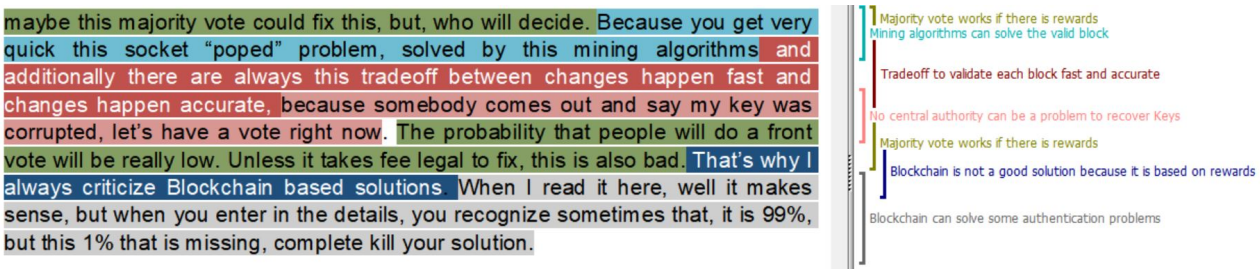

Figure 11 – Example of pieces of text (left side) from interview I1 when talking about the driver Authentication to the System and codes identified with the QDA Miner tool (right side)

During the coding and the qualitative analysis, we also collected all directions for defining solutions for each architecture driver. For instance, considering the driver *Authentication to the System*, we analyzed each expert's statement, such as *"Maximum security is achieved with blockchain encryption, supporting certified device and users to connect to the production line network."* This was said in interview I2 and pointed out to the adoption of blockchain. This statement enabled us to connect it to another statement in favor of blockchain: *"Blockchain is for distributed systems and ensures no centralized point of failures"*, which was claimed

[3] All codes are listed in <https://tinyurl.com/y986xgz7>

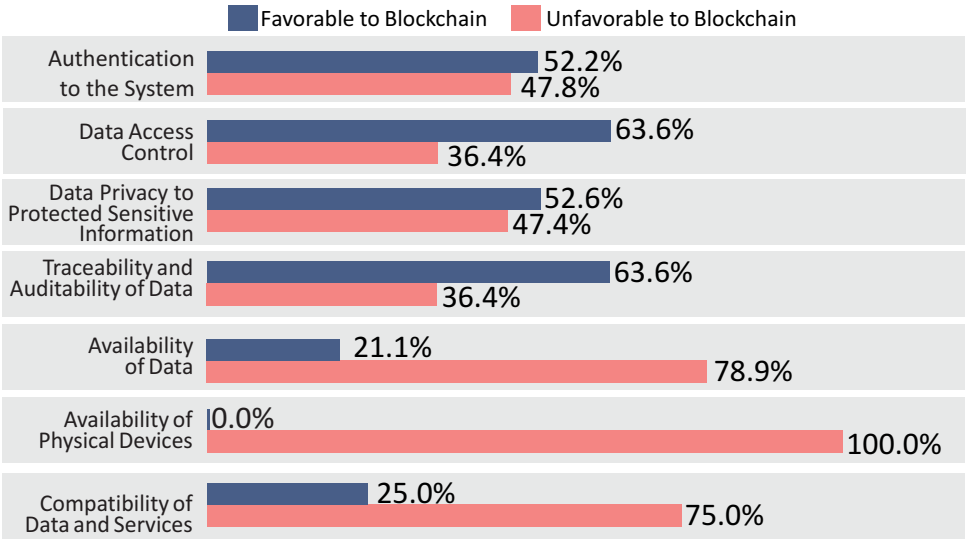

Figure 12 – Experts' opinion regarding adoption of blockchain

Table 10 – Number of codes identified using open coding

Drivers	Interviews								Subtotal of codes	Subtotal of unique codes
	I1	I2	I3	I4	I5	I6	I7	I8		
Authentication to the System	24	18	15	12	13	13	15	15	125	23
Data Access Control	13	15	10	7	9	7	9	20	90	22
Data Privacy to Protect Sensitive Information	17	23	10	13	10	13	8	17	111	19
Traceability and Auditability of Data	15	19	12	11	9	8	9	23	106	22
Availability of Data	16	18	8	10	11	9	6	19	97	19
Availability of Physical Devices	10	10	4	12	6	5	8	19	74	17
Compatibility of Data and Services	10	15	8	4	7	7	7	17	75	16

in interview I8. Another example is the statement *"So, from the security point of view, I am not sure if a blockchain-based concept will have any benefit so only thinking on the security perspective in contrast to a central authority."*, which was said in interview I1 and was against the adoption of blockchain. Another statement against blockchain was *"Especially in security, there are a lot of solutions, such as PKI. So if you use blockchain, you are going to use PKI anyway, so why blockchain? Why not just public key?"*, which was said in interview I2. Both interviews presented concerns about blockchain and the security aspect behind it. Besides, the experts claimed that combining blockchain with traditional authentication servers could provide great benefits for interoperability in Industry 4.0, such as more transparency in the whole chain, better synchronization among participants, flexibility regarding the authentication of distributed systems, and support for compliance with regulations through the implementation of rules in smart contracts.

The analysis used to identify solutions for the other drivers (*Data Access Control*, *Data Privacy to Protect Sensitive Information*, *Traceability and Auditability of Data*, *Availability of Data*, *Availability of Physical Devices*, and *Compatibility of Data and Services*) followed the same procedure as that for *Authentication to the System*. In the context of this work, these solutions refer to claims and assertions made by experts that can be further used for the architecture design and can also be represented by any model or notation (KNODEL; NAAB, 2016), i.e., they do

not refer to models documenting a software architecture solution. In turn, these solutions are represented in terms of (i) favorable or unfavorable for blockchain; (ii) pros or cons of adopting blockchain and associated challenges; (iii) cons, risks, and trade-offs of adopting the solution; and (iv) alternative or complementary technologies. The resulting solutions related to each driver are detailed in the next section.

4.3 Architecture solutions for trustworthy interoperability in Industry 4.0

Seven solutions were established to achieve trustworthy interoperability in Industry 4.0 described as follows:

Authentication to the System

This driver describes the scenario where there is an ever-changing system that needs to support the addition and removal of new devices, users, systems, digital twins, and other entities efficiently and transparently. **Favorable to blockchain:** According to experts, blockchain may be a solution for this driver because entities (i.e., users, devices, machinery, systems) can have more control over their own identity without the need to trust a third party or any centralized authority. Besides, it guarantees non-discriminatory access to a marketplace operated by a player (e.g., Amazon or eBay). Such players can mediate production orders and enable automated agreement on smart contracts for producing goods. Partners who sign in would participate in the revenues (this would be analogous to Bitcoin). **Challenges for adopting blockchain:** The main challenge is the high cost for smaller companies to modify their existing systems as well as the need to create policies that fulfill the security requirements of all partners. **Cons** & **risks**: The main risk is that partners of a private blockchain may face disagreement if they choose to deploy changes unilaterally. **Alternatives:** There are other solutions for authentication to systems, such as federated identity, certificate authorities, PKI, and protocols, such as OAuth 2.0[4], OpenID[5], or multi-factor authentication (id, password, PIN, email account, token device, and fingerprint). Although these alternatives are good solutions for Industry 4.0, they do not solve all issues described in this driver, which requires widespread participation and transparency over users and other connected entities, including competitor companies, that do not rely on each other but must work in the same production line. In this situation, experts recommend combining these solutions with blockchain to solve this driver.

[4] <https://oauth.net/2/>
[5] <https://openid.net/>

Data Access Control

This driver describes several entities (e.g., users, devices, and digital twins) that count on an access control system to manage authorization rights to data. This system makes it possible to protect or prevent the occurrence of illegal access and modification of data generated by several devices (e.g., data from an overheated device or data from an overcrowded pallet). **Favorable to blockchain:** Blockchain can solve the issues described in this driver by providing immutable logs of access and bringing more transparency to the system. Each entity/partner can access and audit data records without the need for a central authority. Besides, blockchain can be used to document the agreements made by partners in smart contracts regarding how the data will be used. **Challenges for adopting blockchain:** implementation of blockchain can bring challenges for Industry 4.0 companies, in particular, higher cost to change the current authorization control system and the necessity to create common policy requirements to properly define a security authorization mechanism to access the production line. **Cons** & **risks:** Risks regarding the adoption of blockchain include the vulnerabilities of smart contracts and the need for an off-chain integration database to store the access policies. **Alternatives:** Traditional access control systems, such as ACL and RBAC model that controls individuals' access to the system (Condry; Nelson, 2016; PERALTA *et al.*, 2019; Polonia; Melgarejo; de Queiroz, 2015), can also be good solutions for this driver. However, these solutions cannot solve problems regarding the presence of third parties that define the access privileges for each user, resulting in a lack of privacy. Besides that, current access control solutions are static and might be inadequate for the dynamism of Industry 4.0 systems. Hence, a combination of these solutions with blockchain is a more appropriate solution.

Data Privacy to Protect Sensitive Information

This driver describes concerns related to protecting intellectual property when information must be shared among different manufacturers in Industry 4.0. This intellectual property refers to financial data, patents, and private data from companies that are under legal protection. **Favorable to blockchain:** The experts opinions were favorable regarding the adoption of blockchain for this driver, as blockchain encrypts sensitive data and separates it into segments that can be accessed by authorized parties at any time using appropriate decryption keys. As blockchain contains a signature of bilaterally exchanged data and not the data itself, partners can check whether a contract was concluded without external parties being able to access the data. This enhances the privacy of data by replacing most identifying fields within a data record with one or more artificial identifiers. **Challenges for adopting blockchain:** The main challenge is how to guarantee data privacy in a technology that is based on the principle of transparency and immutability of data. **Cons** & **risks:** The risk of data privacy in the blockchain is related to whether identifiers keys from off-chain databases are deleted, the on-chain data will be anonymized. **Alternatives:** The current alternative for protecting data is the use of an encryption

protocol managed by a central server. However, the main drawback of traditional solutions is the necessity of a central administrator, which makes confidentiality and privacy a challenging problem. Hence, a good solution for this driver is the adoption of blockchain combined with end-to-end encryption to protect sensitive data and with the solution related to access privileges as described for the driver *Data Access Control*.

Traceability and Auditability of Data

This driver describes a scenario where the system must record every step in a process chain from raw material to the final product in an immutable way. **Favorable to blockchain:** Blockchain naturally provides a data provenance service by recording all transactions. For this reason, a private blockchain was suggested by the experts as a solution for this driver. **Challenges to adopting blockchain:** The main challenge is the dependency on a database to store data, a blockchain cannot support a large amount of data in the chain. This can increase the cost for companies if they need to hire this type of service. **Cons & risks:** The risk of adopting blockchain includes the possibility that response time to requests may increase as the number of devices increases in the production line. **Alternatives:** Current alternatives for traceability of data include the use of external services requests by assigning a unique ID. However, these traditional solutions are centralized and not all of them provide end-to-end traceability of data and tamper-resistant records to support stakeholders indecision-making. Blockchain solves the issues of data traceability but does not solve the issue of data storage. Hence, every block should include hashes pointing to the data sets stored in databases; in this way, the state of each data set can be tracked securely.

Availability of Data

Industry 4.0 systems encompass many entities (e.g., sensors, users, digital twins, and machinery) that increase the amount of data created, either through applications developed or deployed by the company, third-party systems, customers, or suppliers. This data must be available and manufacturers must document and make available data from the production line process. Representatives of the manufacturing process require verification of data related to a specific technical requirement (e.g., temperature and bombing pressure at a specific time in the production line). **Unfavorable to blockchain:** According to the experts, blockchain cannot be a good solution for this driver. Although blockchain does perfectly store the hash to data, the raw data cannot be saved in the blockchain due to performance reasons. **Alternatives:** Current solutions, such as a backup server, databases, and the use of clouds, are recommended alternatives for storing data from the production line. According to the experts, digital twins can also be used to support the availability of data because they are virtual copies of real-world entities (e.g., data flow, production machine, operational processing status, functionalities, sensors, and robots), and they can synchronize manufacturing data and functions related to the plant design. Hence,

we recommend the adoption of redundancy services, storage in the cloud, and/or backup servers to assure data availability.

Availability of Physical Devices

This driver describes the scenario where many plants are connected and must deliver the information even when a failure occurs in the system. **Unfavorable to blockchain:** According to the experts, blockchain cannot restore systems and, for this reason, it is not a good solution for this driver. **Alternatives:** The experts recommend the use of traditional technologies such as redundant servers/devices combined with digital twins. While digital twins enable the monitoring of devices identifying possible upfront failures, redundant servers and devices should exist if a nonstop production process is required. Besides, additional security for the whole production with a real-time monitoring and simulation system must be implemented, which can increase the cost to have a backup physical infrastructure. Hence, a more appropriate alternative is the use of solutions that make it possible to monitor and recover physical devices accordingly to companies' regulatory requirements.

Compatibility of Data and Services

This driver describes a scenario in which new entities from third parties are added to the current manufacturing process and must be semantically and syntactically compatible to exchange and read data. **Unfavorable to blockchain:** According to Industry 4.0 experts, blockchain cannot be used as a solution for this driver, as compatibility refers to how the systems are prepared for some extension and/or have some intelligent mechanism to facilitate changes. **Alternatives:** The experts claimed that a service-oriented middleware could provide the necessary services to enable the compatibility of systems according to semantic and syntactic protocols that must be agreed upon by the partners involved in the production line. However, they also claimed that this type of solution makes it hard to ensure real-time compliance among manufacturers' systems and physical communication. In this scenario, we recommend the adoption of solutions that check the compatibility of data and services. These solutions should provide semantic and syntactic communication protocols, allowing proper communication among heterogeneous entities.

Table 11 summarizes the solutions discussed above. Due to the openness of these solutions, different existing approaches, techniques, and technologies related to alternative solutions can be adapted to implement the set of architecture drivers. When necessary, blockchain must be combined with these solutions. It is worth highlighting that these solutions cover different, complementary aspects of trust to achieve fully interoperable Industry 4.0 systems; hence, all of them must be implemented together. At the same time, if a given aspect is desirable, a specific solution can also be implemented individually.

Table 11 – Summary of solutions for trustworthy interoperability in Industry 4.0 systems

Driver	**Reason to adopt blockchain**	**Solution**
Authentication to the System	Blockchain provides users more control over their own identity.	Combine blockchain with authentication solutions, such as federated identity, certificate authorities, PKI, and multi-factor authentication.
Data Access Control	Blockchain provides access to data without the need for a central authority.	Combine blockchain with traditional access control systems, such as ACL or RBAC, or their privileges control list.
Data Privacy to Protect Sensitive Information.	Blockchain encrypts data and separates it into segments that can be accessed by authorized parties.	Combine blockchain with end-to-end encryption to protect sensitive data and use the solution related to access privileges
Traceability and Auditability of Data	Blockchain provides unmodified access logs and brings more transparency to the system.	Blockchain should be combined with databases and include hashes pointing to the datasets stored in the databases.
Availability of Data	Blockchain is not suitable.	Implementation of services for monitoring and recovering data, including redundancy services, storage in the cloud, and backup servers.
Availability of Physical Devices	Blockchain is not suitable.	Implementation of services for monitoring and recovering physical devices according to company regulatory requirements.
Compatibility of Data and Services	Blockchain is not suitable.	Implementation of services for translating and mapping data according to semantic and syntactic protocols.

4.4 Main findings and limitations

The opinions of experts directly involved in Industry 4.0 projects regarding the adoption of blockchain as a solution for revolutionizing the interactions among entities that require a high degree of trustworthy interoperability in Industry 4.0 are still divided. At the same time, trust must be pervasive in Industry 4.0 (AL-ALI *et al.*, 2018b; Bicaku *et al.*, 2017), meaning that it must be well designed to assure that trust aspects have been properly addressed. In the next sections, we will discuss the main findings, threats to the validity of our work, and perspectives for using the solutions proposed in this work.

Achieving trustworthy interoperability in Industry 4.0 requires recognition that its systems are comprised of subsystems and physical entities, and awareness of how they interact with each other in a cross-layer Industry 4.0 environment (cf. Figure 3). Because of the distributed nature of blockchain, data can be more transparent, preventing fraudulent behavior from non-trusted parties. A private blockchain can be a solution when different parties are involved in a production line and must be well-known by the other participants. Manufacturers, suppliers, and

customers have data assurance; transactions are tracked and accessed transparently (cf. solution for *Traceability and Auditability of Data*) or can be protected by cryptography, which prevents sensitive data from being accessed by non-authorized users (cf. solution for *Data Privacy to Protect Sensitive Information*). Hence, blockchain can provide benefits for data protection through a closed private network (Anjum; Sporny; Sill, 2017). It increases *data transparency* and facilitates *data traceability* in Industry 4.0 production lines.

Blockchain increases problems related to performance as it consumes an enormous amount of energy (Christidis; Devetsikiotis, 2016); besides, it cannot store a large amount of data in the chain (Alladi *et al.*, 2019). Blockchain cannot guarantee data availability for users, but only a hash pointing to the data (HAWLITSCHEK; NOTHEISEN; TEUBNER, 2018). Hence, blockchain cannot solve the drivers *Availability of Data*, *Availability of Physical Devices*, and *Compatibility of Data and Services*.

The adoption of blockchain alone does not solve the requirements of fully trustworthy interoperability in Industry 4.0 projects. Blockchain must be combined with traditional solutions, in particular, to solve *Authentication to the System, Data Access Control, Traceability and Auditability of Data, and Data Privacy to Protect Sensitive Information*. Such combinations decrease the power of blockchain by no longer allowing a decentralized system; instead, they leave the control by a central authority. Hence, participants in the blockchain network have the assurance that the data is recorded and tracked by all participants, avoiding non-repudiation in the chain.

At the same time, using only traditional solutions, such as federated identities, OAuth 2.0, OpenID, Security Assertion Markup Language (SAML)[6] for authentication and authorization (SURESH; UDENDHRAN; BALAMURUGAN, 2020), cryptography for data privacy (Fernandez-Carames; Fraga-Lamas, 2019), backup/redundancy/duplication of data (Link *et al.*, 2018; Schulte; Colombo, 2017), and many others, cannot solve all problems related to trustworthy interoperability in Industry 4.0 systems (Fernandez-Carames; Fraga-Lamas, 2019; Link *et al.*, 2018; PERALTA *et al.*, 2019; Schulte; Colombo, 2017). In this respect, blockchain can complement these solutions by en-coding rules in smart contracts, which in turn enables records to be accessed transparently by users, ensures privacy of data through cryptography, and storage of data and transactions in a distributed ledger.

Regarding the question that drove our research — *Can blockchain solve problems related to trust in interoperability in Industry 4.0?* — we can answer that it can solve some of the problems but brings other issues that can compromise the whole cost and performance of interoperability. Hence, blockchain still needs to mature to demonstrate its potential and value in the Industry 4.0 scenario.

Finally, surveys such as the one used in our work can provide representativeness, which

[6] <https://developers.onelogin.com/saml>

increases the reliability of the results (WOHLIN *et al.*, 2012). The main advantage of surveys is the detailed information obtained from experts and their perception regarding a given topic of interest (MOLLÉRI; PETERSEN; MENDES, 2016), which, in our case, was the use of blockchain as a solution for trustworthy interoperability in Industry 4.0 systems. Moreover, the analysis of data based on coding can lead to further analysis and a broad comprehension of the data considering different experts' opinions (STRAUSS; CORBIN, 1998). The systematic process of coding allows researchers to gain a more statistical representation of theoretical opinions, which supports drawing reliable conclusions about a topic of interest (SEAMAN, 2008; WOHLIN *et al.*, 2012). Considering that we adopted these instruments (i.e., use of a survey and coding to analyze the results) as the foundation of our work, we believe that our findings are reliable.

Regarding threats to the validity of this work, the results might have been affected by the following threats. Regarding **construct validity**, this refers to whether we were able to appropriately collect the measures, i.e., the opinions of the experts interviewed in our study. To minimize this threat, we designed a focused open questionnaire for our survey. We also thoroughly chose potential interviewees to get relevant answers coming from highly trained industry experts.

The **internal validity** refers to whether the treatment used in this study made any difference in terms of achieving the results presented in this work. To mitigate this threat, we selected only experts who were directly involved in real-world Industry 4.0 projects. Also, we took care to present the documentation of the architecture drivers in the same order for all interviewers, aiming at minimizing any interference effects. The **external validity** is regarding the generalization of the results of this study. We minimized this threat by inviting experts with experience in different Industry 4.0projects.

Regarding the **conclusion validity**, this is related to the ability to draw correct conclusions from the results obtained. To mitigate this threat, we invited only experts directly involved in Industry 4.0 projects with years of experience in software development and the design of software systems. Our purpose in this work was to collect initial evidence from the experts' perspective regarding the use of blockchain in Industry 4.0 systems. However, a large sample of experts would be needed to generalize our findings.

4.5 Final considerations

In the era of the fourth industrial revolution, trustworthy interoperability is becoming crucial for the success of Industry 4.0. At the top of the available solutions, blockchain promises to increase the degree of trust, changing the way transactions are done based on the immutability of records and transparent and trustworthy interactions among users and other entities. In this scenario, seven architecture drivers together with their solutions for trustworthy interoperability

in Industry 4.0 systems were presented in this chapter. Founded on the knowledge and experience of highly trained experts in Industry 4.0 and blockchain, these solutions can guide architectural decision-making when it comes to whether or not to adopt blockchain and, more importantly, in which situations. We conclude that, in most situations, blockchain needs to be combined with traditional technologies/solutions to promote fully trustworthy interoperability. We also claim that the importance of this work does not lie in providing the best solution for trustworthy interoperability, but rather in supporting software architects and researchers in systematizing the design of proper solutions for their projects.

Finally, the path to mainstream use of blockchain in Industry 4.0 is still long. It includes its use in other real-world applications to mainly get evidence about its impact on quality attributes (by getting quantitative data on, for instance, performance, safety, security, privacy, and others), on the maintenance of the Industry 4.0 systems and their components, and the availability of technologies and their compatibility.

CHAPTER

5

TIBA: A TRUSTWORTHY INTEROPERABILITY ARCHITECTURE

"If you could see it
then you'd understand
Ideas that you'll never find
All the inventors could never
design"

Coldplay

5.1 Initial considerations

Interoperability is a fundamental architectural concern for improving the way modern factories will work in the context of Industry 4.0. Trustworthy interoperability among manufacturers is one of the most important concerns for the success of Industry 4.0. An important aspect of Industry 4.0 is the complex structure connecting physical devices, digital and virtual entities, which dynamically change accordingly to the business goals. At the same time, blockchain has been widely pointed as the solution for promoting trust, transparency, and security of data. Industry 4.0 has also believed in the capabilities of blockchain, but without any evidence of the guarantee of trustworthy interoperability. Yet, companies interested in Industry 4.0 do not have any guidance on architecting solutions that assure trustworthy interoperability. This chapter contributes with a Trustworthy Interoperability Architecture for Industry 4.0, by combining blockchain with traditional solutions for interoperability. TIBA provides architecture views and guidelines to support architects during the interoperability of systems in the context of Industry 4.0. For the design of TIBA, we defined a set of architecture drivers and architecture solutions based on Industry 4.0 projects. As result, three architecture levels distributed in seven main architecture components are presented by combining blockchain with traditional technologies to

support architects during the development of a trustworthy interoperability system in the context of Industry 4.0.

5.2 TIBA design

The design of TIBA was based on activities of the Architecture Centric Engineering Solutions (ACES) (cf. Figure 13) (KNODEL; NAAB, 2016). The main focus of ACES is the elicitation of architecture drivers and architecture solutions covering quality attributes and concerns related to providing trustworthy interoperability in Industry 4.0. Architecture drivers are a set of key main requirements classified as risky, new, and costly to be maintained and can seriously affect the architecture design and implementation (ANTONINO *et al.*, 2019; KNODEL; NAAB, 2016). Architecture solutions are decisions made to solve each architecture driver in an efficient way (ANTONINO *et al.*, 2019; KNODEL; NAAB, 2016). ACES takes as input implicit information from the context to generate explicit information which is communicated and used by stakeholders to make decisions. The main activities of ACES for designing TIBA were the following:

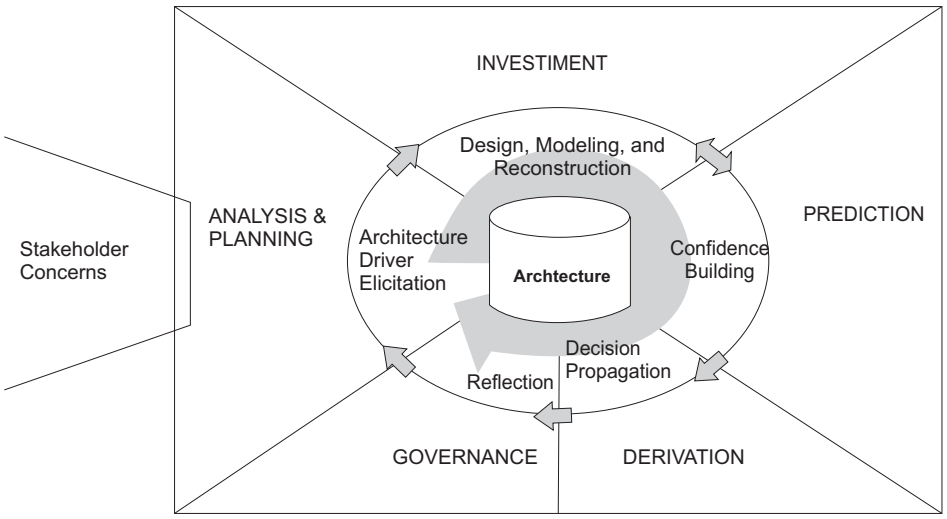

Figure 13 – Architecture-centric engineering. Source (KNODEL; NAAB, 2016)

- **Purpose of the architecture:** This activity is regarding the definition of missions for architecting. The main purpose of TIBA is to provide trustworthy interoperability for Industry 4.0 based on blockchain and concerns from experts of Industry 4.0.

- **Elicit architecture drivers:** Seven architectural drivers for promoting trustworthy interoperability in Industry 4.0 were defined in Chapter 3 centered on security (cf. authentication, access control, data privacy), traceability, availability of physical devices, data availability, and compatibility of data and services.

- **Define architecture solutions:** Seven directions architecture solutions based on experts of Industry 4.0 and experts of blockchain to solve the architecture drivers were defined in Chapter 4.

- **Design and modeling the architecture**: This activity is related to document architecture solution decisions in architecture views 5.3.

- **Decision propagation and Reflection:** Instantiate the architecture to derive systems artifacts and propagate the design decisions to source code. During this activity, TIBA was instantiated in the context of Production-as-a-Service business model and is presented in Chapter 6.

Purpose of the architecture

The purpose of TIBA is to provide directions and guidelines presented as an architecture to promote trustworthy interoperability in Industry 4.0. The TIBA was designed by the supervision of Industry 4.0 experts. The main steps for further design and documentation of TIBA are presented as follows.

Elicit architecture drivers

In Chapter 3, we defined a set of seven architecture drivers that together can assure trustworthy interoperability considering Industry 4.0 scenarios. In turn, architecture drivers are a set of key main requirements classified as risky, new, and costly to be maintained and can seriously affect the architecture design and implementation (ANTONINO *et al.*, 2019; KNODEL; NAAB, 2016). From these drivers, three are centered on security *(Authentication to the System, Data Access Control, Data Privacy to Protect Sensitive Information*), plus *Traceability and Auditability of Data*, *Availability of Physical Devices*, *Availability of Data*, and *Compatibility of Data and Services*. These drivers are defined in terms of (KNODEL; NAAB, 2016): (i) the *environment*, which describes the scenario the event takes places and the current condition of the driver; (ii) the *stimulus*, which refers to an event that triggers the driver; (iii) the *response*, which is the expected driver response according to the event; and (iv) *quantification* to measure the effects and indications associated with the driver.

Define architecture solutions

Seven architecture solutions were established that should be implemented together in Industry 4.0 to achieve trustworthy interoperability. The architecture solutions combine blockchain with traditional technologies for interoperability (Chapter 4) and they are represented in terms of (i) explanation about the design decision environment; (ii) pros and opportunities to implement the solution; (iii) cons and risk regarding adopting the solution; (iv) assumptions and quantification to quantify the solution; and (v) trade-offs to adopt the solution proposed.

5.3 TIBA architecture view

This section presents the design of TIBA. This task encompasses the translation of architecture drivers and solutions into architecture views, which can provide the necessary foundations to solve the underlying business problem. The design of TIBA follows the C4 model, which encompasses four levels of architecture representation (Vazquez-Ingelmo; Garcia-Holgado; Garcia-Penalvo, 2020; LEANPUB, 2017): *(i) Context view* is represented by different actors and their interactions with the system being developed. This view presents a high-level view of TIBA; *(ii) Container view* outlines the necessary components to provide the services that TIBA will offer. This view provides only function description of each container and the relationships among them; *(iii) Component view* describes the collaboration between different components and services or functionalities of the container; *(iv) Code-level* specifies the technical details of objects and classes to be created and can be specified through UML class diagrams, components diagrams or sequence diagrams. In this work, as we are focused on the higher abstraction level of services and components, the code-level view is not represented.

Context view

The context view provides a starting point, showing how the software system in scope fits into the world around it. Figure 14 presents the context view of TIBA that provides the main services for trustworthy interoperability between Entity A and Entity B, which can be users, external systems, devices, machinery, robots, or digital twins.

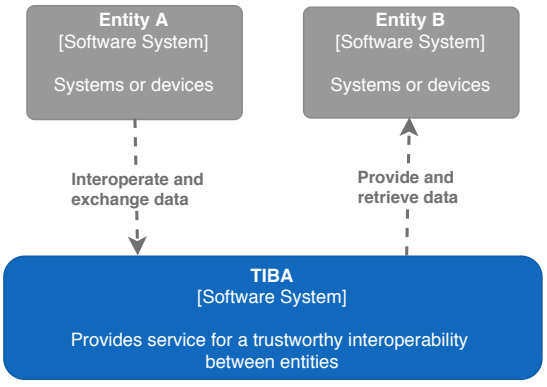

Figure 14 – Context view of TIBA

Container view

The container view shows the high-level structure of the architecture and how responsibilities are distributed across it. It also shows the major technology choices and how the containers communicate with one another. In Figure 15, we show the main containers that provide services for trustworthy interoperability between entity A and entity B. In this view, details about technology are also presented regarding the use of blockchain and database storage. The importance of

this view is to provide guidelines regarding how each service can interact with each other in turn to encompass the seven architecture drivers defined in previous work.

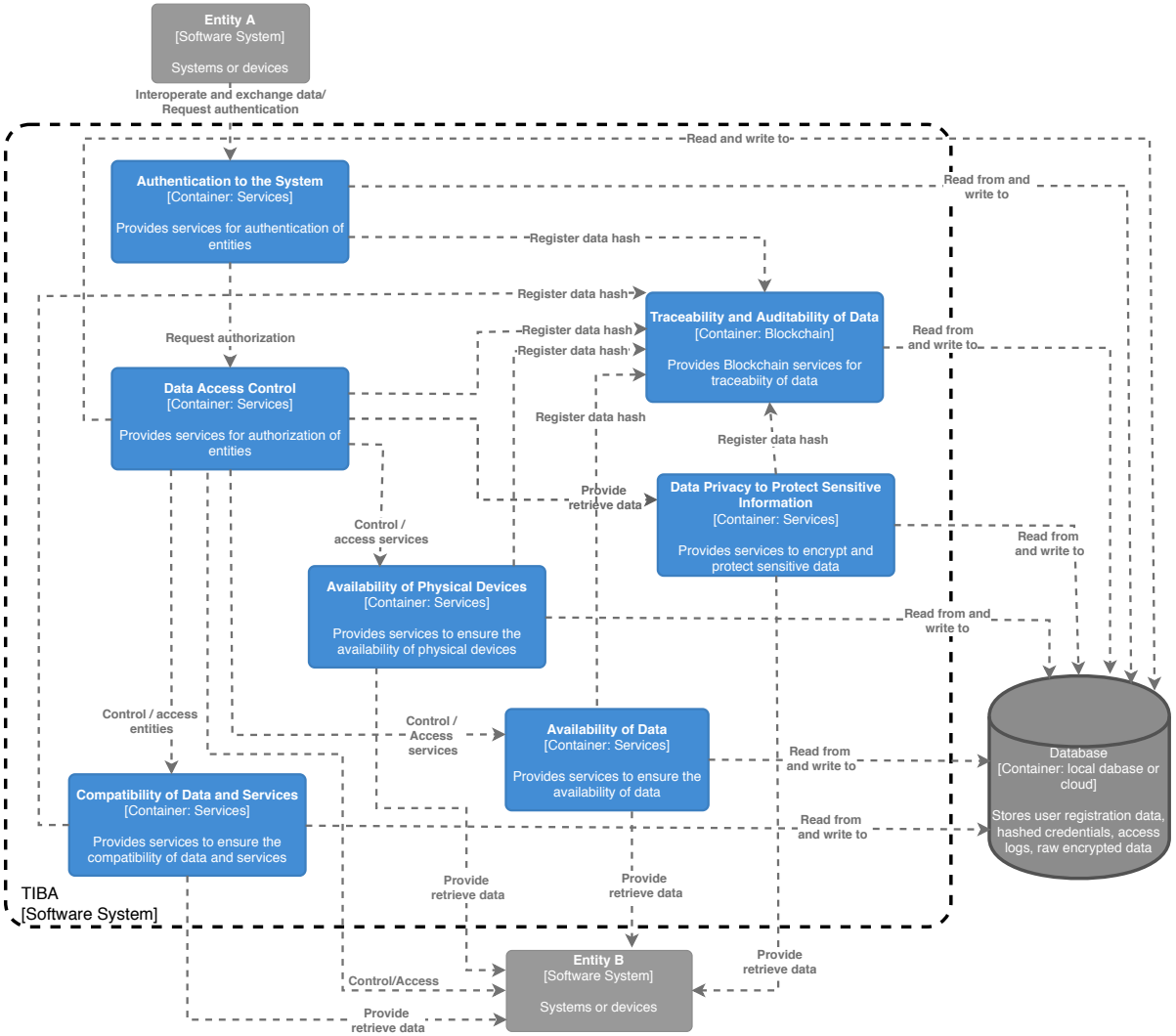

Figure 15 – Container view of TIBA

Component view

The component view brings more details of each container of TIBA. It is a group of related functionalities encapsulated behind a well-defined interface. We defined seven component views, which represent the solutions for the architecture driver. In each component view, we present the main services and how they interact with each other.

Component view for Authentication to the System

The component view for Authentication to the System, shown in Figure 16, describes the main components to authenticate the entities into the system. *Identity management* provides the services to manage human-to-device, device-to-device, and system-to-device or system-to-service identities. This service should establish the naming system for IoT devices and determine

their identification lifecycle, including when they need to be removed or modified to meet the project goals; *Smart contract for identification* takes as input the ID token from the entity and check if it exists and if it is valid in the blockchain. If true, the smart contract allows the authentication of the entity otherwise the request is rejected and forward to the service to add entities; The *Smart contract for adding entity* only includes new entities if their data matches the pre-loaded data that were agreed by all members of TIBA; The container *Database* is responsible for storing a copy of entities attributes, logs, and encrypted authentication keys. The main goal is to support entities for recovering authentication data in case it is lost; The container *Traceability and Auditability of Data* is responsible to distribute the execution of the smart contract, which were triggered by a message or transaction. This data is then distributed and accessible to all members of TIBA. It is important to highlight the focus of this thesis is not to present further details about blockchain technology, but yes to propose guidelines showing how traditional authentication solutions and blockchain can be combined.

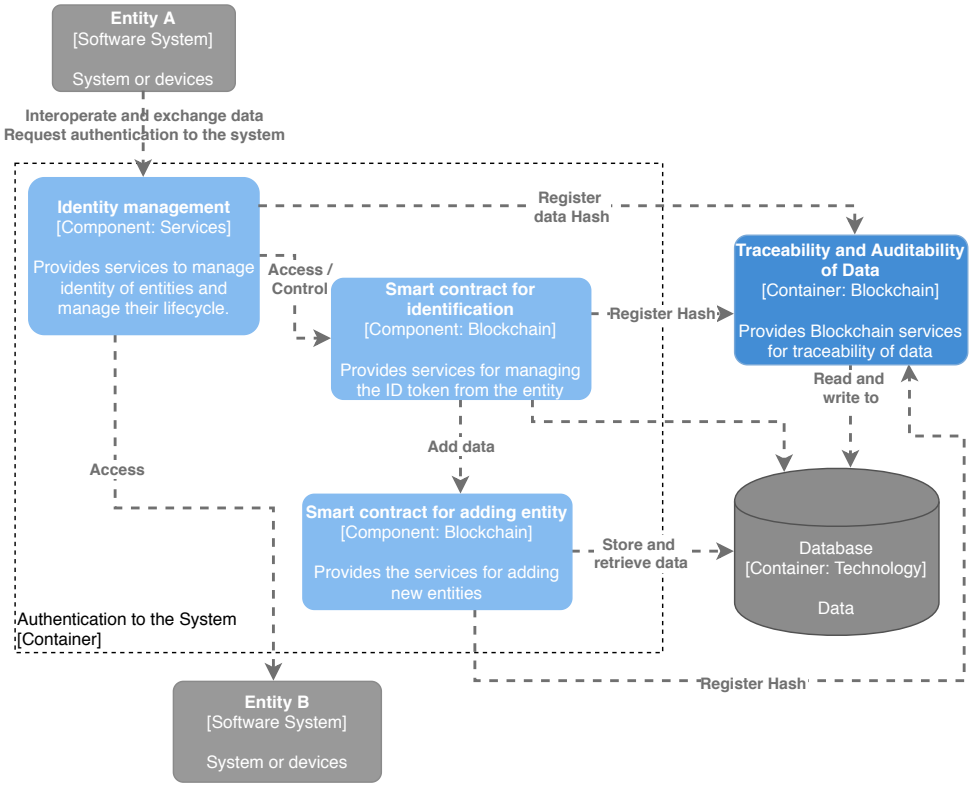

Figure 16 – Component view for Authentication to the System

Component view for Data Access Control

The component view for Data Access Control, shown in Figure 17, describes the main components to provide the rules for authorizing users to access the system. The service *Access control management* manages the privileges of each entity by controlling the access to services, data, or objects accordingly to predefined rules. This service takes as input the ID token from the entity and checks if it has privileges for accessing the system/devices; The service *Smart*

contract for authorization provides the rules and policies for authorizing each entity. These rules and policies must be previously agreed upon by the Industry 4.0 consortium partners. The container *Database* stores the rules and policies permission while the container *Traceability and Auditability of Data* distributes the execution of the smart contract in the blockchain.

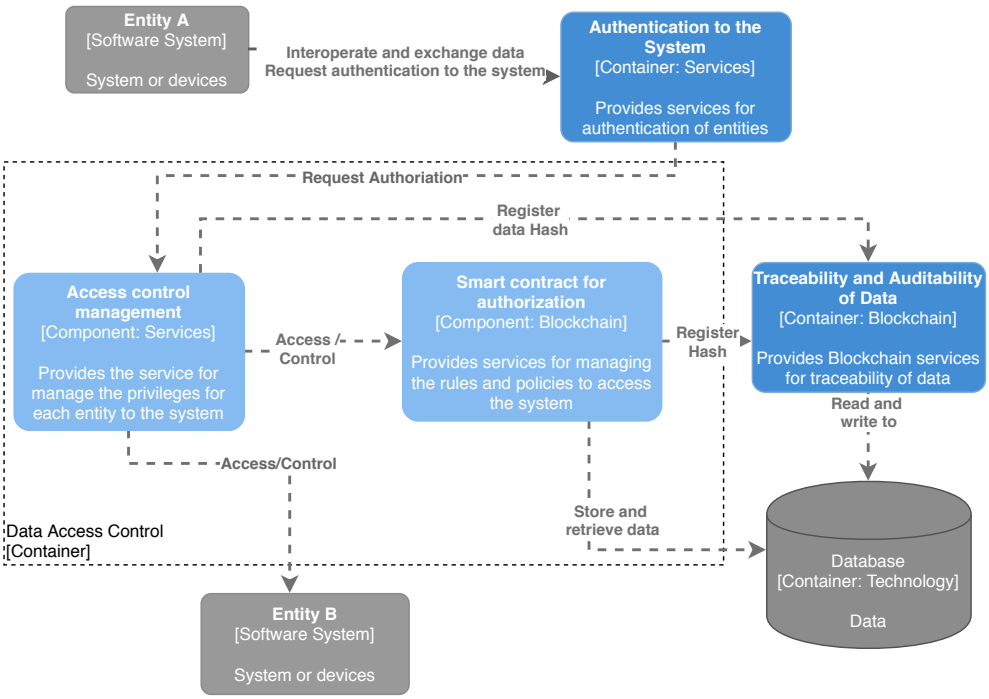

Figure 17 – Component view for Data Access Control

Component view for Data Privacy to Protect Sensitive Information

The component view for Data Privacy to Protect Sensitive Information is regarding the concern of each individual should have control of its data, but when most solutions are centralized, the self-control of data becomes hardly possible. As described previously in the architecture solutions 11, experts from Industry 4.0 recognize the benefits of blockchain for data privacy that can create individual control over their data. The *Data Privacy Management* is responsible to provide services to protect sensitive data by providing an end-to-end encryption infrastructure in which only authorized entities will have the encrypted key to access the data; *Smart contract policies for data privacy* provides services for encryption and pseudonymity that can mitigate the privacy concerns of the distributed ledger. The container *Traceability and Auditability of Data* is responsible to distribute the execution of the smart contract in the distributed ledger.

Component view for Traceability and Auditability of Data

The component view for Traceability and Auditability of Data (Figure 19) provides the features to enable identification, tracking of data, and to configure auditable entries for particular

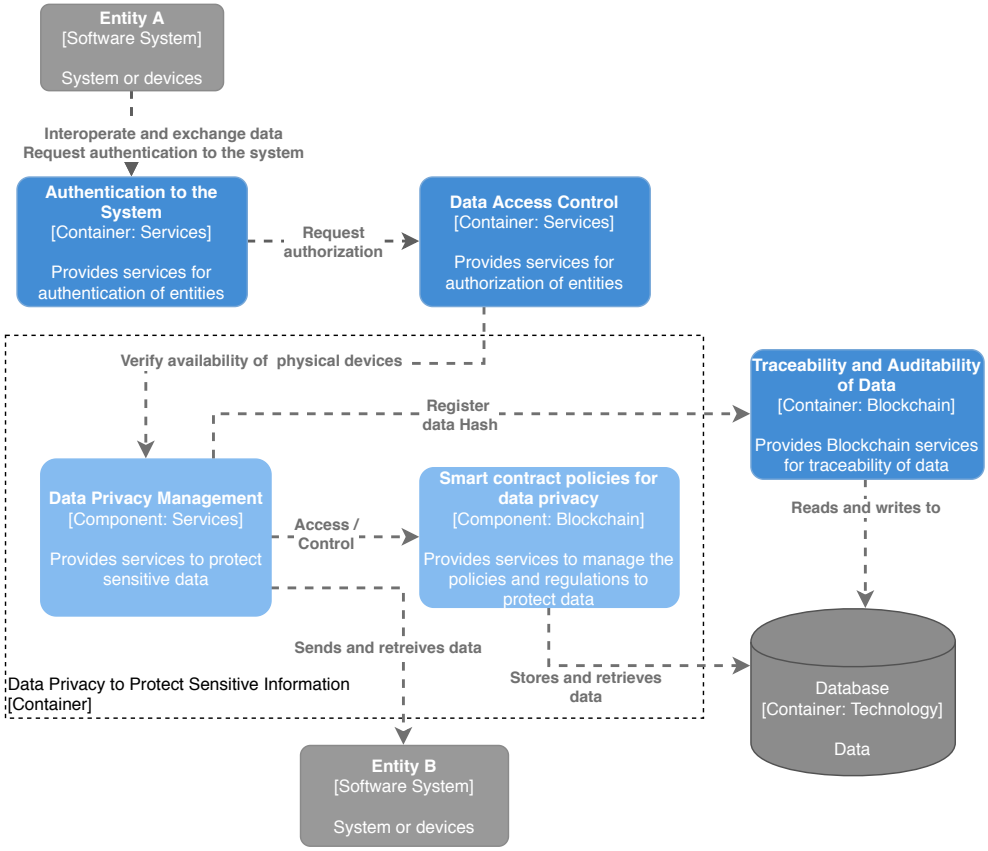

Figure 18 – The component view for Data Privacy to Protect Sensitive Information

data entities. The service *Tracking controller* is used for managing the hash of each event and transactions being executed in TIBA. These hashes point to the data, which is stored in the in a traditional database; The service *Traceability report for auditability* is responsible for supporting auditors to retrieve data regarding transactions in the blockchain for further auditability; The *Private blockchain* represents a private blockchain for only authorized participants. The private blockchain is responsible for recording the hash of each transaction exchanged in TIBA, allowing a secure and cost-effective traceability system. In this view, blockchain is represented as a "Black Box", as no further detail about blockchain is described.

Component view for Availability of Data

Figure 20 presents the component view for Availability of Data. This view relies on the maintenance and monitoring of data to keep the system working reliably. Services must be designed to ensure the availability of data even when organizations experience a power outage. The *Validation check* service provides the services to verify whether data is available and whether it accomplishes the expected data standards. This includes performing checks to verify the syntactic of data received and whether the transmitted data are known to the end system. The *Monitoring availability of data* presents services to identify and remediate anomalies for maintenance, such as rules, events, and triggers to identify issues; The *Recovery of data* provides

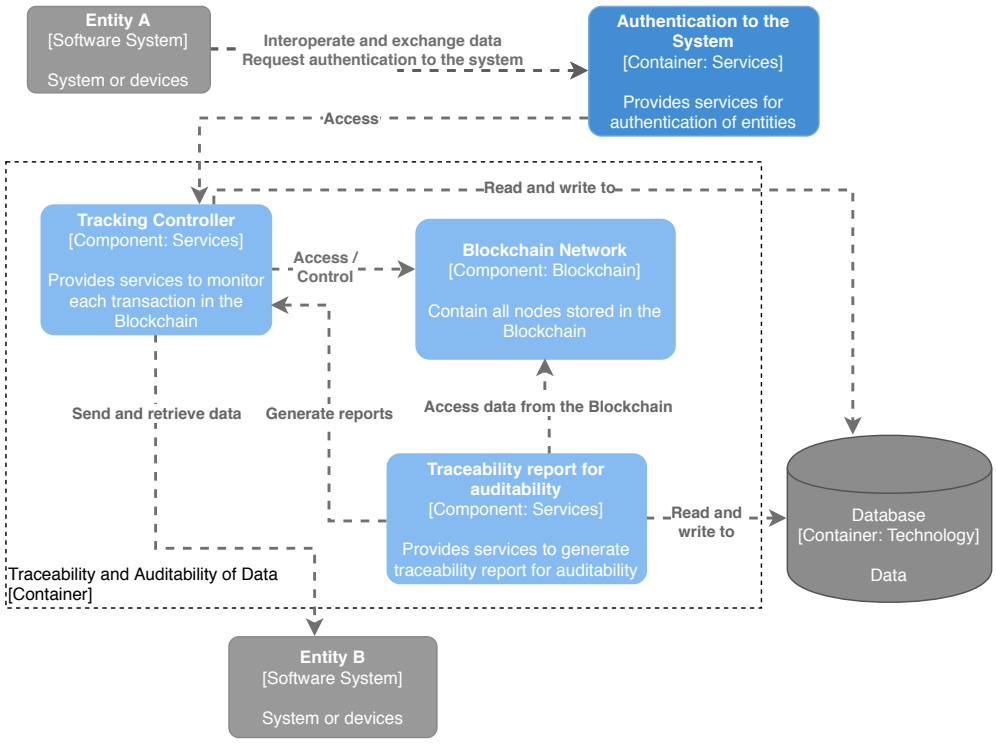

Figure 19 – Component view for Traceability and Auditability of Data

the main services for recoverability of data, including redundancy services, storage in the cloud, and backup servers to recover the last data. The *Traceability and Auditability of Data* is used for managing the hash of each event and transactions being executed in TIBA.

Component view for Availability of Physical Devices

The component view for Availability of Physical Devices encompasses the limit of time that the device is powered on and capable of processing data and transmitting data. Figure 21 presents the main services for the availability of physical devices, such as *Check Reachability of device*, which refers to whether the device is reachable and online. Usually, ping testing can be used to communicate with the target device; *Recovery of physical devices* services provides the recoverability plan to cover both physical location and devices, accordingly to company regulatory requirements; *Monitoring physical devices* presents the service to help determine the condition of devices and improve the prediction in case maintenance or interruption is needed during the production line. The *Traceability and Auditability of Data* records each status of data in the blockchain.

Component view for Compatibility of Data and Services

Figure 22 shows the component view for Compatibility of Data and Services that encompasses the main services to provide semantic and syntactic communication among heterogeneous devices and systems from Industry 4.0. For this, *Authentication to the System* and *Data Access*

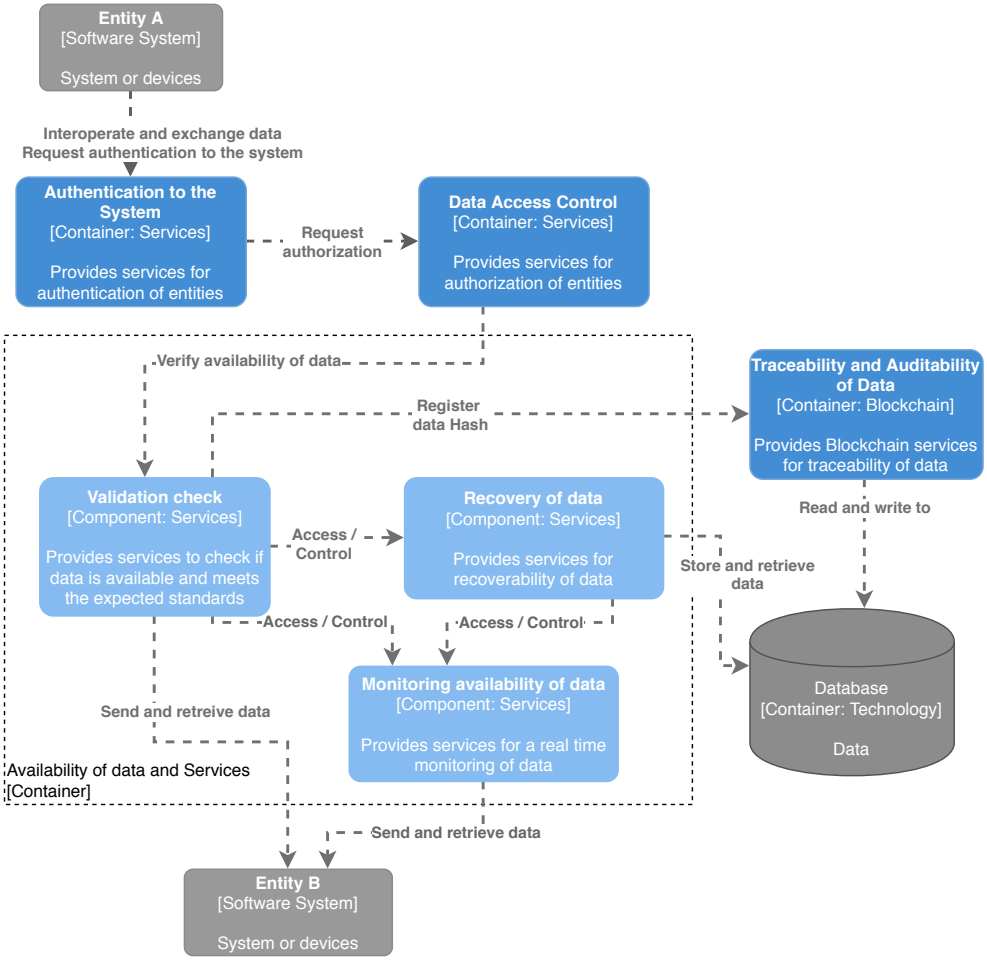

Figure 20 – Component view for Availability of Data

Control must provide the services to manage the identity of each entity and guarantee their identification and authorization for accessing the system. If the identification and authorization are true, the service *Check compatibility* is called for checking whether the input, output, and pre-conditions between data being exchange are compatible with syntactic and semantic policies. The *Policies and rules* provides the main services for syntactic and semantic communication, which were pre-defined by all members of the Industry 4.0 consortium. The *Protocol service* provides the services for translating and mapping data to policies and protocol rules. *Traceability and Auditability of data* stores the attempting of communication between entities to keep track of data being transferred; *Database* container stores all policies and rules for compatibility; The container *Traceability and Auditability of Data* stores the hash pointed to each transaction in the blockchain.

5.4 Main findings and limitations

The combination of blockchain and traditional solutions, as proposed in TIBA, provides a transparent layer of data storage for the manufacturers involved. To secure data transfer,

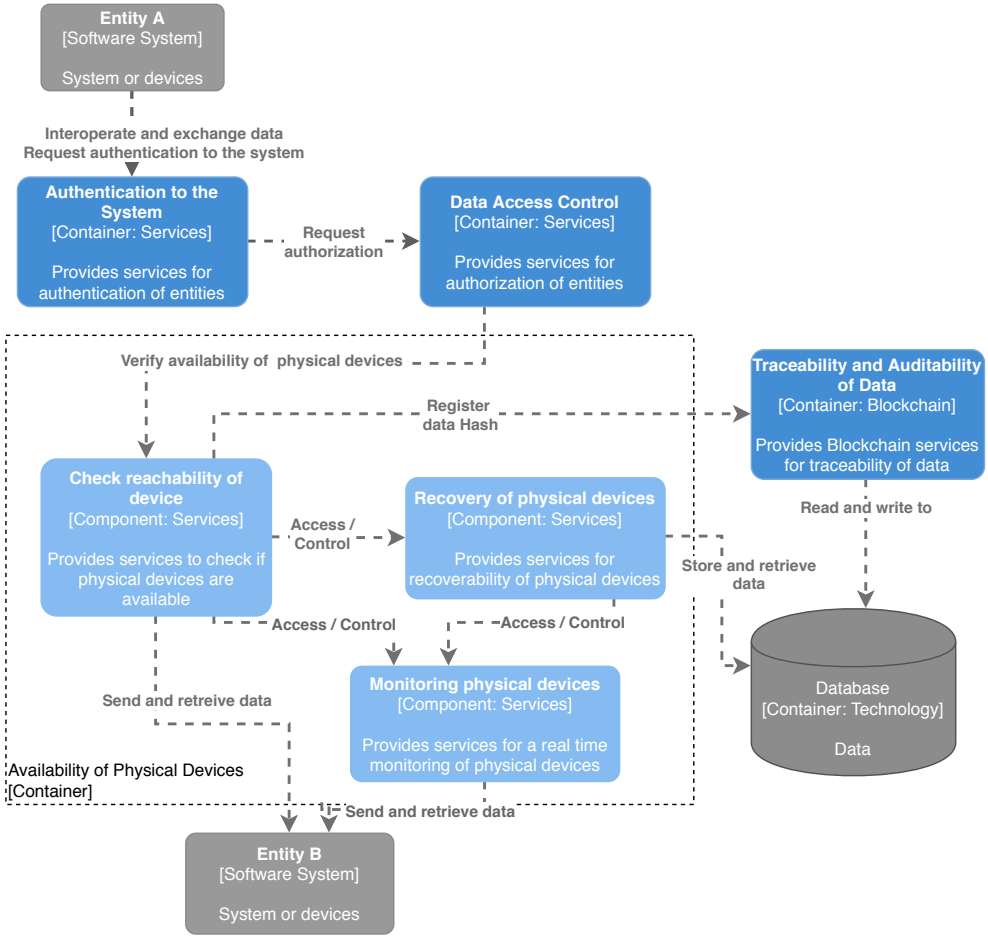

Figure 21 – Component view for Availability of Physical Devices

every piece of data is encrypted before storing it in the blockchain. This provides provenance services by recording the evidence of the data originality and the operations in the chain, which are accessible for all authorized users. Furthermore, the external database is used to store a big amount of data, including authentication tokens, authorization rules, which can be further recovered in case of loss of tokens key, data from sensors, big data analysis, ERP decision making, manufacturers, and customers data.

Very small batch size product line, such as the production of one workpiece, can take advantages of TIBA, by automating the conclusion of contracts to offer such small quantities economically feasible. Contracts regarding authentication, authorization, and privacy of data can be concluded automatically by meeting certain requirements. These requirements would include, for instance, maximum scope, risk assessment, and whether the customer is already known or whether similar contracts have been successfully concluded in the past. Besides, as blockchain contain a signature of bilaterally exchanged data and not the data itself, then it is possible to prove that a contract was concluded without every partner of TIBA being able to see the content in the blockchain.

Another benefit of TIBA is traceability. Digital twins can be signed with the TIBA

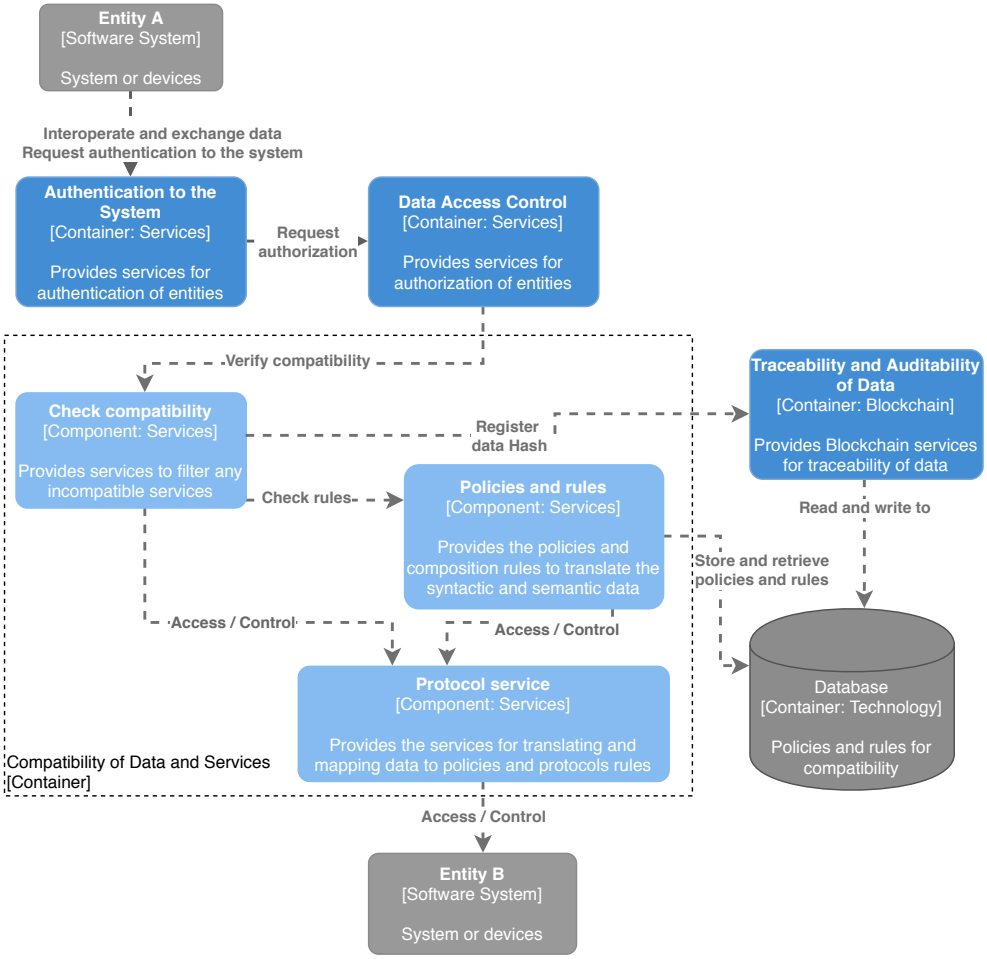

Figure 22 – Component view for Compatibility of Data and Services

and thus document the production steps. TIBA ensures safety guidelines and quality processes through the combination of blockchain, thus avoiding costly certifications and guaranteeing the authenticity of products, and reliably identify plagiarism. This is an advantage for quickly switching suppliers nowadays, such as Production-as-a-Service (PaaS) provider, which is a business model in which manufacturers sell products to clients (product developers) that includes software, hardware, maintenance, installation, and other values adding services for a predefined fee. This allows manufacturers to build an ongoing relationship with clients over service and product lifecycle, which increases the importance of collaboration among industrial partners.

Potential suppliers can also have take advantages by using TIBA. Transactions can be viewed by third parties and thus lead to a reference for the contractor. This could also become part of contracts inside TIBA, so that not only the contract is signed, but also an assessment of product quality and adherence to deadlines.

TIBA is not a total decentralized system, which reduces the scalability problems of the blockchain. Because of this, a possible application of TIBA is to have a central market maker with the operator of the marketplace who primarily drives the blockchain. This is different from Bitcoin, which runs completely decentralized. Thus, in this scenario, we must rely on the

central authority (market maker), because customers do not want to hand over the details of the orders to make the market maker. So, TIBA handles this scenario by allowing each partner to cryptographically sign a transaction on their own and import it into TIBA to turn the transaction valid. This could only regulate market access, partner does not see what the participants are negotiating with each other.

The main challenge of TIBA is to keep the blockchain running. This includes rewards to users for mining and matching transactions in the pool. In this case, the marketplace can also be a solution, which could be operated by a player (analogous to Amazon marketplace or eBay). This mediates production orders and enables the automated closing of smart contracts for very small to big production lines.

We designed this work to avoid bias as much as possible. In the following, we describe the threats to the validity of this study and the corresponding mitigation actions to minimize them. **External validity:** It refers to the generalization of the results of this study. We minimized this threat by performing three phases of work conduction. In the first phase, we defined the architectural drivers through a survey conducted with experts from Industry 4.0. In the second phase, we conducted interviews with experts from Industry 4.0 and blockchain to understand how would be the best solution to solve each architectural driver. Then, in the third phase, with all this knowledge gathered from previous experiences, we designed the TIBA architecture to match with each solution described in previous work. **Internal validity:** It refers to whether the treatment used in this study made any difference to achieve the results presented in this work. We mitigate this threat by evaluating each phase in previous work with experts from Industry 4.0. The results from these studies were the base to construct TIBA and then minimize potential internal bias. **Construct Validity:** It refers to the relationship between theory and observation. To mitigate this threat, we follow conduct this work together with the supervision of experts in Industry 4.0. **Conclusion Validity:** It is related to the ability to draw correct conclusions through the results obtained. We reduce the bias from this study by following the Architecture-centric Engineering Solutions (ACES) approach (KNODEL; NAAB, 2016), which encompass the design of architecture drivers and solutions, modeling, and evaluation. The steps of each process were presented in a previous study and already evaluated by experts.

5.5 Final considerations

This study introduces TIBA, a novel blockchain-based architecture to deal with interoperability considering different views of abstractions. To design TIBA, we defined, in previous work, seven architecture drivers, and seven architecture solutions to provide guidelines for trustworthy interoperability in Industry 4.0. These architecture drivers and solutions were analyzed by conducting surveys and interviews with experts of Industry 4.0 and experts in the blockchain. These drivers and solutions comprise the first set of architectural decision making regarding the combi-

nation of blockchain with traditional technologies to promote more trustworthy interoperability in Industry 4.0. Based on this previous knowledge and experience, TIBA was proposed. TIBA provides an interoperability infrastructure, in which users have a new relationship with data being transmitted. Instead of trusting the source of data from a central provider, users can have direct access to information defined in upper levels of interoperability through smart contracts. In TIBA, smart contracts are synchronized with each trustworthy component, so data of transactions is stored in the blockchain. The advantage of these architectural views is the continuous use of explicit descriptions in every involved element, which brings the first guideline to support architecture identifies the main components to promote trustworthy interoperability and how they can combine blockchain with traditional solutions. These architectural views can be further detailed within other UML diagrams bringing more comprehension of the software architecture being designed.

CHAPTER

6

INSTANTIATION OF TIBA

"It's because I am trustworthy
He gives me strength far more than
my share"

Elvis Presley

6.1 Initial considerations

The increased importance of companies' collaboration and market needs are placing high demands on all areas of industry, including technology, security, organization process, and laws. In this context, Production-as-a-Service highlight the importance of proper trustworthy interoperability and proper agreements to support future demands of services and products, as, in some cases, third parties shall interact with manufacturers to develop and provide goods and services. However, communication between parties relies on common agreements made by intermediaries in many levels of interoperability concerns, which increases the cost and barriers of collaboration, as it usually involves unpredictable behavior of operations made by humans. Issues of trust may cause misuse or even fraud of information being transferred, thus, means to overcome the non-reliable environments are needed. Thus, this chapter presents how TIBA can be instantiated to solve problems regarding trustworthy interoperability in the context of a real Industry 4.0 project.

6.2 Use case scenario

The PaaS is a business model in which manufacturers sell products to clients (product developers) that includes software, hardware, services, maintenance, installation, and other values adding services for a predefined fee. Similarly to PaaS, Manufacturing as a service (Maas) is being implemented around the world, but the main difference is MaaS do manufacturing for

hire, whereas PaaS sells the services and outcomes a product can provide (HERMANN; RÜBEL; RUSKOWSKI, 2020). PaaS offers a plural form of network organization, which brings a change in the traditional labor policies and human management resources. The focus must be on the value of services and products being provided by manufacturers. This allows manufacturers to build an ongoing relationship with clients over service and product lifecycle, which increases the importance of collaboration among industrial partners.

PaaS is not a new business model, the Rolls-Royce trademark[1] has been offering a product as a service through leasing operation since 1962. Recently, with the advances of cloud technology and IoT, PaaS has gained more popularity with companies like Uber or Lyft. Instead of buying a car, customers can access transportation on demand, without the financial burdens of car maintenance.

There are several advantages for adopting PaaS, including reduction of material consumption, energy, cost, and reduction of environmental impact (KUHN; SADIKOW; ANTONINO, 2019). Manufacturers can boost the profitability of their services and improve client engagement. Clients have the opportunity to increase the utilization of their resources by using technology more up to date and increase cost savings with predictive maintenance and better-tailored pricing. Besides, clients do not assume the risk of service, or product failure, or maintenance of machinery, as they are usually included in the service.

PaaS brings many benefits to businesses and creates value for its customers, but currently, the collaboration required in a PaaS model is difficult and costly to maintain due to the personal overhead (KUHN; SADIKOW; ANTONINO, 2019). Organizations are centralized and structured hierarchically, leading to a complex and not transparent business model. Many organization decisions have human intervention, which creates obstacles and bureaucratic models to establish agreements, increasing contract changeability, and costs to maintain PaaS. It is harder to get money back for a service poorly executed. For this reason, collaboration and proper agreements pose a major challenge to turn PaaS economically feasible. Other concerns are also worth mentioning, such as companies' culture might suffer to accomplish many contracts to not get penalized, and uncertainty about the protection of intellectual product properties.

As different as these challenges are, they have two major faces in common (KUHN; SADIKOW; ANTONINO, 2019). The first is related to interoperability concerns to transfer and use information efficiently and uniformly between manufacturers and clients. The second is related to provide a trust PaaS environment with agreements in form of contracts among parties. In practice, a trust PaaS interoperability infrastructure must be actively agreed upon between parties involved.

The scenario proposed in this work for the instantiation of TIBA is based on the project from one of the Industry 4.0 partner of the BaSys 4.0 project regarding digitalization of the

[1] https://www.iotworldtoday.com/2017/06/14/8-strategies-transition-product-service-business-model/

automated pallet transport of workpieces (Figure 23) (ANTONINO *et al.*, 2019; KUHN *et al.*, 2018). The transport system includes roller conveyors, shift tables, turntables, and a third-party industrial robot, which were integrated into the current transport system to make the production more efficient. This scenario describes a real situation that is becoming more common in Industry 4.0 context[2], (FRAGAPANE *et al.*, 2020; BOSCH, 2020).

Many sensors are controlling the speed, temperature, position, and shift of the workpiece. Sensors, devices, and applications are interconnected and need to interoperate with many systems and users inside and outside the production line. This infrastructure has digital twins, which provide information and a virtual copy of the platform. The information includes transport system occupation status, workpiece status, and localization status. The control system of the automated transport is composed of a high-level IT system, such as ERP and CRM, and the platform is a shop floor devices.

The communication between the automated transport system and the shop floor devices crosses multiple levels of the automation pyramid presented in Figure 3. End-to-end communication is possible through the Virtual Automation Bus, which bridges the gaps between many communication protocols for Industry 4.0. The virtual automation bus allows communication with different networks, shop floors, enterprise components in the office floor via different communication protocols (i.e., HTTP/REST web services and OPC-UA) (KUHN *et al.*, 2018).

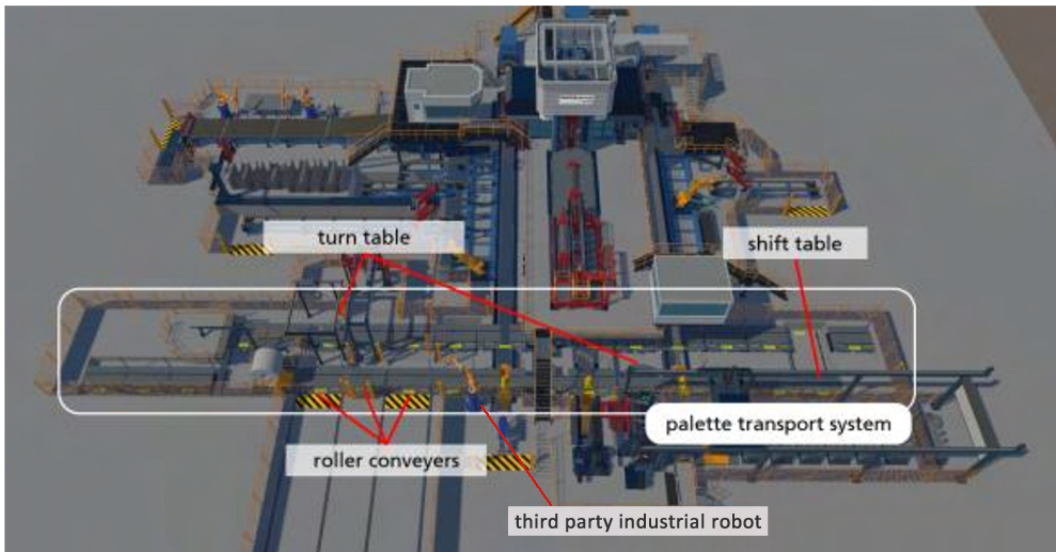

Figure 23 – Digitalization of the automated pallet transport. Adapted from (ANTONINO *et al.*, 2019)

The integration of the third-party robot into the manufacturer's production line increases the cooperation among the companies and expands their portfolio of products, creating the best conditions for improving existing process structures, increasing efficiency, and improving overall productivity in the long term. However, the inclusion of the third-party robot rises many concerns related to trustworthy interoperability that must be properly defined.

[2] An example of smart manufacturing cooperation can be found at https://www.boschrexroth.com/en/xc/company/press/index2-31616

To better understand this scenario, we simplify it into three main stakeholders: ManufacturerA, ManufacturerB, and Customer. The scenario above is generalized in the following steps:

- Step 1: ManufacturerA offers an online service to create products.
- Step 2: Customer requires the production of a workpiece.
- Step 3: Customer sends information and contract related to producing the product.
- Step 4: ManufacturerA accepts a contract to produce the product.
- Step 5: ManufacturerA recognizes that for fast production of the workpiece, he/she needs to hire an industrial robot from ManufacturerB.
- Step 6: ManufactureB accepts the contract to be part of the process to produce the product.
- Step 7: The *third party industrial robot* is integrated into the automated pallet transport system.
- Step 8: Digital twins exist to bridge the physical and virtual environment and to represent the new device integrated into the transport system.
- Step 9: Information from the production line is shared among the participants involved in the production of the workpiece, including data from each device and process.
- Step 10: ManufacturerA and ManufacturerB have access to each device, system, and digital twin involved in the production of the workpiece.
- Step 11: Customer has access to the status of the workpiece and to each process, the workpiece is passing in the automated transport system.
- Step 12: ManufacturerA and ManufacturerB produce the workpiece and send it to the logistic transport system.
- Step 13: Logistic transport scans the product tag to deliver it to the customer.
- Step 14: Customer receives the product and authorizes the payment within his bank account.
- Step 15: ManufacturerA and ManufacturerB receive the payment according to previous contracts.

6.3 Blueprint for architecture drivers and solutions

Regarding the scenario previously described, we present in this section a compilation of common needs to provide trustworthy interoperability between the third-party industrial robot and the automated pallet transport system. For this, we defined seven specifications of architecture

drivers and three architecture solutions, which, together, form a blueprint of key aspects that might be considered for integrating the third-party industrial robot into the automated pallet transport system. Besides, it is also presented the architectural views of TIBA encompassing the main components and flow of messages to support the architects considering the main quality aspects, in turn, to provide trustworthy interoperability among these entities.

The architecture drivers for this instantiation focus on the following quality aspects: *Authentication of the System, Data Privacy to Protect Sensitive Information, Data Access Control, Availability of Data, Availability of Physical Devices, Traceability and Auditability of Data*, and *Compatibility of Data and Service*. The architecture solutions blueprints combine concepts of digital twins, blockchain, service-oriented middleware, and security protocols combined with blockchain to ensure the identification and authorization of each entity connected in the production line.

6.3.1 Architecture drivers

The first architecture driver for this scenario is the *Authentication third-party robot into the system*, shown in Table 12. This driver describes the process of confirming and ensuring the identification of the third-party robot into the system. In this case, as described in the field *environment*, we assume that the third-party robot is already installed in the production line system. The *stimulus* for this architecture driver is when the third-party robot is physically connected and turned on withing the production line infrastructure. As *response*, the credentials of the new entity is sent and verified by the production line systems.

Table 12 – Driver *Authentication of the third-party robot into the system*

Authentication to the System	**Quantification**
Environment: The third-party robot is already installed in the production line.	Entities >0
Stimulus: The third-party robot is turned on.	Credential keys !=NULL
Response: The system verifies the credentials preventing unauthenticated access.	Pair of credential keys= TRUE

The architecture *Data access control for the third-party robot to the system* (Table 13) refers to privileges that the third-party robot must have to coordinate and access other entities (i.e., sensors, robots, machinery, pallet transport system). The *environment* describes the access control for the third-party robot, which is limited to access the workpiece every five seconds and turn its position 90 degrees (ANTONINO *et al.*, 2019). The *stimulus* to authorize the third-party robot to access the workpiece is through a QR code on each workpiece. The third-party robot scan the QR code from each workpiece and the system authorized the robot to modify the workpiece position.

The driver *Tracking the third-party robot production* (Table 14) describes the ability to track data and support an audit trail in case of failure in the production line. For the *environment*,

Table 13 – Driver *Data access control for the third-party robot to the system*

Data Access Control	Quantification
Environment: There is workpiece passing in front of the third-party robot in every 5 seconds	Workpiece >0
Stimulus: The third-party robot scan the QR code to get access the workpiece.	Permission rights !=NULL
Response: The system verifies the grant permission and allow the third-party robot to access the workpiece and turn it in 90 degrees.	If (Permission rights = TRUE) than modify.

we assume the third-party robot is installed and ready to be turned on. The *stimulus* for this architecture driver is regarding the initiation of the production of the workpiece. The *response* of the system is to track every activity performed by the third-party robot, including the registration of QR code, temperature, workpiece weight, and every step of the process chain. Information must be available and accessible for authorized entities (i.e., users, systems, machinery). This allows managers to make decisions and improve quality and audit readiness throughout the product line lifecycle.

Table 14 – Driver *Tracking the third-party robot production*

Traceability and Auditability of Data	Quantification
Environment: The third-party robot is connected to the main system.	Transactions != NULL.
Stimulus: The third party-robot is turned on and initiates the production of a product.	New timestamp != old timestamp
Response: The system records each step of third party robot, including what was changed, in which way, and who made the changes.	Current step of production != previous step of production

The driver *Availability of the third-party robot* (Table 15) deals with the current information of the thirdy-party robot for scheduling their maintenance operations and / or identification of flaws and unforeseen situations. The *environment* for this driver describes the thirdy-party robot working in its capacity. The *stimulus* is regarding an unexpected event happens in the power energy supply, which turns off the robot. As *response*, this driver is responsible to send real-time information of robot's condition, including the temperature of the robot, connectivity, speed, and power energy consumption. Besides, real time reports from the current use of the robot is generated, which is used to calculate the capacity to process the production of the product's workpiece stopped by the failure.

The driver *Availability of data from the third-party robot* (Table 8) is responsible for documenting data from the third-party robot and the whole production line system. The *environment* for this driver describes the robot interconnect to the automated pallet system, which stores data in a database. The *stimulus* describes an authorized entity requesting access to the robot to

Table 15 – Driver *Availability of the third-party robot*

Availability of Physical Devices	Quantification
Environment: The third-party robot is working in its full capability.	Devices >0. Products scheduled >0.
Stimulus: An unexpected event happens and turns off the third-party robot.	Error alert >0.
Response: The system emits an alert related to the robot with defects. The system send the error by message for the responsible stakeholder.	Complete workpiece=0. Process P=producing. Reschedules= 1

collect data from the QR code sensor. As *response*, the system grant access to the authorized entity to get the data from the third-party robot.

Table 16 – Driver *Availability of data from the third-party robot*

Availability of Data	Quantification
Environment: The third-party robot is interconnected with the automated pallet system. All data from the production line is stored.	Data !=NULL
Stimulus: External system requests access to the robot to collect information from the QR code sensor.	Timestamp != NULL.
Response: Data is retrieved from the robot at real time.	If (grantPermission=TRUE AND UserID=TRUE AND end-to-end encryption = TRUE) then access data

The driver *Data privacy to protect data from the third-party robot* (Table 17) is regarding formal contracts made by manufacturers to regulate who will have access to data. The *environment* for this driver describes the third-party robot connected to the production line and communicating in real time with the automated pallet system. The *stimulus* describes an employee from the production line trying to change manually the instructions of the third-party robot. As *response*, the third-party robot emits alerts of intrusion and block the access for non authorized users.

Table 17 – Driver *Data privacy to protect data from the third-party robot*

Data Privacy to Protect Sensitive Information	Quantification
Environment: The third-party robot is interconnected and communicating in a transparent manner with the automated pallet system.	Entities >0.
Stimulus: A user tries to access the robot and change the its instructions by manual command.	Sensitive data != NULL.
Response: The third-party robot emit alerts of intrusion and block the access for non authorized users.	If (grant permission = TRUE AND UserID = TRUE AND end-to-end encryption = TRUE) then access data.

The driver *Compatibility of the third-party robot to the system* (Table 18) describes the infrastructure required to connect, translate, and use information between the third-party robot to the production line system. The *environment* describes the third-party robot already connected to the production line system and working with at least one product scheduled. Besides, the third-party robot is already addressable via many different communication channels (i.e., TCP/UDP, IP, MAC address, and IDs). The *stimulus* is regarding the additional of a new entity to the system, which has to access data from the third-party robot. As *response*, the robot recognize and grant access to the new entity by verifying its identification parameter. Besides, the third-party robot system checks the compatibility of the communication protocols (i.e., syntax and semantic protocols) to allow a proper communication with the new entity.

Table 18 – Driver *Compatibility of third-party robot to the system*

Compatibility of Data and Services	Quantification
Environment: The third-party robot is working with at least one product scheduled. The third-party robot is already addressable via many different communication channels (i.e., TCP/UDP, IP, MAC address, and IDs)	Product scheduled >0. Digital copy = Number of entity.
Stimulus: A new device is added to the system and must have access to the third-party robot.	Device ID parameter != NULL.
Response: The system integrates the new device in the system with its identification parameter accordingly to common protocols for communication.	New entity value = new digital copy value. Devices are addressable.

6.3.2 Architecture solution

We specified architecture solutions for addressing the goals of the seven architecture drivers described previously. Each solution is detailed according to (i) an overview description, (ii) pros and opportunities, (iii) assumptions and quantification, (iv) cons and risks, and (v) trade-offs.

The first architecture solution is the implementation of a private blockchain combined with traditional solutions used for authentication and authorization. Among these solutions, cryptography infrastructure such as PKI, security protocols for authentication, Attribute Based Control (ABAC) system for privileges control, and an off-chain database to store data and the access policies. The *pros and opportunities* of this combination include: a) more security for exchanging data, as blockchain relies on end-to-end cryptography, b) ensure only authorized users to access the third-party robot, c) enable a semi-decentralized infrastructure with data being saved in an off-chain database. These avoid the risks of loosing identity keys used by manufactures and entities to access the private blockchain, as data can be also stored in an off-chain database. The main *cons and risk* of this combination of technologies is still the need

of central authorities, such as the off-chain database, to control and store data. The main *trade-off* is regarding the privacy and transparency of data, as data should be spread in the network. For this reason, data marked as privacy should follow different policies with the support of smart contracts.

The second solution is the use of digital twins to represent the third-party robot in the production line. The communication of IoT devices to cloud are through communications MQTT protocol. The MQTT protocol is a simple application layer protocol used to transport messages between IoT devices and infrastructure. The data in the MQTT protocol are transported in a textured, structured JSON format to the cloud. The *pros and opportunities* of this decision is digital twins follow standardized structure to simulate the whole production line. Besides, it provides data regarding the physical and logical devices, which can be used to prevent failures or delays in the third-party robot and in the whole production line. The *assumptions and quantifications* of adopting digital twins is the unique identifiable state of each entity in the simulate system. The *cons and risks* is related to collect unnecessary data that must be stored. The *trade-offs* is regarding the costs to configure and simulate the real product line scenario.

The third solution is the use of a service-oriented middleware as a communication channel between the third-party robot and product line systems. The *pros and opportunities* of this solutions is it provides the necessary services to enable the compatibility of data according to policies and rules and describes the syntactic and semantic communication protocol for exchanging data. The *cons and risks* is regarding the difficulty to ensure real-time compliance among third-party robot and the production line systems that interacts with the robot. This is because it is often very difficult to get in-depth data view of a large physical system. The *trade-offs* includes the standardization vs flexibility of the communication channel.

6.4 Instantiation design

The purpose of TIBA is to provide directions and guidelines presented as an architecture view to promoting trustworthy interoperability between the third-party industrial robot and the product line systems. TIBA architecture encompasses the architecture drivers and architecture solutions described previously.

The design of this architecture follows the C4 model, which is represented with three levels of architecture representation (Vazquez-Ingelmo; Garcia-Holgado; Garcia-Penalvo, 2020; LEANPUB, 2017): *(i) Context view* to represent the third-party industrial robot and the automated pallet transport system; *(ii) Container view* to represent the main components used to represent the interoperability for this instantiation; *(iii) Component view* describes the collaboration between the third-party industrial robot and the automated pallet transport system and main functionalities and flow of messages.

Context view

The *Context View* (Figure 24) presents the entities ManufacturerA and ManufacturerB interacting with TIBA to exchange data. The *third party industrial robot* must be compatible with the *automated pallet transport system* to exchange and communicate properly. TIBA provides the main services and for the interoperability of these entities.

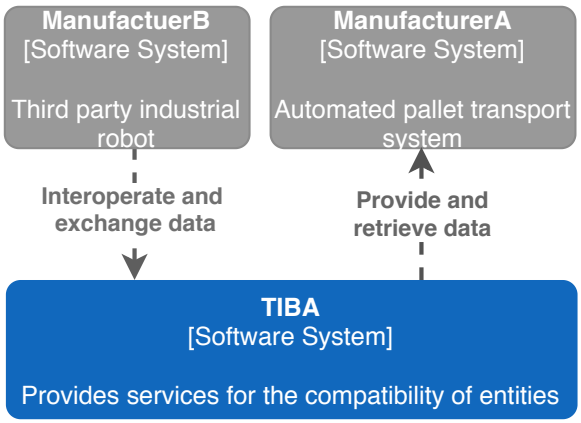

Figure 24 – Context View

Container view

The interoperability of the third-party robot into the automated pallet systems counts with seven main quality containers designed to provide services for trustworthy interoperability (Figure 25). This view presents the high-level structure of the architecture and an overview of the solutions using the blockchain and off-chain database. The container view provides guidelines on how each container regarding the quality aspects for trustworthy interoperability should be defined and the way they can interact in turn to promote trustworthy interoperability.

Component view

The *Component View*, shown in Figure 26, presents the collaboration between the different components to provide the main services and systems for trustworthy interoperability between the *third party industrial robot* and the *automated pallet transport system*.

The component **Authentication management** provides services to manage the identity of entities and manage their lifecycle. This component is responsible for the implementation of a primary smart contract with rules for accessing the system. The manufacturer B and its third-party industrial robot receive an invitation containing an identification key to access the automated pallet transport system and the production line system from manufacturer A. Manufactures A inserts the identification of the third-party industrial robot into the private blockchain. The **Smart contract for authentication** checks the validity of the authentication key to authorized the third-party robot to have access to the system.

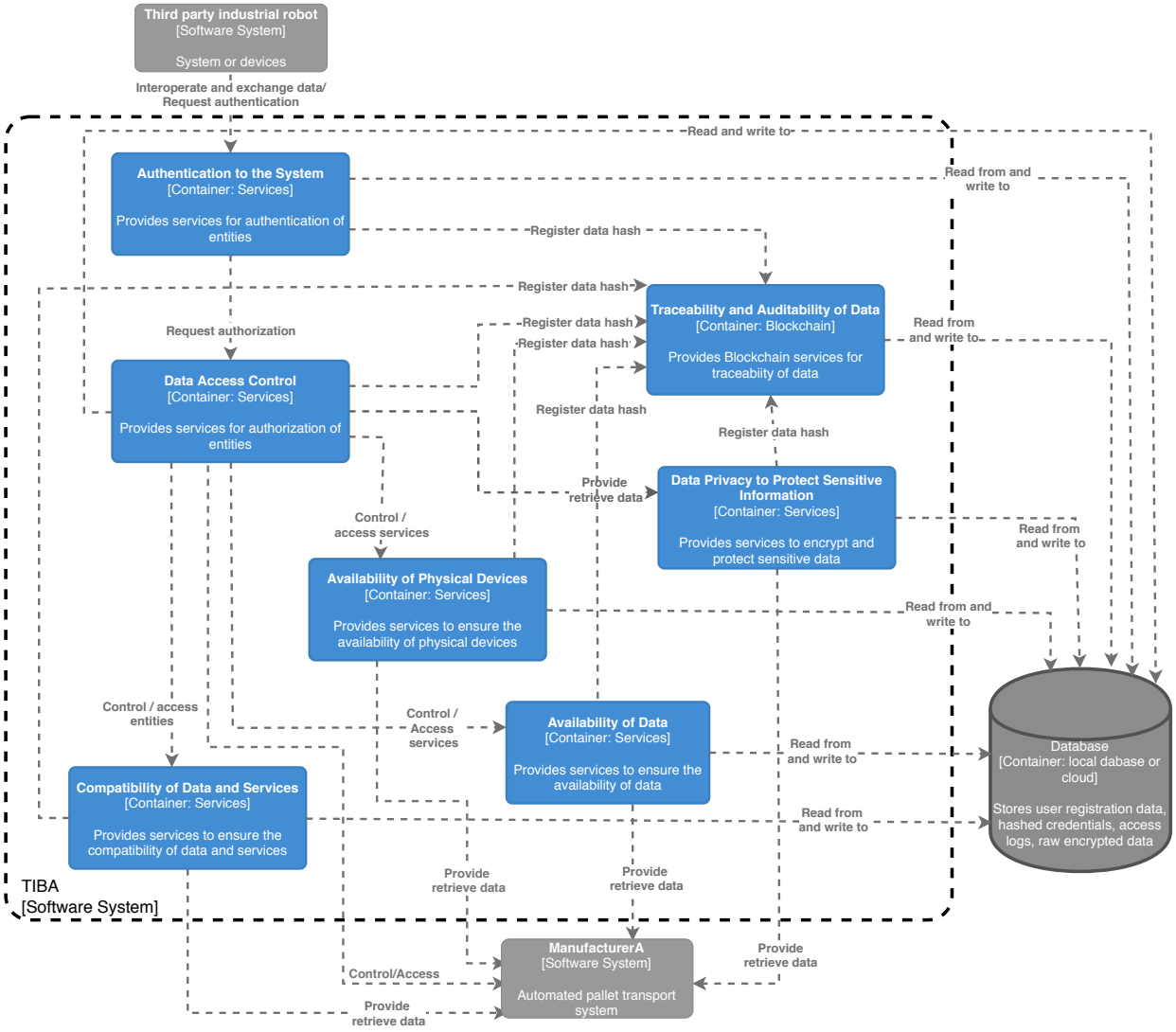

Figure 25 – Container view

The component **Access control management** provides the service for managing the privileges for each entity to the system. Previous access control rules exist in form of the smart contract. Manufacturer B requests a Token to access a service and to integrate the industrial robot into the automated pallet transport system. The **Smart contracts for authorization** verify the identity of the Manufacturers B and from the third-party industrial robot and provide the IDs and the address for access to the specific service that will be used by the third-party robot into the autonomous transport system.

The **Digital Twin** component provides the services for real-time monitoring of data from each entity being part of the product line. Data collected includes the physical and logical specifications from the third-party robot, power consumption, speed, weight, and any data sent and received by the robot. These data are stored in an off-chain database.

The **Middlware** component provides services to define the compatibility between the third-party industrial robot and the automated transport pallet system. This component is con-

nected to **Protocol service** responsible for providing the services for translating and mapping data to policies and protocols rules and the component **Policies and rules** responsible for providing the policies and composition rules to translate the syntactic and semantic data from the third-party robot. Any different semantic or syntactic protocols outside the ones defined in the protocol and policies rules for compatibility are not allowed due to security reasons.

The component **Private blockchain** contains all nodes stored in the private blockchain. It also provides traceability and data encryption. The private blockchain records every step of the third-party robot and the systems related to the autonomous transport system in a process chain. From the raw material to the final product, tracking what was changed, in which way, and who made the changes. Data collected is encrypted and stored in the off-chain database. A hash key for each transaction is created and pointed to the raw data stored in the off-chain database. Each hash is stored in the blockchain and shared by all members for further auditablity. Each member can retrieve the hash, which points to the raw data stored in the database, and keeps track of each transaction between entities.

6.5 Main findings and limitations

The scenario of the automated transport system interoperating with a third party industrial robot brings many challenges regarding quality concerns. We based on the ISO/IEC 25010 to characterize the architecture drivers for interoperability in Industry 4.0. The architecture drivers proposed in this work cover the following quality attributes (ISO/IEC, 2011): Compatibility (referred to as Compatibility of Data and Services in this work), Reliability (Availability of Physical Devices and Data Availability), Security (Authentication to the System, Data Access Control, Data Privacy Control to Protect Sensitive Information, Traceability and Auditability of Data). This set provided us the quality attributes that must be jointly considered for designing a trustworthy interoperability architecture solution.

The novelty of this instantiation is the cooperation of different companies during the production of the workpiece, which integrates other companies' technologies into the manufacturing production line. This collaboration requires new forms of cooperation and agreement between companies on the way to produce goods and brings many challenges regarding trusting the whole production line. The architecture views for the instantiation presents more manageable parts of systems that can be better analyzed and developed. One of the strengths of these architecture views is the continuous use of explicit descriptions in every involved element, which can be further detailed within the diagrams bringing more comprehension of the software architecture being designed.

Achieving trustworthy interoperability in this real use case scenario requires recognition that its systems are comprised of subsystems and physical entities, and awareness of how they interact with each other in a cross-layer Industry 4.0 environment. The combination of

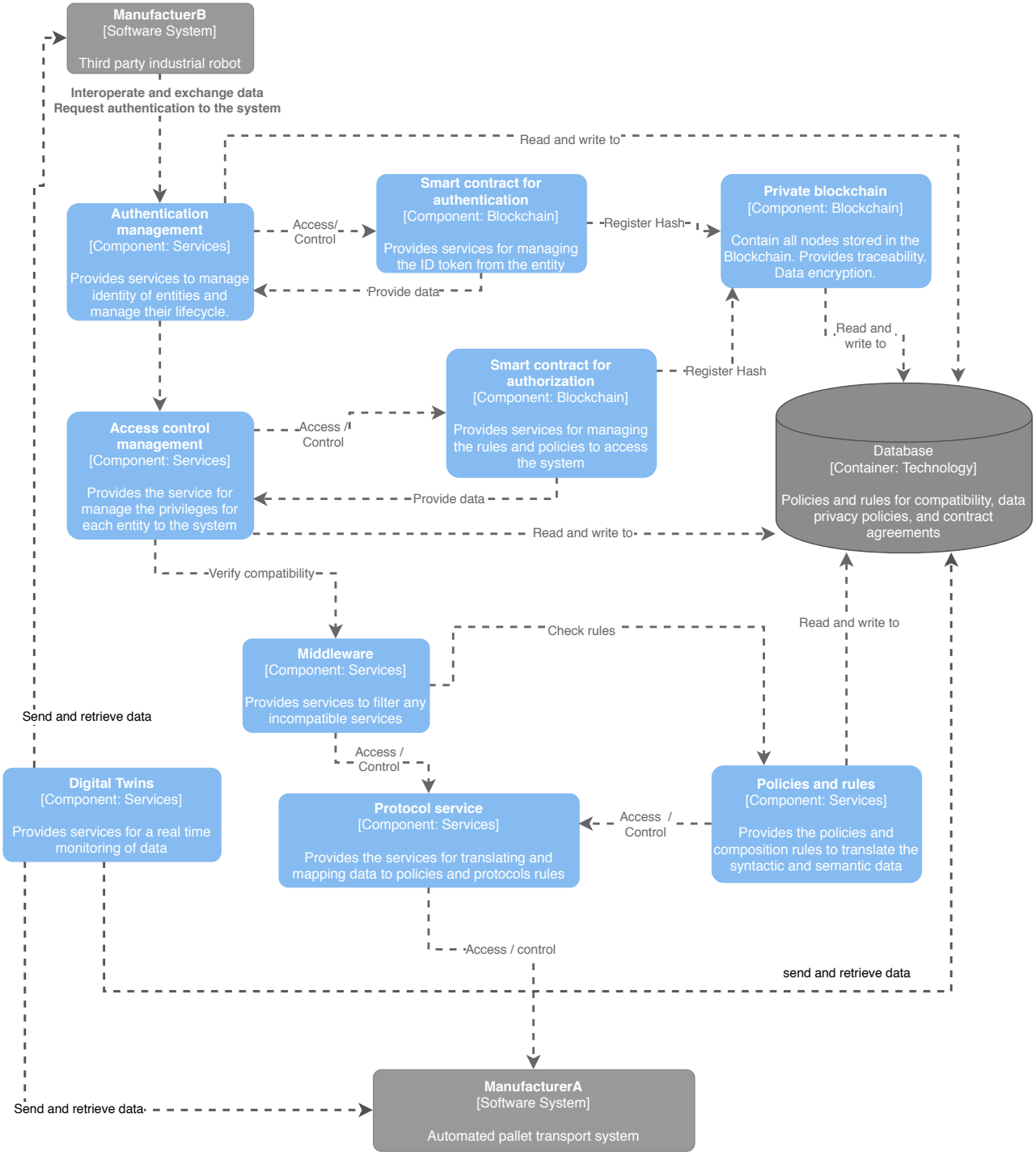

Figure 26 – Component View

private blockchain with traditional Industry 4.0 solutions provides more transparency, security, and reduce the risk of behavior from non-trusted parties. However, blockchain is still a new technology and how organizations adopt this technology also depends on how existing and related challenges are resolved.

We designed this instantiation to avoid bias as much as possible. The **external validity**

was minimized by considering real use case scenarios from Industry 4.0 partner. Besides, experts from Industry 4.0 gave feedback and opinion on how to improve it to properly fit the real use case scenario. The **internal validity** was mitigated by evaluating each phase in previous work with experts from Industry 4.0. TIBA is the result of this evaluation and its instantiation follows its guidelines. **Construct validity** refers to the relationship between theory and observation. To mitigate this threat, we conduct this work together with the supervision of experts in Industry 4.0. To minimize the bias regarding the **conclusion to validity**, we follow the previous step to define the architecture drivers and solutions. Based on this, we follow the guidelines proposed on TIBA to design the architecture views for this instantiation.

6.6 Final considerations

In the manufacturing environments, automation systems continue to become part of globally connected systems, meaning that intrusion attempts will increase and non-authorized access to information may also create a risk for the production process. Consequences can be in different areas or dimensions, such as interruption of an operation, modification of an operational process or sabotage with intention to cause harm. Manipulating or interrupting such systems could also affect safety in the Industry 4.0, which can have consequences such as environmental damage, injury or loss of life. Therefore, to maximize the trustworthy interoperability among the entities, this chapter presented how TIBA can be instantiated considering a real use case scenario from Industry 4.0. The instantiation must start by analyzing the use case scenario in the holistic of architecture drivers. Towards these drivers, architecture solutions are defined and proposed. TIBA provides the guidelines to design these solutions based on seven quality aspects that must be consider for creating trustworthy interoperability solutions for Industry 4.0.

CHAPTER

7

CONCLUSION AND FUTURE WORK

7.1 Final conclusion

The companies' collaboration is placing high demands on all areas of industry, including technology, security, organization process, and laws. In this context, trustworthy interoperability in Industry 4.0 highlights the importance of proper agreements and collaboration contracts to support future demands of services and products. This work introduces TIBA, a novel blockchain-based architecture to deal with different aspects of interoperability in Industry 4.0. TIBA focuses on interoperability aspects between manufacturers and clients, increasing the trust to develop products and services. Trustworthy interoperability at different levels, ranging from technical to organizational interoperability, is crucial for setting up Industry 4.0 operations. The main innovation of this work is to provide the essential requirements that can assure the trustworthy interoperability in Industry 4.0 systems, represented as architecture drivers — *Authentication to the System, Data Access Control, Data Privacy to Protect Sensitive Information, Traceability and Auditability of Data, Availability of Physical Devices, Availability of Data,* and *Compatibility of Data and Services* — that should be jointly implemented.

While the seven architecture drivers can serve as a set of core requirements that together assure trustworthy interoperability in Industry 4.0 systems, the architectural solutions presented in this work go further by directly supporting architectural decisions, which were based on a real-world system of a partner of the BaSyS 4.0 project[1]. The main feature of this system is the digitalization of an automated transport system to move workpieces throughout the shop floor. This system includes roller conveyors, shift tables, turntables, many sensors that control speed, temperature, position, and shift of the workpieces, as well as high-level systems, i.e., ERP and Customer Relationship Management (CRM). It also includes a digital twin, which refers to a virtual copy of the entire platform and provides information, such as the status of the transport system occupation, status of workpieces, and localization. All parts of this system are

[1] <https://www.basys40.de/>

interconnected with each other and interoperate with many other systems and users inside and outside the production line, including a third-party robot. All end-to-end communication crosses multiple levels of the automation pyramid and is made possible by the VAB, which bridges the gaps between different communication protocols.

The novelty of the scenario presented in this work is the need for trustworthy interoperability of the third-party robot with the entities of the automated transport system. Scenarios like this are becoming increasingly common in the Industry 4.0 context[2]. The third-party robot must be compatible with the automated transport system to properly exchange data and communicate with all entities of this system. This raises requirements related to trustworthy interoperability: (i) authorized users and entities may be allowed to access the system and its components; (ii) every step in the production of workpieces must be tracked and protected, including the step in which the workpieces pass through the third-party robot; (iii) devices, data, and systems must be available to complete the production of workpieces; and (iv) communication among heterogeneous entities inside and outside the production line, including the third-part robot, must be assured.

The flexibility of our architecture drivers make it possible to adopt different relevant studies already conducted in the past (which sometimes present individual, technical solutions, including a large set of interoperability standards) to cover the requirements stated by each driver. We highlight that works like ours are important at this stage of Industry 4.0 development as they pave the way by guiding the architecture design solutions of large and complex software-intensive systems, which are essential for making Industry 4.0 a reality. At the top of the available solutions, blockchain promises to increase the degree of trust, changing the way transactions are done based on the immutability of records and transparent and trustworthy interactions among users and other entities. In this scenario, architecture solutions for trustworthy interoperability in Industry 4.0 systems were presented in this work. Founded on the knowledge and experience of highly trained experts in Industry 4.0 and blockchain, these solutions can guide architectural decision-making when it comes to whether or not to adopt blockchain and, more importantly, in which situations. We conclude that, in most situations, blockchain needs to be combined with traditional technologies/solutions to promote fully trustworthy interoperability. We also claim that the importance of this work does not lie in providing the best solution for trustworthy interoperability, but rather in supporting software architects and researchers in systematizing the design of proper solutions for their projects.

The path to mainstream use of blockchain in Industry 4.0 is still long. It includes its use in other real-world applications to mainly get evidence about its impact on quality attributes (by getting quantitative data on, for instance, performance, safety, security, privacy, and others), on the maintenance of the Industry 4.0 systems and their components, and the availability of

[2] An example of smart manufacturing cooperation can be found at https://www.boschrexroth.com/en/xc/company/press/index2-31616

technologies and their compatibility. TIBA provides an interoperability infrastructure, in which users have a new relationship with data being transmitted. Instead of trusting the source of data from a central provider, users can have direct access to information defined in upper levels of interoperability through smart contracts. In TIBA, smart contracts are synchronized with each trustworthy component, so data of transactions is stored in the blockchain. The evaluation of this work counts with surveys and interviews with experts of Industry 4.0 and blockchain. Besides, TIBA encompasses architectural views for the continuous use of explicit descriptions in every involved element, which brings the first guideline to support architecture identifies the main components to promote trustworthy interoperability and how they can combine blockchain with traditional solutions. These architectural views can be further detailed within other UML diagrams bringing more comprehension of the software architecture being designed.

7.2 Main contributions

The main contributions of this thesis are framed in topics of Industry 4.0, interoperability, software architecture, and are summarized as follows:

Quality concerns for trustworthy interoperability in Industry 4.0: An SLR was investigating studies proposing means to promote trust in interoperability in Industry 4.0 were conducted following the guidelines proposed in (KITCHENHAM; CHARTERS, 2007). The analysis of the SLR provided us evidence of the lack of studies that encompass these main quality aspects that can further affect the whole architecture. Architectural solutions for interoperability in Industry 4.0 must be first designed by identifying the main quality aspects that can interfere with the whole project. To support this identification, we found that use case scenarios and specific requirements for Industry 4.0 should also be analyzed (Polonia; Melgarejo; de Queiroz, 2015; Sisinni *et al.*, 2018; XU; XU; LI, 2018; Habib; Chimsom, 2019).

Architecture drivers for trustworthy interoperability in Industry 4.0: Seven architectural drivers for promoting trustworthy interoperability in Industry 4.0 were defined and centered on security (cf. Authentication to the System, Data Access Control, Data Privacy to Protect Sensitive Information, Traceability and Auditability of Data, Availability of Data, Availability of Physical Devices, and Compatibility of Data and Services). Representing the seven quality concerns using architecture drivers has benefits. This is because by definition: (i) architecture drivers delineate only the significant requirements (and information related to them) needed to implement and maintain software-intensive systems, which in our case refers to Industry 4.0 systems; (ii) a set of architecture drivers for a given purpose must not overlap in terms of content (i.e., there must be no redundant information) and, at the same time, each one must be self-contained (making it also possible for each one to be used independently without the obligation to adopt others); (iii) architecture drivers make it possible to avoid costly and risky decisions; (v) by nature, architecture drivers must be presented at a higher level of

abstraction, and (iv) they can often determine the success or failure of projects. Hence, we recommend the adoption of architecture drivers as a first key step for developing large, complex software-intensive systems, such as systems-of-systems and ultra-large-scale systems for different challenging application domains. Hence, for instance, if failures occur in the production line containing several virtual and physical entities interconnected, manufactures can access traced data records thought the *Traceability and Auditability of Data* service. This increases trust by empowering the manufacturers and stakeholders involved to have more control over their production line, by clarifying issues, and by preparing them for the further evolution of their production lines.

Architecture solutions for the architecture drivers: The adoption of blockchain as a solution to revolutionize the interactions among entities that require high degree of trustworthy communication in Industry 4.0 has still divided the opinion of who has been in fact directly involved in Industry 4.0 projects. Because of the distributed nature of blockchain, data can be more transparent, preventing fraudulent behavior from non-trusted parties. A private blockchain is a good solution when different parties are involved in a production line and must be well-known by the other participants. Manufacturers, suppliers, and customers have data assurance; transactions are tracked and accessed transparently (cf. solution for *Traceability and Auditability Data*) or can be protected by cryptography, which prevents sensitive data from being accessed by non-authorized users (cf. solution for *Data Privacy to Protect Sensitive Information*). It increases *data transparency* and facilitates *data traceability* in Industry 4.0 production lines. Blockchain cannot guarantee data availability for users, but only a hash pointing to the data. Hence, blockchain cannot solve the drivers *Availability of Data*, *Availability of Physical Devices*, and *Compatibility of Data and Services*. The adoption of blockchain alone does not solve the requirements of fully trustworthy interoperability in Industry 4.0 projects. Blockchain must be combined with traditional solutions from Industry 4.0, such as digital twins, service-oriented middleware, security protocols to ensure the identification and authorization of each entity connected in the production line.

Experts opinions summarized in interviews: Surveys and interviews were conducted with experts highly trained in both Industry 4.0 and blockchain. These experts provided important improvements for the seven architecture driver and architecture solution presented in this work. These improvements were regarding specific adjustments to fit better the architecture drivers into Industry 4.0 context and improvements related to the adoption or not of blockchain technology. These interviews were systematic analyzed based on procedures from Grounded Theory methodology. The opinions of experts regarding the adoption of blockchain as a solution for Industry 4.0 are still divided.

Design of the architecture for trustworthy interoperability in Industry 4.0: This activity described in Chapter 5 is related to document architecture solution decisions in architecture views. To systematize the design of TIBA, we followed the modeling profile from the C4 model,

which proposes four levels of abstraction to represent the architecture: i) context, ii) containers, iii) components, and iv) code. The C4 Model translate the architecture drivers previously defined, which encompass quality attributes, functional requirements, and constraints into a technical view, creating the overall structure of the system.

Instantiation of architecture for trustworthy interoperability in Industry 4.0: During this activity, TIBA was instantiated in the considering the digitalization of an automated transport system based on a real project from one of the partners of the BaSyS 4.0 project. The novelty of this use case scenario was the inclusion of a third-party industrial robot into the production line process. The architecture instantiation supports the derivation of systems artifacts and propagation of the design decisions to source code.

7.3 Limitations and future works

In this section, limitations of this thesis are presented as well as some approaches that can be used to tackle them in the future.

The architecture drivers defined in this work do not consider malicious attacks made by users who are authenticated in Industry 4.0 systems. Besides, the social and cultural aspects of trust in terms of human behavior are not addressed in this work because these must embrace principles regarding human resources management, which encompasses many psychological concerns related to identifying whether a person is reliable or not when it comes to working reliably in a manufacturing environment.

Solutions for the drivers *Availability of Data* and *Availability of Physical Devices* are suitable in this case. Blockchain is not a good solution to assure data availability due to performance reasons when a large amount of data is in the chain. Besides, blockchain does not guarantee the availability of devices. Hence, another solution is necessary. In this case, a digital twin of the entire automated transport system is adopted to create a virtualized platform. This digital twin provides unified real-time data access regarding the behavior of real-world environment and entities (i.e., data flow, production machine, operational processing status, functionalities, sensors, and also the third-party robot). This twin supports predictive maintenance aimed at diagnosing problems and monitors services to quickly identify and remediate anomalies regarding maintenance, such as rules, events, and triggers, to identify issues.

Blockchain provides provenance services by recording evidence of the data's originality and the operations in the chain, which are also accessible only for authorized users and devices. In summary, blockchain can store each step of the workpieces, without the intermediation of third parties. However, its main drawback is the limited storage space and the lack of performance to manage data. For these reasons, cryptography functions and off-chain databases must be combined with blockchain.

Solutions for recoverability of data, including redundancy services, storage in the cloud, and backup servers to recover the last data, must also be implemented. The main drawback of these solutions is the cost to maintain redundant devices and systems available at any time. The need to assure requirement communication among heterogeneous entities inside and outside the production line also leads to the need for the third-party robot to be compatible with the automated transport system.

The implementation of the solution for the driver *Compatibility Data and Service* is recommended in this case. Blockchain is no suitable in this case because it does not provide automated or intelligent means to translate and map the data that must be exchanged between the third-party robot and the automated transport system. Hence, a specific communication channel is necessary for which all entities connected to it are typed and have well-defined properties. Additionally, a service-oriented middleware provides the necessary services to enable the compatibility of data according to policies and rules and describes the syntactic and semantic communication protocol for exchanging data. The main drawback of this solution is how to ensure real-time compliance among entities when different semantic and syntactic types are identified and need to be translated and mapped to allow proper compatibility.

Regarding future works, possible extensions and opportunities of research emerged during the development of this thesis. Some of them are the conduction of new interviews and surveys with experts of Industry 4.0 to identify other solutions for trustworthy interoperability. Creation of guidelines to support architect identify each trustworthy interoperability aspect to be implemented in their own Industry 4.0 context. Evaluation of the architecture drivers using formal representation and analysis of interoperability to verify the effectiveness of each quality aspect identified in this work. The formal representation is required to allow the verification and development of code regarding each quality aspect. Towards the formal representation, new ways to represent TIBA architecture views should be defined by using other languages and models. Instantiation of TIBA considering other context such as IoT systems.

REFERENCES

Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In: **2017 IEEE Technology Engineering Management Conference (TEMSCON)**. [S.l.: s.n.], 2017. p. 137–141. Citation on page 27.

AL-ALI, R.; BURES, T.; HARTMANN, B.-O.; HAVLIK, J.; HEINRICH, R.; HNETYNKA, P.; JUAN-VERDEJO, A.; PARIZEK, P.; SERMANN, S.; WALTER, M. **Use Cases in Dataflow-Based Privacy and Trust Modeling and Analysis in Industry 4.0 Systems**. [S.l.], 2018. (Karlsruhe Reports in Informatics, 9). Citation on page 41.

AL-ALI, R.; HEINRICH, R.; HNETYNKA, P.; JUAN-VERDEJO, A.; SEIFERMANN, S.; WALTER, M. Modeling of dynamic trust contracts for industry 4.0 systems. In: **European Conference on Software Architecture (ECSA)**. Madrid, Spain: [s.n.], 2018. p. 45:1–45:4. Citations on pages 26, 27, and 79.

Alladi, T.; Chamola, V.; Parizi, R.; Choo, K. Blockchain applications for industry 4.0 and industrial IoT: A review. **IEEE Access**, v. 7, p. 176935–176951, 2019. Citation on page 80.

ALLHOFF, F.; HENSCHKE, A. The internet of things: Foundational ethical issues. **Internet of Things**, v. 1-2, p. 55 – 66, 2018. Citation on page 25.

ALLIAN, A. P. Promoting trust in interoperability of systems-of-systems. In: **European Conference on Software Architecture (ECSA)**. Paris, France: [s.n.], 2019. p. 67–70. Citation on page 26.

Anjum, A.; Sporny, M.; Sill, A. Blockchain standards for compliance and trust. **IEEE Cloud Computing**, v. 4, n. 4, p. 84–90, 2017. Citations on pages 27 and 80.

ANTONINO, P. O.; SCHNICKE, F.; ZHANG, Z.; KUHN, T. Blueprints for architecture drivers and architecture solutions for industry 4.0 shopfloor applications. In: **European Conference on Software Architecture (ECSA)**. Paris, France: ACM, 2019. p. 261–268. Citations on pages 15, 23, 34, 35, 44, 55, 63, 84, 85, 99, and 101.

BASS, L.; CLEMENTS, P.; KAZMAN, R. **Software Architecture in Practice**. 3. ed. [S.l.]: Addison-Wesley, 2012. Citations on pages 24 and 36.

Bicaku, A.; Maksuti, S.; Palkovits-Rauter, S.; Tauber, M.; Matischek, R.; Schmittner, C.; Mantas, G.; Thron, M.; Delsing, J. Towards trustworthy end-to-end communication in industry 4.0. In: **IEEE International Conference on Industrial Informatics (INDIN)**. Emden, Germany: [s.n.], 2017. p. 889–896. Citations on pages 26, 27, 41, 54, and 79.

BOSCH. **State of Play of Interoperabilityin Europe**. [S.l.], 2016. 1–52 p. Accessed on September 2020. Available: <https://snig.dgterritorio.gov.pt/sites/default/files/documentos/372/report_2016_rev9_single_pages.pdf>. Citation on page 36.

____. **Bosch Rexroth presents collaborative robot based on KUK**. [S.l.], 2020. 1–3 p. Accessed on September 2020. Available: <https://dc-corp.resource.bosch.com/media/xc/company_

1/press/corporate_information/pi_year_2018/04_april_2/PI_009_18_APAS_en.pdf>. Citation on page 99.

BURNABY, P.; HOWE, M.; MUEHLMANN, B. W. Detecting fraud in the organization: an internal audit perspective. **Journal of Forensic & Investigative Accounting**, v. 3, n. 1, p. 195–233, 2011. Citation on page 26.

Castelluccia, C.; Cunche, M.; Le Metayer, D.; Morel, V. Enhancing transparency and consent in the iot. In: **IEEE European Symposium on Security and Privacy Workshops (EuroS PW)**. London, United Kingdom: [s.n.], 2018. p. 116–119. Citation on page 25.

CHARALABIDIS, Y.; LAMPATHAKI, F.; ASKOUNIS, D. A review of interoperability standards and initiatives in electronic government. In: POULYMENAKOU, A.; POULOUDI, N.; PRAMATARI, K. (Ed.). **The 4th Mediterranean Conference on Information Systems, MCIS**. Athens, Greece: Athens University of Economics and Business / AISeL, 2009. p. 128. Citation on page 36.

Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. **IEEE Access**, v. 4, p. 2292–2303, 2016. Citations on pages 27, 45, and 80.

Condry, M. W.; Nelson, C. B. Using smart edge iot devices for safer, rapid response with industry iot control operations. **Proceedings of the IEEE**, v. 104, n. 5, p. 938–946, 2016. Citations on pages 52, 54, and 76.

Delsing, J. Local cloud internet of things automation: Technology and business model features of distributed internet of things automation solutions. **IEEE Industrial Electronics Magazine**, v. 11, n. 4, p. 8–21, 2017. Citations on pages 42, 52, 53, 54, and 55.

DOBAJ, J.; IBER, J.; KRISPER, M.; KREINER, C. A microservice architecture for the industrial internet-of-things. In: **Proceedings of the 23rd European Conference on Pattern Languages of Programs (EuroPLoP)**. Irsee, Germany: ACM, 2018. p. 11:1–11:15. Citations on pages 53, 54, and 55.

DURAND, A.; GREMAUD, P.; PASQUIER, J. Decentralized web of trust and authentication for the internet of things. In: **7th International Conference on the Internet of Things (IoT)**. Linz, Austria: ACM, 2017. p. 27:1–27:2. Citation on page 46.

DYCK, A.; MORSE, A.; ZINGALES, L. **How Pervasive is Corporate Fraud?** [S.l.], 2014. 1–56 p. Available on Decebme 2020. Available: <http://dx.doi.org/10.2139/ssrn.2222608>. Citation on page 25.

EIF. **The New European Interoperability Framework**. 2017. Accessed in 2018. Available: <https://ec.europa.eu/isa2/eif>. Citation on page 24.

EKBLAW, A.; AZARIA, A.; HALAMKA, J. D.; MD; LIPPMAN, A. **A Case Study for Blockchain in Healthcare: MedRec prototype for electronic healthrecords and medical research data**. Cambridge, Massachusetts, USA, 2016. 1–13 p. Accessed on December 2020. Available: <https://dci.mit.edu/research/blockchain-medical-records>. Citation on page 45.

EUBLOCKCHAIN. **Blockchain for Government and Public Services**. [S.l.], 2018. Accessed on December 2020. Available: <https://www.eublockchainforum.eu>. Citations on pages 27 and 45.

Fernandez-Carames, T. M.; Fraga-Lamas, P. A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. **IEEE Access**, v. 7, p. 45201–45218, 2019. Citations on pages 27 and 80.

FORECARE. **Interoperability comes at the speed of trust**. [S.l.], 2018. Accessed on December 2019. Available: <https://www.owler.com/reports/forcare/forcare-blog-interoperability-comes-at-the-speed-o/1513164481809>. Citation on page 24.

FRAGAPANE, G.; IVANOV, D.; PERON, M.; SGARBOSSA, F.; STRANDHAGEN, J. O. Increasing flexibility and productivity in Industry 4.0 production networks with autonomous mobile robots and smart intralogistics. **Annals of Operations Research**, v. 293, p. 1–19, 2020. Citation on page 99.

Fraile, F.; Tagawa, T.; Poler, R.; Ortiz, A. Trustworthy industrial iot gateways for interoperability platforms and ecosystems. **IEEE Internet of Things Journal**, v. 5, n. 6, p. 4506–4514, 2018. Citations on pages 26, 27, 41, 54, and 55.

GAZQUEZ, J. L. R.; BUENO-DELGADO, M. V. Software architecture solution based on sdn for an industrial iot scenario. **Wireless Communications and Mobile Computing**, v. 2018, n. 2946575, p. 1–14, 2018. Citation on page 55.

Golosova, J.; Romanovs, A. The advantages and disadvantages of the blockchain technology. In: **IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)**. Vilnius, Lithuania: [s.n.], 2018. p. 1–6. Citation on page 27.

GORDON, W. J.; CATALINI, C. Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. **Computational and Structural Biotechnology Journal**, v. 16, p. 224 – 230, 2018. ISSN 2001-0370. Citation on page 45.

GRIDWISE. **GridWise Interoperability Context-Setting Framework**. [S.l.], 2008. Accessed on December 2020. Available: <https://www.gridwiseac.org/pdfs/interopframework_v1_1.pdf>. Citation on page 24.

GRILO, A.; JARDIM-GONCALVES, R. Value proposition on interoperability of bim and collaborative working environments. **Automation in Construction**, v. 19, n. 5, p. 522 – 530, 2010. Building Information Modeling and Collaborative Working Environments. Citation on page 24.

GUERREIRO, S.; GUÉDRIA, W.; LAGERSTRÖM, R.; KERVEL, S. van. A meta model for interoperability of secure business transaction using blockchain and demo. In: **9th International Conference on Knowledge Engineering and Ontology Development (KEOD)**. Madeira, Portugal: [s.n.], 2017. Citation on page 45.

Habib, M. K.; Chimsom, C. 20th international conference on research and education in mechatronics (rem). In: **REM**. Wels, Austria: [s.n.], 2019. p. 1–8. Citations on pages 42, 53, 54, 55, and 113.

HAWLITSCHEK, F.; NOTHEISEN, B.; TEUBNER, T. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. **Electronic Commerce Research and Applications**, v. 29, p. 50 – 63, 2018. Citations on pages 27 and 80.

HEADAYETULLAH, M.; PRADHAN, G. K. Interoperability, trust based information sharing protocol and security: Digital government key issues. **Computing Research Repository**, ACM, abs/1006.1198, 2010. Citations on pages 23, 24, 26, 34, and 46.

HERMANN, J.; RÜBEL, P.; RUSKOWSKI, M. Development of a system architecture enabling a dynamic generation of process chains for production as a service. In: **IEEE Conference on Industrial Cyberphysical Systems, ICPS**. Tampere, Finland: IEEE, 2020. p. 15–20. Citation on page 98.

HEVNER, A. R.; MARCH, S. T.; PARK, J.; RAM, S. Design science in information systems research. **MIS Quarterly**, Society for Information Management and The Management Information Systems Research Center, v. 28, n. 1, p. 75–105, 2004. Citation on page 28.

HOFER, F. Architecture, technologies and challenges for cyber-physical systems in industry 4.0: A systematic mapping study. In: **ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)**. Oulu, Finland: ACM, 2018. p. 1:1–1:10. Citation on page 42.

IEEE Recommended Practice for Architectural Description for Software-Intensive Systems. **IEEE Std 1471-2000**, p. 1–30, 2000. Citation on page 42.

Imtiaz, J.; Jasperneite, J. Scalability of opc-ua down to the chip level enables "internet of things". In: **11th IEEE International Conference on Industrial Informatics (INDIN)**. Bochum, Germany: [s.n.], 2013. p. 500–505. Citation on page 53.

ISO/IEC. **Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE)–System and software quality models**. [S.l.]: ISO, Geneva, Switzerland, 2011. Citations on pages 28, 36, and 108.

IWANICKI, K. A Distributed Systems Perspective on Industrial IoT. In: **IEEE 38th International Conference on Distributed Computing Systems (ICDCS)**. Vienna, Austria: [s.n.], 2018. p. 1164–1170. Citations on pages 42, 52, 53, and 55.

Jin, H.; Dai, X.; Xiao, J. Towards a novel architecture for enabling interoperability amongst multiple blockchains. In: **IEEE 38th International Conference on Distributed Computing Systems (ICDCS)**. Vienna, Austria: [s.n.], 2018. p. 1203–1211. Citation on page 46.

JUNGO, C. **Integrity and trust in the Internet of Things**. [S.l.], 2015. Accessed on March 2020. Available: <https://www.swisscom.ch/dam/swisscom/en/about/responsibility/digital-switzerland/security/documents/integrity-and-trust-in-the-internet-of-things.pdf>. Citations on pages 26 and 46.

KAGERMANN, H.; HELBIG, J.; HELLINGER, A.; WAHLSTER, W. **Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0: Securing the Future of German Manufacturing Industry ; Final Report of the Industrie 4.0 Working Group**. Forschungsunion, 2013. Available: <https://books.google.de/books?id=AsfOoAEACAAJ>. Citations on pages 15 and 34.

KAUR, K.; SELWAY, M.; GROSSMANN, G.; STUMPTNER, M.; JOHNSTON, A. Towards an open-standards based framework for achieving condition-based predictive maintenance. In: **8th International Conference on the Internet of Things (IOT)**. Santa Barbara, California, USA: ACM, 2018. p. 16:1–16:8. Citation on page 54.

KITCHENHAM, B.; CHARTERS, S. **Guidelines for performing Systematic Literature Reviews in Software Engineering**. [S.l.], 2007. 57 p. Citations on pages 29, 50, 66, and 113.

KIZZA, J. M. **Ethical and Social Issues in the Information Age**. 5th. ed. [S.l.]: Springer Publishing Company, Incorporated, 2013. ISBN 1447149890, 9781447149897. Citation on page 25.

KJERSGAARD, J.; ERIKSENA, M. **ACCESS CONTROL FOR INDUSTRY 4.0 Initial Trust with Blockchain**. Aalborg, Denmark, 2018. 1–99 p. Accessed on March 2020. Available: <https://projekter.aau.dk/projekter/files/281557079/>. Citations on pages 26, 27, 41, and 46.

KJERSGAARD, J.; ERIKSENA, M.; HARLAMOVA, M. **Industry 4.0 Security Trust and Access Control in Industry 4.0**. Bydgoszcz, Poland, 2018. 1–29 p. Accessed on April 2019. Available: <http://epic.utp.edu.pl/epic/resources/CyberSecurity>. Citations on pages 26, 27, 41, and 46.

KNODEL, J.; NAAB, M. **Pragmatic Evaluation of Software Architectures**. Germany: Springer, 2016. 170 p. Citations on pages 15, 43, 44, 57, 74, 84, 85, and 95.

Kolluru, K. K.; Paniagua, C.; van Deventer, J.; Eliasson, J.; Delsing, J.; DeLong, R. J. An aaa solution for securing industrial iot devices using next generation access control. In: **IEEE Industrial Cyber-Physical Systems (ICPS)**. St. Petersburg, Russia: [s.n.], 2018. p. 737–742. Citation on page 52.

KUHN, T.; ANTONINO, P. O.; DAMM, M.; MORGENSTERN, A.; SCHULZ, D.; ZIESCHE, C.; MüLLER, T. Industrie 4.0 virtual automation bus. In: **40th International Conference on Software Engineering (ICSE)**. Gothenburg, Sweden: Association for Computing Machinery, 2018. p. 121–122. Citations on pages 34, 35, and 99.

KUHN, T.; SADIKOW, S.; ANTONINO, P. O. A service-based production ecosystem architecture for industrie 4.0. **Künstliche Intell.**, v. 33, n. 2, p. 163–169, 2019. Citation on page 98.

KWON, J.; ETHANBUCHMAN. **Cosmos - A Network of Distributed Ledgers**. [S.l.], 2019. 1–53 p. Accessed on December 2020. Available: <https://cosmos.network/cosmos-whitepaper.pdf>. Citation on page 45.

LEANPUB (Ed.). **Software Architecture for Developers**. [S.l.: s.n.], 2017. Citations on pages 30, 86, and 105.

LI, W.; PING, L. Trust model to enhance security and interoperability of cloud environment. In: JAATUN, M. G.; ZHAO, G.; RONG, C. (Ed.). **Cloud Computing**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. p. 69–79. Citations on pages 24, 26, and 46.

Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium blockchain for secure energy trading in industrial internet of things. **IEEE Transactions on Industrial Informatics**, v. 14, n. 8, p. 3690–3700, 2018. Citation on page 45.

LIN, C.; HE, D.; HUANG, X.; CHOO, K.-K. R.; VASILAKOS, A. V. Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. **Journal of Network and Computer Applications**, v. 116, p. 42 – 52, 2018. Citation on page 27.

LIN, S.-W.; MILLER, B.; DURAND, J.; BLEAKLEY, G.; CHIGANI, A.; MARTIN, R.; MURPHY, B.; CRAWFORD, M. **INDUSTRIAL INTERNET REFERENCE ARCHITECTURE v 1.8**. [S.l.], 2017. 1–2 p. Accessed on November 2020. Available: <https://www.iiconsortium.org/IIRA-1.8.htm>. Citations on pages 15 and 39.

Link, J.; Waedt, K.; Ben Zid, I.; Lou, X. Current challenges of the joint consideration of functional safety cyber security, their interoperability and impact on organizations: How to manage rams + s (reliability availability maintainability safety + security). In: **12th International Conference on Reliability, Maintainability, and Safety (ICRMS**. Shanghai, China: [s.n.], 2018. p. 185–191. Citation on page 80.

LU, Y. Industry 4.0: A survey on technologies, applications and open research issues. **Journal of Industrial Information Integration**, v. 6, p. 1 – 10, 2017. Citation on page 42.

MARTIN, K. E. Ethical issues in the big data industry. **MIS Quarterly Executive**, v. 14, n. 2, 2015. Citation on page 25.

Mohamed, N.; Al-Jaroodi, J. Applying blockchain in industry 4.0 applications. In: **IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)**. Las Vegas, NV, USA: [s.n.], 2019. p. 0852–0858. Citations on pages 26, 27, 46, 54, and 55.

MOLLÉRI, J. S.; PETERSEN, K.; MENDES, E. Survey guidelines in software engineering: An annotated review. In: **10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)**. Ciudad Real, Spain: ACM, 2016. p. 58:1–58:6. Citations on pages 56 and 81.

MORKUNAS, V. J.; PASCHEN, J.; BOON, E. How blockchain technologies impact your business model. **Elsevier Business Horizons**, p. 1–12, 2019. ISSN 0007-6813. Citation on page 45.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. [S.l.], 2009. 1–9 p. Accessed on December 2020. Available: <https://bitcoin.org/bitcoin.pdf>. Citations on pages 27 and 44.

NICHOL, P. B.; BRANDT, J. **Co-Creation of Trust for Healthcare: The Cryptocitizen Framework for Interoperability with Blockchain**. USA, 2016. 1–9 p. Accessed on December 2020. Available: <https://www.cio.com/article/3041641/person-centric-healthcare-amplified-by-blockchain.html>. Citation on page 45.

PAZAITIS, A.; FILIPPI, P. D.; KOSTAKIS, V. Blockchain and value systems in the sharing economy: The illustrative case of backfeed. **Technological Forecasting and Social Change**, v. 125, p. 105 – 115, 2017. ISSN 0040-1625. Citations on pages 27 and 45.

PERALTA, G.; CID-FUENTES, R. G.; BILBAO, J.; CRESPO, P. M. Homomorphic encryption and network coding in iot architectures: Advantages and future challenges. **Electronics**, v. 8, n. 8, 2019. ISSN 2079-9292. Citations on pages 54, 76, and 80.

PERERA, S.; NANAYAKKARA, S.; RODRIGO, M.; SENARATNE, S.; WEINAND, R. Blockchain technology: Is it hype or real in the construction industry? **Journal of Industrial Information Integration**, v. 17, p. 100125, 2020. Citation on page 27.

PETERSON, K.; DEEDUVANU, R.; KANJAMALA, P.; BOLES, K. **A Blockchain-Based Approach to Health Information Exchange Networks**. Phoenix, no Arizona, USA, 2016. 1–10 p. Accessed on December 2020. Available: <https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf>. Citation on page 45.

Petroulakis, N. E.; Lakka, E.; Sakic, E.; Kulkarni, V.; Fysarakis, K.; Somarakis, I.; Serra, J.; Sanabria-Russo, L.; Pau, D.; Falchetto, M.; Presenza, D.; Marktscheffel, T.; Ramantas, K.; Mekikis, P.; Ciechomski, L.; Waledzik, K. Semiotics architectural framework: End-to-end security, connectivity and interoperability for industrial iot. In: **Global IoT Summit (GIoTS)**. [S.l.: s.n.], 2019. p. 1–6. Citations on pages 41, 52, 53, 54, and 55.

Polonia, P. V.; Melgarejo, L. F. B.; de Queiroz, M. H. A resource oriented architecture for web-integrated scada applications. In: **IEEE World Conference on Factory Communication Systems (WFCS)**. Palma de Mallorca, Spain: [s.n.], 2015. p. 1–8. Citations on pages 52, 53, 54, 76, and 113.

Qiu, T.; Zhao, Z.; Zhang, T.; Chen, C.; Chen, C. L. P. Underwater internet of things in smart ocean: System architecture and open issues. **IEEE Transactions on Industrial Informatics**, v. 16, n. 7, p. 4297–4307, 2020. Citation on page 38.

RUNESON, P.; HÖST, M. Guidelines for conducting and reporting case study research in software engineering. **Empirical Software Engineering volume**, v. 14, n. 2, p. 131–164, 2009. Citation on page 70.

Sadeghi, A.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In: **52nd ACM/EDAC/IEEE Design Automation Conference (DAC)**. San Francisco, CA, USA: [s.n.], 2015. p. 1–6. Citation on page 25.

SARTOR, G. Privacy, reputation, and trust: Some implications for data protection. In: STØLEN, K.; WINSBOROUGH, W. H.; MARTINELLI, F.; MASSACCI, F. (Ed.). **Trust Management**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006. p. 354–366. Citations on pages 24 and 25.

SCHRECKER, S.; SOROUSH, H.; MOLINA, J. **Industrial Internet of Things Volume G4: Security Framework**. CreateSpace Independent Publishing Platform, 2016. Available: <https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf>. Citation on page 41.

Schulte, D.; Colombo, A. W. Rami 4.0 based digitalization of an industrial plate extruder system: Technical and infrastructural challenges. In: **3rd Annual Conference of the IEEE Industrial Electronics Society (IECON)**. Beijing, China: [s.n.], 2017. p. 3506–3511. Citations on pages 42, 53, 54, 55, and 80.

Schulz, D. FDI and the industrial internet of things. In: **IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA)**. Luxembourg, Luxembourg: [s.n.], 2015. p. 1–8. Citation on page 54.

SEAMAN, C. B. Qualitative methods. In: **Guide to Advanced Empirical Software Engineering**. [S.l.: s.n.], 2008. p. 35–62. Citations on pages 57, 70, 71, and 81.

Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. **IEEE Transactions on Industrial Informatics**, v. 14, n. 11, p. 4724–4734, 2018. Citations on pages 42, 53, 54, 55, and 113.

SPOKE, M.; NUCO, T. E. **Aion:Enabling the decentralized Internet**. California, USA, 2017. 1–23 p. Accessed in March 2019. Available: <https://aion.network/media/en-aion-network-technical-introduction.pdf>. Citation on page 45.

STRAUSS, A. L.; CORBIN, J. M. **Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory**. second. [S.l.]: SAGE Publications, 1998. ISBN 9780803959408. Citations on pages 71 and 81.

SURESH, A.; UDENDHRAN, R.; BALAMURUGAN, M. Integrating IoT and machine learning–the driving force of industry 4.0. In: **Internet of Things for Industry 4.0**. [S.l.]: Springer, 2020. p. 219–235. Citation on page 80.

Tama, B. A.; Kweka, B. J.; Park, Y.; Rhee, K. A critical review of blockchain and its current applications. In: **International Conference on Electrical Engineering and Computer Science (ICECOS)**. Palembang, Indonesia: [s.n.], 2017. p. 109–113. Citation on page 27.

TAO, F.; QI, Q.; WANG, L.; NEE, A. Digital twins and cyber–physical systems toward smart manufacturing and industry 4.0: Correlation and comparison. **Engineering**, v. 5, n. 4, p. 653 – 661, 2019. Citation on page 35.

TOGAF. **The TOGAF Standard, Version 9.2**. [S.l.], 2018. (TOGAF Series). Accessed in March 2019. Available: <https://www.opengroup.org>. Citation on page 24.

UHLEMANN, T. H.-J.; LEHMANN, C.; STEINHILPER, R. The digital twin: Realizing the cyber-physical production system for industry 4.0. **The 24th Conference on Life Cycle Engineering (CIRP)**, v. 61, p. 335 – 340, 2017. Citations on pages 34 and 35.

UM, T.; LEE, G. M.; CHOI, J. K. Strengthening trust in the future social-cyber-physical infrastructure: an itu-t perspective. **IEEE Communications Magazine**, v. 54, n. 9, p. 36–42, Sep. 2016. Citation on page 25.

Urbina, M.; Acosta, T.; Lázaro, J.; Astarloa, A.; Bidarte, U. Smart sensor: Soc architecture for the industrial internet of things. **IEEE Internet of Things Journal**, v. 6, n. 4, p. 6567–6577, 2019. Citation on page 52.

VAIDYA, S.; AMBAD, P.; BHOSLE, S. Industry 4.0 – a glimpse. **Procedia Manufacturing**, v. 20, p. 233 – 238, 2018. Citation on page 34.

Vazquez-Ingelmo, A.; Garcia-Holgado, A.; Garcia-Penalvo, F. J. C4 model in a software engineering subject to ease the comprehension of uml and the software. In: **IEEE Global Engineering Education Conference (EDUCON)**. Porto, Portugal: [s.n.], 2020. p. 919–924. Citations on pages 30, 86, and 105.

Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F. Blockchain-powered parallel healthcare systems based on the acp approach. **IEEE Transactions on Computational Social Systems**, v. 5, n. 4, p. 942–950, 2018. Citations on pages 27 and 45.

WEBER, I.; XU, X.; RIVERET, R.; GOVERNATORI, G.; PONOMAREV, A.; MENDLING, J. Untrusted business process monitoring and execution using blockchain. In: ROSA, M. L.; LOOS, P.; PASTOR, O. (Ed.). **Business Process Management**. Sydney, NSW, Australia: Springer International Publishing, 2016. p. 329–347. Citation on page 45.

WIERINGA, R. **Design Science Methodology for Information Systems and Software Engineering**. [S.l.]: Springer, 2014. ISBN 978-3-662-43838-1. Citations on pages 28 and 30.

WOHLIN, C.; RUNESON, P.; HöST, M.; OHLSSON, M. C.; REGNELL, B.; WESSLÉN, A. **Experimentation in Software Engineering: An Introduction**. 2. ed. Norwell, MA, USA: Springer-Verlag, 2012. ISBN 3642432263. Citations on pages 56, 70, and 81.

XU, L. D.; XU, E. L.; LI, L. Industry 4.0: State of the art and future trends. **International Journal of Production Research**, Taylor and Francis Ltd., v. 56, n. 8, p. 2941–2962, 2018. Citations on pages 23, 34, 38, 52, 53, 55, and 113.

YANG, H.; YANG, B. A blockchain-based approach to the secure sharing of healthcare data. **Nisk Journal**, Oslo, Norway, p. 1–12, 2017. Citation on page 45.

Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V. C. M. Blockchain-based decentralized trust management in vehicular networks. **IEEE Internet of Things Journal**, v. 6, n. 2, p. 1495–1505, 2019. Citations on pages 27, 45, and 72.

ZAMYATIN, A.; HARZ, D.; LIND, J.; PANAYIOTOU, P.; GERVAIS, A.; KNOTTENBELT, W. J. Xclaim: A framework for blockchain interoperability. **IEEE Symposium on Security and Privacy**, p. 193–210, 2019. Citation on page 45.

ZHANG, P.; WHITE, J.; SCHMIDT, D. C.; LENZ, G. **Applying software patterns to address interoperability in blockchain-based healthcare apps**. Ithaca, Nova Iorque, USA, 2017. 1–14 p. Citation on page 45.

ZIEGELDORF, J. H.; GARCÍA-MORCHÓN, Ó.; WEHRLE, K. Privacy in the internet of things: Threats and challenges. **Security and Communication Networks**, v. 7, n. 12, p. 2728–2742, 2014. Citation on page 25.

ZVEI-ELEKTROINDUSTRIE. **Industrie 4.0: The Reference Architectural Model Industrie 4.0 (RAMI 4.0)**. [S.l.], 2015. 1–2 p. Citations on pages 15 and 38.

APPENDIX

A

SLR PROTOCOL AND RESULTS

In this Appendix, we attached the Systematic Literature Review protocol and results.

SLR PROTOCOL

Title: Architecture Drivers for Trustworthy Interoperability in Industry 4.0

Purpose: Identify the main quality attributes regarding interoperability in Industry 4.0

Objective: Conduct a systematic literature review to gather studies regarding trustworthy interoperability in Industry 4.0

Research Questions: RQ1: How has trust in the interoperability in

Languages: English

Sources: Scopus, Science Direct, IEEE, ACM

Key-words: Industry 4.0, Industrial Internet of Things, interoperability

Search String: (("Industry 4.0" OR "I4.0" OR "I4" O**R "industrial revolution" OR "Industrial Internet of Things" OR "IIOT") AND ("interoperability"))**

Inclusion Criteria:
IC1. Quality attributes to promote trust in interoperability
IC2. Requirements to promote trust in interoperability

Exclusion Criteria:
EC1. Papers not related to Industry 4.0 context
EC2. Paper not describe trust requirements
EC3. Duplicated studies.
EC4. Study containing an editorial, abstract, or introduction; and
EC5. Study not written in English.

Selection of a data exchange format for industry 4.0 manufacturing systems

Nro.	title	author	year	source	First Selection	Selection by title and Abstract	Selection by full reading
1	A distributed systems perspective on industrial IoT	Iwanicki, K.	2018	Scopus	IC1	Accepted	Accepted
2	A microservice architecture for the industrial internet-of-things	Dobaj, J. and Krisper, M. and Iber,	2018	Scopus	IC1	Accepted	Accepted
3	A resource oriented architecture for Web-integrated SCADA applications	Polonia, P.V. and Melgarejo, L.F.B.	2015	Scopus	IC2	Accepted	Accepted
4	An AAA solution for securing industrial IoT devices using next generation access contro	K. K. {Kolluru} and C. {Paniagua} ar	2018	IEEE	IC2	Accepted	Accepted
5	Applying blockchain in industry 4.0 applications	Mohamed et a.	2019	ACM	IC2	Accepted	Accepted
6	FDI and the Industrial Internet of Things: Protection of Investment for Industrie 4.0	Schulz et al.	2015	Scopus	IC2	Accepted	Accepted
7	Homomorphic encryption and network coding in IoT architectures: Advantages and fut	Peralta et al.	2019	Scopus	IC1	Accepted	Accepted
8	Industrial internet of things: Challenges, opportunities, and directions	Sisinni, E. and Saifullah, A. and Hai	2018	Scopus	IC2	Accepted	Accepted
9	Industry 4.0: Sustainability and design principles	Habib, M.K. and Chimsom, C.	2019	Scopus	IC2	Accepted	Accepted
10	Local Cloud Internet of Things Automation: Technology and Business Model Features o	J. {Delsing}	2017	IEEE	IC2	Accepted	Accepted
11	RAMI 4.0 based digitalization of an industrial plate extruder system: Technical and infr	D. {Schulte} and A. W. {Colombo}	2017	IEEE	IC2	Accepted	Accepted
12	SEMIoTICS Architectural Framework: End-to-end Security, Connectivity and Interopera	N. E. {Petroulakis} and E. {Lakka} a	2019	IEEE	IC2	Accepted	Accepted
13	Smart Sensor: SoC Architecture for the Industrial Internet of Things	Urbina et al.	2019	Scopus	IC2	Accepted	Accepted
14	Software architecture solution based on SDN for an industrial IoT scenario	Romero-Gázquez, J.L. and Bueno-I	2018	Scopus	IC2	Accepted	Accepted
15	Towards an Open-standards Based Framework for Achieving Condition-based Predictiv	Kaur, Karamjit and Selway, Matt a	2018	ACM	IC2	Accepted	Accepted
16	Towards trustworthy end-to-end communication in industry 4.0	Bicaku et al.	2017	Scopus	IC2	Accepted	Accepted
17	Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems	F. {Fraile} and T. {Tagawa} and R. {	2018	IEEE	IC2	Accepted	Accepted
18	Using Smart Edge IoT Devices for Safer, Rapid Response with Industry IoT Control Oper	Condry, M.W. and Nelson, C.B.	2016	Scopus	IC2	Accepted	Accepted

19	Challenges and research directions for blockchains in the internet of things	Golatowski, F. and Butzin, B. and B	2019	Scopus	IC2	Accepted	Rejected
20	Cross reality to enhance worker cognition in industrial assembly operations	Simões, B. and De Amicis, R. and B	2019	Scopus	IC2	Accepted	Rejected
21	Current Challenges of the Joint Consideration of Functional Safety & Cyber Security, Th	Link, J. and Waedt, K. and Ben Zid,	2018	Scopus	IC2	Accepted	Rejected
22	Developments and trends in shopfloor-related ICT systems	Sauer, O.	2014	Scopus	IC2	Accepted	Rejected
23	Enabling Industrial Internet of Things (IIoT) towards an emerging smart energy system	Ding Zhang and Ching Chuen Char	2018	Sciencel	IC2	Accepted	Rejected
24	Exploiting interoperable microservices in web objects enabled Internet of Things	Jarwar, M.A. and Ali, S. and Kibria,	2017	Scopus	IC2	Accepted	Rejected
25	IoT Interoperability—On-Demand and Low Latency Transparent Multiprotocol Translat	H. {Derhamy} and J. {Eliasson} and	2017	IEEE	IC2	Accepted	Rejected
26	Manufacturing in the fourth industrial revolution: A positive prospect in Sustainable M	Núbia Carvalho and Omar Chaim a	2018	Sciencel	IC2	Accepted	Rejected
27	Scalability of OPC-UA down to the chip level enables "internet of Things"	Imtiaz, J. and Jasperneite, J.	2013	Scopus	IC2	Accepted	Rejected
28	Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeas	Panchal, A.C. and Khadse, V.M. an	2019	Scopus	IC1	Accepted	Rejected
29	Smart Sensor: SoC Architecture for the Industrial Internet of Things	M. {Urbina} and T. {Acosta} and J.	2019	IEEE	IC2	Accepted	Rejected
30	Software architecture solution based on SDN for an industrial IoT scenario	Gazquez et al.	2018	Scopus	IC2	Accepted	Rejected
31	Systematic Analysis of IT Complexity Challenges Hindering the Implementation of Indu	Schuh, Günther and Bleider, Marti	2019	ACM	IC2	Accepted	Rejected
32	Systems engineering analysis approach based on interoperability for reconfigurable m	M. {Hammadi} and J. {Choley} and	2016	IEEE	IC2	Accepted	Rejected
33	The Integration of LwM2M and OPC UA: An Interoperability Approach for Industrial IoT	A. {Karaagac} and N. {Verbeeck} an	2019	IEEE	IC2	Accepted	Rejected
34	Towards an open-standards based framework for achieving condition-based predictive	Kaur, K. and Selway, M. and Gross	2018	Scopus	IC1	Accepted	Rejected
35	Towards smart factory: Multi-agent integration on industrial standards for service-orie	Rosendahl, R. and Cala, A. and Kiro	2018	Scopus	IC2	Accepted	Rejected
36	FDI and the Industrial Internet of Things: Protection of Investment for Industrie 4.0	Schulz, D.	2015	Scopus	IC2	Accepted	Rejected
37	Towards an open-standards based framework for achieving condition-based predictive	Kaur, Karamjit and Selway, Matt and G	2020	Scopus	IC2	Accepted	Rejected
38	A B2B Team Formation Microservice for Collaborative Manufacturing in Industry 4.0	S. {Cisneros-Cabrera} and P. {Samp	2018	IEEE	EC3	Duplicated	
39	A Distributed Systems Perspective on Industrial IoT	K. {Iwanicki}	2018	IEEE	EC3	Duplicated	
40	A fault compensation algorithm for a Distributed manufacturing system	Maldonado-Ramirez, A. and Osori	2017	Scopus	EC3	Duplicated	
41	A Framework of Energy Consumption Modelling for Additive Manufacturing Using Inte	Qin, J. and Liu, Y. and Grosvenor, R	2017	Scopus	EC3	Duplicated	
42	A Microservice Architecture for the Industrial Internet-Of-Things	Dobaj, Jürgen and Iber, Johannes a	2018	ACM	EC3	Duplicated	
43	A middleware architecture for vertical integration	A. {Ismail} and W. {Kastner}	2016	IEEE	EC3	Duplicated	
44	A model-based approach for process monitoring in oil production industry	E. {Irisarri} and M. V. {García} and	2016	IEEE	EC3	Duplicated	
45	A Model-Driven Approach for Visualisation Processes	Morgan, Rebecca and Grossmann,	2019	ACM	EC3	Duplicated	
46	A modular interoperability layer for connecting the business and manufacturing syster	Glanon, P. and Azaiez, S. and Mrai	2018	Scopus	EC3	Duplicated	
47	A neutral approach for interoperability in the field of 3D measurement data manageme	Emmer, C. and Hofmann, T.M. and	2018	Scopus	EC3	Duplicated	
48	A proposal to make OCF and OPC UA interoperable	S. {Cavalieri} and M. S. {Scroppo}	2018	IEEE	EC3	Duplicated	
49	A resource oriented architecture for Web-integrated SCADA applications	P. V. {Polônia} and L. F. B. {Melgar	2015	IEEE	EC3	Duplicated	
50	A standards framework for value networks in the context of Industry 4.0	Mazak, A. and Huemer, C.	2016	Scopus	EC3	Duplicated	
51	A web-based platform for OPC UA integration in IIoT environment	Cavalieri, S. and Di Stefano, D. and	2018	Scopus	EC3	Duplicated	
52	Achieving interoperability using low-cost middleware OPC UA wrapping structure. Cas	A. {Korodi} and I. {Silea}	2017	IEEE	EC3	Duplicated	
53	Adapting an agile manufacturing concept to the reference architecture model industry	Yli-Ojanperä, M. and Sierla, S. and	2019	Scopus	EC3	Duplicated	
54	Adaptive synchronization in multi-hop TSCH networks	Tengfei Chang and Thomas Watte	2015	Sciencel	EC3	Duplicated	
55	Advanced Information Technology Solutions for Implementing Information Sharing Acr	Marinagi, Catherine and Skourlas,	2018	ACM	EC3	Duplicated	
56	An AAA solution for securing industrial IoT devices using next generation access contro	Kolluru, K.K. and Paniagua, C. and	2018	Scopus	EC3	Duplicated	
57	An Agile Information Processing Framework for High Pressure Die Casting Applications	Michael Rix and Bernd Kujat and T	2016	Sciencel	EC3	Duplicated	
58	An Application-Layer Restful Sleepy Nodes Implementation for Internet of Things Syste	M. {Thoma} and T. {Afouras} and T	2015	IEEE	EC3	Duplicated	
59	An industrial IoT framework to simplify connection process using system-generated co	Kim-Hung, L. and Datta, S.K. and B	2017	Scopus	EC3	Duplicated	
60	An Industry 4.0 Cyber-Physical Framework for Micro Devices Assembly	J. {Cecil} and S. {Albuhamood} and	2018	IEEE	EC3	Duplicated	
61	An interactive architecture for industrial scale prediction: Industry 4.0 adaptation of m	Dutta, R. and Mueller, H. and Lian	2018	Scopus	EC3	Duplicated	
62	Analysis of CoAP Implementations for Industrial Internet of Things: A Survey	Markel Iglesias-Urkia and Adrián C	2017	Sciencel	EC3	Duplicated	
63	Analysis of CoAP Implementations for Industrial Internet of Things: A Survey	Iglesias-Urkia, M. and Orive, A. an	2017	Scopus	EC3	Duplicated	
64	Architectural Aspects of Digital Twins in IIoT Systems	Malakuti, Somayeh and Grüner, St	2018	ACM	EC3	Duplicated	
65	ASID: Advanced system for process control towards intelligent specialization in the pov	I. {Stamatescu} and G. {Stamatesc	2017	IEEE	EC3	Duplicated	
66	Assessing the impact of attacks on OPC-UA applications in the Industry 4.0 era	Polge, J. and Robert, J. and Traon,	2019	Scopus	EC3	Duplicated	
67	Assessment of interoperability in cloud manufacturing	Mohamed H. Mourad and Aydin N	2020	Sciencel	EC3	Duplicated	
68	Asset and Production Tracking through Value Chains for Industry 4.0 using the Arrowh	C. {Hegedűs} and A. {Frankó} and P	2019	IEEE	EC3	Duplicated	
69	Automated Reasoning and Knowledge Inference on OPC UA Information Models	J. {Bakakeu} and M. {Brossog} and	2019	IEEE	EC3	Duplicated	
70	Challenges and Research Directions for Blockchains in the Internet of Things	F. {Golatowski} and B. {Butzin} and	2019	IEEE	EC3	Duplicated	

71	Chatting Roles: A Pragmatic Service Resolution Infrastructure for Service Choreograph	Helmut Zörrer and Georg Weichha	2018	Sciencel	EC3	Duplicated	
72	Communication with CNC machine through DNC interface	S. {Jokanović}	2016	IEEE	EC3	Duplicated	
73	Continuous Integration of Field Level Production Data into Top-level Information Syste	Max Hoffmann and Christian Büsc	2016	Sciencel	EC3	Duplicated	
74	Current Challenges of the Joint Consideration of Functional Safety Cyber Security, Thei	J. {Link} and K. {Waedt} and I. {Ben	2018	IEEE	EC3	Duplicated	
75	Data analytics for energy consumption of digital manufacturing systems using Internet	Qin, J. and Liu, Y. and Grosvenor, F	2018	Scopus	EC3	Duplicated	
76	Data Exchange Standard for Industrial Internet of Things	Madhikermi, M. and Yousefnezhad	2019	Scopus	EC3	Duplicated	
77	Delay Estimation of Industrial IoT Applications Based on Messaging Protocols	P. {Ferrari} and A. {Flammini} and	2018	IEEE	EC3	Duplicated	
78	Developing the industrial Internet of Things with a network centric approach: A holisti	B. {van Lier}	2014	IEEE	EC3	Duplicated	
79	Developments and trends in shopfloor-related ICT systems	O. {Sauer}	2014	IEEE	EC3	Duplicated	
80	Digital Technologies of Industry 4.0 in Management of Natural Disasters	Schwertner, Krasimira and Zlateva	2018	ACM	EC3	Duplicated	
81	Enabling an automation architecture of CPPs based on UML combined with IEC-61499	E. X. {Castellanos} and C. A. {Garci	2017	IEEE	EC3	Duplicated	
82	EverySense: An End-to-end IoT Market Platform	Mano, Hiroshi	2016	ACM	EC3	Duplicated	
83	Exploiting interoperable microservices in web objects enabled Internet of Things	M. A. {Jarwar} and S. {Ali} and M. (	2017	IEEE	EC3	Duplicated	
84	Extending OpenFlow with flexible time-triggered real-time communication services	L. {Silva} and P. {Gonçalves} and R.	2017	IEEE	EC3	Duplicated	
85	Flexible factory automation: Potentials of contactless transmission systems, combining	D. {Wesemann} and S. {Witte} and	2016	IEEE	EC3	Duplicated	
86	Flow configuration software implemented on FDT2 standard	Ito, A. and Wai, J.C.S.	2017	Scopus	EC3	Duplicated	
87	HaRTKad: A P2P-based concept for deterministic communication and its limitations	Konieczek, B. and Skodzik, J. and D	2016	Scopus	EC3	Duplicated	
88	Honeypot Inside an OPC UA Wrapper for Water Pumping Stations	C. {Petre} and A. {Korodi}	2019	IEEE	EC3	Duplicated	
89	I4.0-Device Integration: A Qualitative Analysis of Methods and Technologies Utilized by	Burzlaff, F. and Bartelt, C.	2018	Scopus	EC3	Duplicated	
90	IFC Monitor – An IFC schema extension for modeling structural health monitoring syste	Michael Theiler and Kay Smarsly	2018	Sciencel	EC3	Duplicated	
91	Implementation and Performance Analysis of Power and Cost-Reduced OPC UA Gatew	Cho, H. and Jeong, J.	2019	Scopus	EC3	Duplicated	
92	Implementation of enterprise operating system (EOS) in industry 4.0 based on the dece	Youssef, J.R. and Zacharewicz, G. a	2018	Scopus	EC3	Duplicated	
93	Industrial data-collector by enabling OPC-UA standard for Industry 4.0	M. {Ghazivakili} and C. {Demartini	2018	IEEE	EC3	Duplicated	
94	Industrial Internet of Things: Challenges, Opportunities, and Directions	E. {Sisinni} and A. {Saifullah} and S	2018	IEEE	EC3	Duplicated	
95	Industrial Internet of Things: Covering standardization gaps for the next generation of	Meyer, O. and Rauhoeft, G. and Sc	2018	Scopus	EC3	Duplicated	
96	Industry 4.0: A survey on technologies, applications and open research issues	Lu, Y.	2017	Scopus	EC3	Duplicated	
97	Information Technology for the Factory of the Future – State of the Art and Need for Ac	Olaf Sauer	2014	Sciencel	EC3	Duplicated	
98	Integrated Data Model and Structure for the Asset Administration Shell in Industrie 4.0	Tantik, E. and Anderl, R.	2017	Scopus	EC3	Duplicated	
99	Integrating OPC UA with web technologies to enhance interoperability	Salvatore Cavalieri and Marco Giu	2019	Sciencel	EC3	Duplicated	
100	Integration of Small and Medium Enterprises for Industry 4.0 in the South African Wate	P. {Nthutang} and A. {Telukdarie}	2018	IEEE	EC3	Duplicated	
101	Interoperability Mismatch Challenges in Heterogeneous SOA-based Systems	C. {Paniagua} and J. {Eliasson} and	2019	IEEE	EC3	Duplicated	
102	Interoperability rules for heterogenous multi-agent systems: Levels of conceptual inter	E. {Wassermann} and A. {Fay}	2017	IEEE	EC3	Duplicated	
103	Interoperable meta model for simulation-in-the-loop	Ciavotta, M. and Bettoni, A. and Iz	2018	Scopus	EC3	Duplicated	
104	IoT Integration for Adaptive Manufacturing	C. {Alexakos} and C. {Anagnostopo	2018	IEEE	EC3	Duplicated	
105	IoTCrawler: Browsing the Internet of Things	A. F. {Skarmeta} and J. {Santa} and	2018	IEEE	EC3	Duplicated	
106	Knowledge-Driven Architecture Composition: Case-Based Formalization of Integration	F. {Burzlaff} and C. {Bartelt}	2017	IEEE	EC3	Duplicated	
107	Local Cloud Internet of Things Automation: Technology and Business Model Features o	Delsing, J.	2017	Scopus	EC3	Duplicated	
108	Manufacturing in the fourth industrial revolution: A positive prospect in Sustainable M	Carvalho, N. and Chaim, O. and Ca	2018	Scopus	EC3	Duplicated	
109	Mapping OPC UA AddressSpace to OCF resource model	S. {Cavalieri} and M. G. {Salafia} ar	2018	IEEE	EC3	Duplicated	
110	Metaprogramming Environment for Industry 4.0	M. {Papazoglou}	2018	IEEE	EC3	Duplicated	
111	Modbus-OPC UA Wrapper Using Node-RED and IoT-2040 with Application in the Wate	S. {Toc} and A. {Korodi}	2018	IEEE	EC3	Duplicated	
112	Model similarity evidence and interoperability affinity in cloud-ready Industry 4.0 tech	G. Pedone and I. Mezgár	2018	Sciencel	EC3	Duplicated	
113	Model-Based Interoperability IoT Hub for the Supervision of Smart Gas Distribution Ne	A. {Ahmed} and M. {Kleiner} and L.	2019	IEEE	EC3	Duplicated	
114	Modelling Industrial Cyber-Physical Systems using IEC 61499 and OPC UA	Dai, W. and Song, Y. and Zhang, Z.	2018	Scopus	EC3	Duplicated	
115	Modularized assembly system: A digital innovation hub for the Swedish Smart Industry	Åkerman, M. and Fast-Berglund, Å	2018	Scopus	EC3	Duplicated	
116	Multi-paradigm modelling of Cyber-Physical Systems	Dmitry Morozov and Mario Lezoch	2018	Sciencel	EC3	Duplicated	
117	Multi-scale approach from mechatronic to Cyber-Physical Systems for the design of ma	Penas, O. and Plateaux, R. and Pat	2017	Scopus	EC3	Duplicated	
118	New IT Driven Service-Oriented Smart Manufacturing: Framework and Characteristics	F. {Tao} and Q. {Qi}	2019	IEEE	EC3	Duplicated	
119	Node-Red and OPC UA Based Lightweight and Low-Cost Historian with Application in t	Nicolae, A. and Korodi, A.	2018	Scopus	EC3	Duplicated	
120	O-MI/O-DF standards as interoperability enablers for Industrial Internet: A performanc	J. {Robert} and S. {Kubler} and Y. L.	2016	IEEE	EC3	Duplicated	
121	On a Frame Work of Curriculum for Engineering Education 4.0	L. {Jeganathan} and A. N. {Khan} a	2018	IEEE	EC3	Duplicated	
122	On a Frame Work of Curriculum for Engineering Education 4.0	L. {Jeganathan} and A. N. {Khan} a	2018	IEEE	EC3	Duplicated	

123	On a frame work of curriculum for engineering education 4.0	Jeganathan, L. and Khan, A.N. and	2019	Scopus	EC3	Duplicated	
124	OPC UA and Dynamic Web Services: A Generic Flexible Industrial Communication Appr	Banerjee, Suprateek and Gro\ssm	2019	ACM	EC3	Duplicated	
125	Process monitoring and industrial informatics for online optimization of Welding Proce	R. {French} and M. {Benakis} and H	2018	IEEE	EC3	Duplicated	
126	Protocol interoperability of OPC UA in service oriented architectures	H. {Derhamy} and J. {Rönnholm} a	2017	IEEE	EC3	Duplicated	
127	Realising Interoperability Between OPC UA and OCF	S. {Cavalieri} and M. G. {Salafia} ar	2018	IEEE	EC3	Duplicated	
128	Real-Time Wireless Data Plane for Real-Time-Enabled SDN	Ribeiro, P.A. and Duoba, L. and Pri	2019	Scopus	EC3	Duplicated	
129	Requirements Analysis for Machine to Machine Integration within Industry 4.0	R. M. d. {Salles} and F. A. {Coda} ar	2018	IEEE	EC3	Duplicated	
130	Resilient Ontology Support Facilitating Multi-Perspective Process Integration in Indust	Kaar, Claudia and Frysak, Josef an	2018	ACM	EC3	Duplicated	
131	Role Models and Lifecycles in IoT and Their Impact on the W3C WoT Thing Description	Blank, Michele and Lahbaiel, Haifa	2018	ACM	EC3	Duplicated	
132	Runtime reconfiguration of time-sensitive networking (TSN) schedules for Fog Comput	M. L. {Raagaard} and P. {Pop} and	2017	IEEE	EC3	Duplicated	
133	Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeas	A. C. {Panchal} and V. M. {Khadse}	2018	IEEE	EC3	Duplicated	
134	Selection of a data exchange format for industry 4.0 manufacturing systems	Peres, R.S. and Parreira-Rocha, M.	2016	Scopus	EC3	Duplicated	
135	Semantic Degrees for Industrie 4.0 Engineering: Deciding on the Degree of Semantic Fo	Cheng, Chih-Hong and Guelfirat, T	2015	ACM	EC3	Duplicated	
136	Semantic enrichment of product data supported by machine learning techniques	Costa, R. and Figueiras, P. and Jard	2018	Scopus	EC3	Duplicated	
137	Semantic interoperability for asset communication within smart factories	Diedrich, C. and Belyaev, A. and Sc	2018	Scopus	EC3	Duplicated	
138	Semantic Interoperability for Coalition Creation by Mobile Robots and Humans: an App	Alexander Smirnov and Alexey Kas	2018	ScienceI	EC3	Duplicated	
139	Semantic Interoperability in Industry 4.0: Survey of Recent Developments and Outlook	J. {Nilsson} and F. {Sandin}	2018	IEEE	EC3	Duplicated	
140	Smart interoperable logistic environment innovation driver for modern technologies	Forkel, E. and Schumann, C.-A.	2018	Scopus	EC3	Duplicated	
141	Smart Sensor: SoC Architecture for the Industrial Internet of Things	Urbina, M. and Acosta, T. and Laza	2019	Scopus	EC3	Duplicated	
142	Social relationship paradigm applied to object interactions in industrial IoT	Eddy, B. and Oussama, H.	2018	Scopus	EC3	Duplicated	
143	Subject-oriented Design of Smart Hyper-connected Logistics Systems	Neubauer, Matthias and Krenn, Fl	2017	ACM	EC3	Duplicated	
144	Sustainable Data Management for Manufacturing	K. {Burow} and M. {Franke} and Q.	2019	IEEE	EC3	Duplicated	
145	Syntactic Translation of Message Payloads Between At Least Partially Equivalent Encod	E. {Palm} and C. {Paniagua} and U.	2019	IEEE	EC3	Duplicated	
146	Systems engineering analysis approach based on interoperability for reconfigurable m	Hammadi, M. and Choley, J.-Y. and	2016	Scopus	EC3	Duplicated	
147	The adoption stages (Evaluation, Adoption, and Routinisation) of ERP systems with bus	Junior, C.H. and Oliveira, T. and Ya	2019	Scopus	EC3	Duplicated	
148	The Industrial Internet of Things as an enabler for a Circular Economy Hy-LP: A novel II	George Hatzivasilis and Konstantii	2018	ScienceI	EC3	Duplicated	
149	The industry 4.0 standards landscape from a semantic integration perspective	I. {Grangel-González} and P. {Bapt	2017	IEEE	EC3	Duplicated	
150	The role of comprehensive function models in the management of heterogeneous indu	Olaya, S.S.P. and Wollschlaeger, M	2019	Scopus	EC3	Duplicated	
151	The role of Information and Communication Technologies in healthcare: taxonomies, p	Aceto, G. and Persico, V. and Pesc	2018	Scopus	EC3	Duplicated	
152	The Role of Interoperability in The Fourth Industrial Revolution Era	Yongxin Liao and Luiz Felipe Pierin	2017	ScienceI	EC3	Duplicated	
153	Towards an Open-standards Based Framework for Achieving Condition-based Predicti	Kaur, Karamjit and Selway, Matt a	2018	ACM	EC3	Duplicated	
154	Towards industrial Internet of Things: An efficient and interoperable communication fr	J. {Eliasson} and J. {Delsing} and H.	2015	IEEE	EC3	Duplicated	
155	Towards interoperability between OPC UA and OCF	Salvatore Cavalieri and Marco Giu	2019	ScienceI	EC3	Duplicated	
156	Towards the Shop Floor App Ecosystem: Using the Semantic Web for Gluing Together A	Miclaus, Andrei and Clauss, Wolfg	2016	ACM	EC3	Duplicated	
157	Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems	Fraile, F. and Tagawa, T. and Poler	2018	Scopus	EC3	Duplicated	
158	UH4SP: A Software Platform For Integrated Management Of Connected Smart Plants	N. {Santos} and H. {Rodrigues} and	2018	IEEE	EC3	Duplicated	
159	Using Smart Edge IoT Devices for Safer, Rapid Response With Industry IoT Control Ope	M. W. {Condry} and C. B. {Nelson}	2016	IEEE	EC3	Duplicated	
160	VSOMEIP - OPC UA Gateway Solution for the Automotive Industry	Ioana, A. and Korodi, A.	2019	Scopus	EC3	Duplicated	
161	15th IFIP WG 5.1 International Conference on Product Lifecycle Management, PLM 2018		2018	Scopus	EC1	Rejected	
162	25th ISTE International Conference on Transdisciplinary Engineering, 2018		2018	Scopus	EC2	Rejected	
163	2nd International Conference on Interoperability in IoT, InterIoT 2016 and 3rd International Conference on Safety and Sec		2017	Scopus	EC2	Rejected	
164	8th International Conference on Cloud Computing and Services Science, CLOSER 2018		2019	Scopus	EC1	Rejected	
165	A b2b team formation microservice for collaborative manufacturing in industry 4.0	Cisneros-Cabrera, S. and Sampaio,	2018	Scopus	EC2	Rejected	
166	A cloud-based framework for shop floor big data management and elastic computing a	German Terrazas and Nicolas Ferr	2019	ScienceI	EC2	Rejected	
167	A collaboration-oriented M2M messaging mechanism for the collaborative automation	Meng, Z. and Wu, Z. and Gray, J.	2017	Scopus	EC2	Rejected	
168	A common core for information modeling in the Industrial Internet of Things	Pfrommer, J. and Grüner, S. and G	2016	Scopus	EC1	Rejected	
169	A comparative study on digital twin models	Liu, Q. and Liu, B. and Wang, G. an	2019	Scopus	EC1	Rejected	
170	A Conceptual Design for Smell Based Augmented Reality: Case Study in Maintenance D	Jeff Wang and John Erkoyuncu and	2018	ScienceI	EC2	Rejected	
171	A Distributed Time Server for the Real-Time Extension of CoAP	B. {Konieczek} and M. {Rethfeldt} a	2016	IEEE	EC2	Rejected	
172	A fault compensation algorithm for a distributed manufacturing system	A. {Maldonado-Ramirez} and I. {Lo	2017	IEEE	EC2	Rejected	
173	A Framework of Energy Consumption Modelling for Additive Manufacturing Using Inte	Jian Qin and Ying Liu and Roger Gr	2017	ScienceI	EC2	Rejected	
174	A guideline of quality steps towards zero defect manufacturing in industry	Eleftheriadis, R.J. and Myklebust,	2016	Scopus	EC1	Rejected	

175	A hybrid intelligent model for network selection in the industrial Internet of Things	Goudarzi, S. and Anisi, M.H. and A	2019	Scopus	EC2	Rejected	
176	A Lightweight XMPP Publish/Subscribe Scheme for Resource-Constrained IoT Devices	H. {Wang} and D. {Xiong} and P. {W	2017	IEEE	EC2	Rejected	
177	A literature survey on open platform communications (OPC) applied to advanced indus	González, I. and Calderón, A.J. and	2019	Scopus	EC2	Rejected	
178	A middleware architecture for vertical integration	Ismail, A. and Kastner, W.	2016	Scopus	EC2	Rejected	
179	A model-based approach for process monitoring in oil production industry	Irisarri, E. and Garcia, M.V. and Pe	2016	Scopus	EC1	Rejected	
180	A Model-Driven Approach for Visualisation Processes	Morgan, R. and Grossmann, G. and	2019	Scopus	EC2	Rejected	
181	A modular interoperability layer for connecting the business and manufacturing syster	P. {Glanon} and S. {Azaiez} and C. {	2018	IEEE	EC2	Rejected	
182	A neutral approach for interoperability in the field of 3D measurement data managem	Christian Emmer and Timo Marcel	2018	ScienceI	EC2	Rejected	
183	A proposal to make OCF and OPC UA interoperable	Cavalieri, S. and Scroppo, M.S.	2018	Scopus	EC1	Rejected	
184	A smart performance measurement approach for collaborative design in Industry 4.0	Yin, Y. and Qin, S.-F.	2019	Scopus	EC1	Rejected	
185	A standards framework for value networks in the context of Industry 4.0	A. {Mazak} and C. {Huemer}	2015	IEEE	EC2	Rejected	
186	A Triangular NodeTrix Visualization Interface for Overlapping Social Community Struct	C. {Lin} and D. {Deng} and S. {Jhong	2017	IEEE	EC2	Rejected	
187	A Typology of Architectural Strategies for Interoperability	Valle, Pedro Henrique Dias and Ga	2019	ACM	EC2	Rejected	
188	A web-based platform for OPC UA integration in IIoT environment	S. {Cavalieri} and D. {Di Stefano} a	2017	IEEE	EC2	Rejected	
189	Accelerating IIOT adoption with OPC UA	Eruvankai, S. and Muthukrishnan,	2017	Scopus	EC1	Rejected	
190	Achieving interoperability using low-cost middleware OPC UA wrapping structure. Cas	Korodi, A. and Silea, I.	2017	Scopus	EC2	Rejected	
191	ACM International Conference Proceeding Series		2018	Scopus	EC2	Rejected	
192	Adapting an agile manufacturing concept to the reference architecture model industry	Matti Yli-Ojanperä and Seppo Sier	2018	ScienceI	EC2	Rejected	
193	Adaptive synchronization in multi-hop TSCH networks	Chang, T. and Watteyne, T. and Pi	2015	Scopus	EC1	Rejected	
194	Adoption of miniaturized safety-related systems for industrial internet-of-things applic	Hayek, A. and Telawi, S. and Bieler	2017	Scopus	EC1	Rejected	
195	Advanced information technology solutions for implementing information sharing acr	Marinagi, C. and Skourlas, C. and	2018	Scopus	EC1	Rejected	
196	An Agent-Based Framework for Complex Networks	Wendt, A. and Götzinger, M. and S	2019	Scopus	EC1	Rejected	
197	An Agile Information Processing Framework for High Pressure Die Casting Applications	Rix, M. and Kujat, B. and Meisen, T	2016	Scopus	EC1	Rejected	
198	An Application-Layer Restful Sleepy Nodes Implementation for Internet of Things Syste	Thoma, M. and Afouras, T. and Bra	2016	Scopus	EC1	Rejected	
199	An approach supporting real-time project management in plant building and the const	Dallasega, P. and Frosolini, M. and	2016	Scopus	EC1	Rejected	
200	An industrial IoT framework to simplify connection process using system-generated co	L. {Kim-Hung} and S. K. {Datta} and	2017	IEEE	EC2	Rejected	
201	An Industry 4.0 Cyber-Physical Framework for Micro Devices Assembly	Cecil, J. and Albuhamood, S. and C	2018	Scopus	EC1	Rejected	
202	An interactive architecture for industrial scale prediction: Industry 4.0 adaptation of m	R. {Dutta} and H. {Mueller} and D.	2018	IEEE	EC2	Rejected	
203	An introduction to IWoT: How the web of things helps solve industry 4.0 challenges	Retamar, A. and Ibaseta, D. and M	2018	Scopus	EC1	Rejected	
204	An open internet of thing architecture integrating OnEM2M and OGC sensorthings API	Chen, L.-Y. and Huang, C.-Y.	2018	Scopus	EC2	Rejected	
205	Analysis of CoAP implementations for industrial Internet of Things: a survey	Iglesias-Urkia, M. and Orive, A. an	2019	Scopus	EC2	Rejected	
206	Architectural aspects of digital twins in IIoT systems	Malakuti, S. and Grüner, S.	2018	Scopus	EC2	Rejected	
207	ARTI reference architecture – PROSA revisited	Valckenaers, P.	2019	Scopus	EC1	Rejected	
208	ASID: Advanced system for process control towards intelligent specialization in the pov	Stamatescu, I. and Stamatescu, G.	2017	Scopus	EC2	Rejected	
209	Assembly validation in virtual reality—a demonstrative case	Jayasekera, R.D.M.D. and Xu, X.	2019	Scopus	EC1	Rejected	
210	Assessing the impact of attacks on OPC-UA applications in the Industry 4.0 era	J. {Polge} and J. {Robert} and Y. L. {	2019	IEEE	EC2	Rejected	
211	Assessment of interoperability in cloud manufacturing	Mourad, M.H. and Nassehi, A. and	2020	Scopus	EC2	Rejected	
212	Asset and production tracking through value chains for industry 4.0 using the arrowhe	Hegedus, C. and Franko, A. and Va	2019	Scopus	EC2	Rejected	
213	Automated reasoning and knowledge inference on OPC UA information models	Bakakeu, J. and Brossog, M. and Z	2019	Scopus	EC2	Rejected	
214	Beyond interoperability in the systems	Lodwich, A. and Alvarez-Rodrígue	2017	Scopus	EC1	Rejected	
215	Beyond Testbeds: Real-World IoT Deployments	F. {Michahelles} and F. {Kawsar} a	2018	IEEE	EC4	Rejected	
216	Big Data on Machine to Machine Integration’s Requirement Analysis Within I	Coda, F.A. and Salles, R.M. and Vit	2019	Scopus	EC1	Rejected	
217	Building Blocks for Adopting Smart Manufacturing	Sameer Mittal and Muztoba Ahma	2019	ScienceI	EC2	Rejected	
218	CEUR Workshop Proceedings		2015	Scopus	EC2	Rejected	
219	Chapter 10 - RESTful IoT Authentication Protocols	H.V. Nguyen and L. Lo Iacono	2017	ScienceI	EC4	Rejected	
220	Chapter 5 - Modeling and Simulation: The Essential Tools to Manage the Complexities	Fabienne Salimi and Frederic Salin	2018	ScienceI	EC2	Rejected	
221	Chatting Roles: A Pragmatic Service Resolution Infrastructure for Service Choreograph	Zörrer, H. and Weichhart, G. and F	2018	Scopus	EC1	Rejected	
222	C-MARS-ABM: A deployment approach for cloud manufacturing	Mourad, M. and Nassehi, A. and N	2017	Scopus	EC1	Rejected	
223	Communication protocols of an industrial internet of things environment: A comparati	Jaloudi, S.	2019	Scopus	EC2	Rejected	
224	Communication with CNC machine through DNC interface	Jokanovic, S.	2016	Scopus	EC1	Rejected	
225	Continuous Integration of Field Level Production Data into Top-level Information Syste	Hoffmann, M. and Büscher, C. and	2016	Scopus	EC1	Rejected	
226	Controller Interface for Industry 4.0 based on RAMI 4.0 and OPC UA	P. F. S. {de Melo} and E. P. {Godoy}	2019	IEEE	EC2	Rejected	

227	Cyber physical systems for predictive production systems	Lee, J. and Jin, C. and Bagheri, B.	2017	Scopus	EC2	Rejected	
228	Cyber-physical systems in factory automation - Towards the 4th industrial revolution	J. {Schlick}	2012	IEEE	EC4	Rejected	
229	Data analytics challenges in industry 4.0: A case-based approach	Brichni, M. and Guedria, W.	2018	Scopus	EC1	Rejected	
230	Data analytics for energy consumption of digital manufacturing systems using Internet	J. {Qin} and Y. {Liu} and R. {Grosve	2017	IEEE	EC2	Rejected	
231	Data Exchange Standard for Industrial Internet of Things	M. {Madhikermi} and N. {Yousefne	2018	IEEE	EC2	Rejected	
232	Decision-support for business process optimization modelling framework based on ind	Chuks, M. and Arnesh, T.	2018	Scopus	EC1	Rejected	
233	Delay Estimation of Industrial IoT Applications Based on Messaging Protocols	Ferrari, P. and Flammini, A. and Si	2018	Scopus	EC1	Rejected	
234	Developing the industrial Internet of Things with a network centric approach: A holisti	Van Lier, B.	2014	Scopus	EC2	Rejected	
235	Development of an assessment system based on manufacturing readiness level for sm	Choi, S. and Jung, K. and Lee, J.Y.	2017	Scopus	EC1	Rejected	
236	Development of prototype for IoT and IoE scalable infrastructures, architectures and p	Touati, F. and Tariq, H. and Crescir	2018	Scopus	EC1	Rejected	
237	Digital technologies of industry 4.0 in management of natural disasters	Schwertner, K. and Zlateva, P. and	2018	Scopus	EC2	Rejected	
238	Digital twin workshop: a new paradigm for future workshop	Tao, F. and Zhang, M. and Cheng, J	2017	Scopus	EC1	Rejected	
239	Digital twin-based WEEE recycling, recovery and remanufacturing in the background o	Wang, X.V. and Wang, L.	2019	Scopus	EC2	Rejected	
240	ECA2LD: From entity-component-attribute runtimes to linked data applications	Spieldenner, T. and Schubotz, R. a	2018	Scopus	EC1	Rejected	
241	Educational Setup for Service Oriented Process Automation with 5G Testbed	Jukka Kortela and Babak Nasiri an	2017	Sciencel	EC2	Rejected	
242	Emerging manufacturing paradigm shifts for the incoming industrial revolution	Yao, X. and Lin, Y.	2016	Scopus	EC1	Rejected	
243	Enabling an automation architecture of CPPs based on UML combined with IEC-61499	Castellanos, E.X. and Garcia, C.A. a	2017	Scopus	EC2	Rejected	
244	Enabling technologies of industry 4.0 and their global forerunners: An empirical study	Knudsen, M.S. and Kaivo-Oja, J. an	2019	Scopus	EC1	Rejected	
245	Evaluation of Interoperability between Automation Systems using Multi-criteria Meth	Maicon Saturno and Luiz Felipe Pi	2017	Sciencet	EC2	Rejected	
246	EverySense: An end-to-end IoT market platform	Mano, H.	2016	Scopus	EC1	Rejected	
247	Executing model-based software development for embedded I4.0 devices properly	Burzlaff, F. and Bartelt, C. and Jac	2018	Scopus	EC1	Rejected	
248	Experiences of Using Linked Data and Ontologies for Operational Data Sharing in Syste	J. {Axelsson}	2019	IEEE	EC2	Rejected	
249	Experiential Learning of CAD Systems Interoperability in Social Network-based Educati	Cátia Alves and Goran Putnik	2019	Sciencel	EC2	Rejected	
250	Extending OpenFlow with flexible time-triggered real-time communication services	Silva, L. and Goncalves, P. and Ma	2018	Scopus	EC1	Rejected	
251	Factories of the future: challenges and leading innovations in intelligent manufacturing	Jardim-Goncalves, R. and Romero,	2017	Scopus	EC1	Rejected	
252	FDI and the Industrial Internet of Things	D. {Schulz}	2015	IEEE	EC2	Rejected	
253	Flexible factory automation: Potentials of contactless transmission systems, combining	Wesemann, D. and Witte, S. and S	2016	Scopus	EC1	Rejected	
254	Flow configuration software implemented on FDT2 standard	A. {Ito} and J. C. S. {Wai}	2017	IEEE	EC2	Rejected	
255	Fog Computing-Based Cyber-Physical Machine Tool System	Z. {Zhou} and J. {Hu} and Q. {Liu} a	2018	IEEE	EC2	Rejected	
256	Fourth industrial revolution: A way forward to attain better performance in the textile	Ślusarczyk, B. and Haseeb, M. and	2019	Scopus	EC1	Rejected	
257	From lean manufacturing to lean enterprise 4.0: Intergration of theoretical foundation	Caldwell, E.	2018	Scopus	EC2	Rejected	
258	Giving Camel to Artifacts for Industry 4.0 Integration Challenges	Amaral, C.J. and Cranefield, S. and	2019	Scopus	EC1	Rejected	
259	Guest Editorial Information Technology in Automation	H. {Prähofer} and V. {Vyatkin} and	2018	IEEE	EC4	Rejected	
260	Guest Editorial Special Issue on Industrial IoT Systems and Applications		2017	IEEE	EC4	Rejected	
261	Guest Editorial Special Section on Recent Trends and Developments in Industry 4.0 Mo	M. {Indri} and A. {Grau} and M. {Ru	2018	IEEE	EC4	Rejected	
262	HaRTKad: A P2P-based concept for deterministic communication and its limitations	B. {Konieczek} and J. {Skodzik} and	2016	IEEE	EC4	Rejected	
263	HAVE WE CREATED A STANDARDS-SETTING TOWER OF BABEL?	Helms, Jay F.	1981	Scopus	EC1	Rejected	
264	Holonic-based task scheduling in smart manufacturing systems	Vlad, V.	2019	Scopus	EC1	Rejected	
265	Honeypot inside an opc ua wrapper for water pumping stations	Petre, C.-A. and Korodi, A.	2019	Scopus	EC2	Rejected	
266	IFC Monitor – An IFC schema extension for modeling structural health monitoring syste	Theiler, M. and Smarsly, K.	2018	Scopus	EC1	Rejected	
267	Implementation and Performance Analysis of Power and Cost-Reduced OPC UA Gatew	H. {Cho} and J. {Jeong}	2018	IEEE	EC2	Rejected	
268	Implementation of cloud services for advance management of steel transport for conti	Kudriashov, N. and Protasov, I. an	2016	Scopus	EC1	Rejected	
269	Implementation of enterprise operating system (EOS) in industry 4.0 based on the dec	J. R. {Youssef} and G. {Zacharewicz	2017	IEEE	EC2	Rejected	
270	Industrial data-collector by enabling OPC-UA standard for Industry 4.0	Ghazivakili, M. and Demartini, C. a	2018	Scopus	EC2	Rejected	
271	Industrial Internet of Things: covering standardization gaps for the next generation of	O. {Meyer} and G. {Rauhoeft} and	2018	IEEE	EC2	Rejected	
272	Industrial internet platforms: A conceptual evaluation from a product lifecycle manage	Menon, K. and Kärkkäinen, H. and	2019	Scopus	EC2	Rejected	
273	Industrial IoT gateway with machine learning for smart manufacturing	Lojka, T. and Miškuf, M. and Zolot	2016	Scopus	EC1	Rejected	
274	Industrial socio-cyberphysical system's consumables tokenization for smart contracts i	Teslya, N.	2019	Scopus	EC1	Rejected	
275	Industry 4.0 – challenges to implement circular economy	Rajput, S. and Singh, S.P.	2019	Scopus	EC1	Rejected	
276	Industry 4.0 and its impacts on society	Moraes, E.C. and Lepikson, H.A.	2017	Scopus	EC1	Rejected	
277	Industry 4.0 as enabler for effective manufacturing virtual enterprises	Ferreira, F. and Faria, J. and Azeve	2016	Scopus	EC1	Rejected	
278	Industry 4.0 potential in textile production	Jerzembeck, J.	2016	Scopus	EC1	Rejected	

279	Industry 4.0 through organizational interoperability perspective: A multicriteria decisi	Gomes, P.F.O. and Bordini, G.A. ar	2018	Scopus	EC1	Rejected	
280	Influence of Industry 4.0 on the production and service sectors in Pakistan: Evidence fr	Imran, M. and ul Hameed, W. and	2018	Scopus	EC1	Rejected	
281	Information and communication technologies within industry 4.0 concept	Peraković, D. and Periša, M. and S	2019	Scopus	EC1	Rejected	
282	Information technology for the factory of the future - State of the art and need for acti	Sauer, O.	2014	Scopus	EC1	Rejected	
283	Innovations in IoT for a Safe, Secure, and Sustainable Future	Bhunia, Swarup	2019	ACM	EC4	Rejected	
284	Integrated Data Model and Structure for the Asset Administration Shell in Industrie 4.0	Erdal Tantik and Reiner Anderl	2017	Sciencel	EC2	Rejected	
285	Integrating OPC UA with web technologies to enhance interoperability	Cavalieri, S. and Salafia, M.G. and	2019	Scopus	EC2	Rejected	
286	Integration of Small and Medium Enterprises for Industry 4.0 in the South African Wate	Nthutang, P. and Telukdarie, A.	2019	Scopus	EC2	Rejected	
287	Internet of Things for Disaster Management: State-of-the-Art and Prospects	P. P. {Ray} and M. {Mukherjee} and	2017	IEEE	EC2	Rejected	
288	Internet of Things: A possible change in the distributed modeling and simulation archit	Riecken, M. and Lessmann, K. and	2016	Scopus	EC1	Rejected	
289	Interoperability between BIM models and 4.0 approach: Theoretical models and practi	Pini, K. and Cataldi, G. and Faini, G	2019	Scopus	EC1	Rejected	
290	Interoperability for human-centered manufacturing	Åkerman, M. and Fast-Berglund, Å	2018	Scopus	EC1	Rejected	
291	Interoperability in smart manufacturing: Research challenges	Zeid, A. and Sundaram, S. and Mog	2019	Scopus	EC2	Rejected	
292	Interoperability mismatch challenges in heterogeneous SOA-based systems	Paniagua, C. and Eliasson, J. and D	2019	Scopus	EC2	Rejected	
293	Interoperability of the time of Industry 4.0 and the Internet of Things	Lelli, F.	2019	Scopus	EC2	Rejected	
294	Interoperability rules for heterogenous multi-agent systems: Levels of conceptual inter	Wassermann, E. and Fay, A.	2017	Scopus	EC2	Rejected	
295	Interoperable meta model for simulation-in-the-loop	M. {Ciavotta} and A. {Bettoni} and	2018	IEEE	EC2	Rejected	
296	IO-Link Wireless enhanced factory automation communication for Industry 4.0 applica	Heynicke, R. and Krush, D. and Car	2018	Scopus	EC1	Rejected	
297	IoT integration for adaptive manufacturing	Alexakos, C. and Anagnostopoulos	2018	Scopus	EC1	Rejected	
298	IoT-based automatic non-conformity detection: A metalworking sme use case	Marques, M. and Cunha, A. and M	2019	Scopus	EC1	Rejected	
299	IoTCrawler: Browsing the internet of things	Skarmeta, A.F. and Santa, J. and M	2018	Scopus	EC1	Rejected	
300	Knowledge-driven architecture composition: Case-based formalization of integration k	Burzlaff, F. and Bartelt, C.	2017	Scopus	EC2	Rejected	
301	Lessons learned from the 6TiSCH plugtests	Palattella, M.R. and Vilajosana, X.	2016	Scopus	EC1	Rejected	
302	Literature review of Industry 4.0 and related technologies	Oztemel, E. and Gursev, S.	2018	Scopus	EC1	Rejected	
303	Main principals and issues of digital twin development for complex technological proc	Ponomarev, K. and Kudryashov, N	2017	Scopus	EC1	Rejected	
304	Managing complexity of assembly with modularity: a cost and benefit analysis	Shoval, S. and Efatmaneshnik, M.	2019	Scopus	EC1	Rejected	
305	Mapping OPC UA AddressSpace to OCF resource model	Cavalieri, S. and Salafia, M.G. and	2018	Scopus	EC1	Rejected	
306	Maturity Models and tools for enabling smart manufacturing systems: Comparison and	De Carolis, A. and Macchi, M. and	2017	Scopus	EC1	Rejected	
307	Metamodeling wireless communication in cyber-physical systems	Smarsly, K. and Fitz, T. and Legatiu	2019	Scopus	EC1	Rejected	
308	Metaprogramming environment for industry 4.0	Papazoglou, M.P.	2018	Scopus	EC2	Rejected	
309	Modbus-OPC UA Wrapper Using Node-RED and IoT-2040 with Application in the Wate	Toc, S.-I. and Korodi, A.	2018	Scopus	EC1	Rejected	
310	Model based, modular configuration of cyber physical systems for the information ma	Jaekel, F.-W. and Torka, J. and Epp	2018	Scopus	EC2	Rejected	
311	Model similarity evidence and interoperability affinity in cloud-ready Industry 4.0 tech	Pedone, G. and Mezgár, I.	2018	Scopus	EC1	Rejected	
312	Model-based development of modular complex systems for accomplishing system inte	Suri, K. and Cuccuru, A. and Cadav	2017	Scopus	EC1	Rejected	
313	Model-Based Interoperability IoT Hub for the Supervision of Smart Gas Distribution Ne	Ahmed, A. and Kleiner, M. and Rou	2019	Scopus	EC2	Rejected	
314	Modelling Industrial Cyber-Physical Systems using IEC 61499 and OPC UA	W. {Dai} and Y. {Song} and Z. {Zhan	2018	IEEE	EC2	Rejected	
315	Modularized assembly system: A digital innovation hub for the Swedish Smart Industry	Magnus Åkerman and Åsa Fast-Be	2018	Sciencel	EC1	Rejected	
316	Multi-agent Manufacturing Execution System (MES): Concept, architecture & ML algor	Mantravadi, S. and Li, C. and Mølle	2019	Scopus	EC1	Rejected	
317	Multi-paradigm modelling of Cyber-Physical Systems	Morozov, D. and Lezoche, M. and	2018	Scopus	EC1	Rejected	
318	Multi-scale approach from mechatronic to Cyber-Physical Systems for the design of ma	Olivia Penas and Régis Plateaux an	2017	Sciencel	EC2	Rejected	
319	New IT driven service-oriented smart manufacturing: Framework and characteristics	Tao, F. and Qi, Q.	2019	Scopus	EC1	Rejected	
320	No need to marry to change your name! attacking profinet io automation networks usi	Mehner, S. and König, H.	2019	Scopus	EC1	Rejected	
321	Node-Red and OPC UA Based Lightweight and Low-Cost Historian with Application in t	A. {Nicolae} and A. {Korodi}	2018	IEEE	EC2	Rejected	
322	O-MI/O-DF standards as interoperability enablers for Industrial Internet: A performanc	Robert, J. and Kubler, S. and Le Tra	2016	Scopus	EC1	Rejected	
323	On a frame work of curriculum for engineering education 4.0	Jeganathan, L. and Khan, A.N. and	2019	Scopus	EC2	Rejected	
324	Ontologies for web of things: A pragmatic review	Kolchin, M. and Klimov, N. and An	2015	Scopus	EC1	Rejected	
325	OPC UA and dynamic web services – A generic flexible industrial communication appro	Banerjee, S. and Großmann, D.	2019	Scopus	EC2	Rejected	
326	Performance evaluation of industrial OPC UA gateway with energy cost-saving	Cho, H. and Jeong, J.	2018	Scopus	EC1	Rejected	
327	PLUGandWORK-Upgrade legacy systems for the industrial internet of things [PLUGand	Sauer, O.	2017	Scopus	EC1	Rejected	
328	Proceedings of the ACM Symposium on Applied Computing		2019	Scopus	EC1	Rejected	
329	Process monitoring and industrial informatics for online optimization of Welding Proce	French, R. and Benakis, M. and Ma	2019	Scopus	EC2	Rejected	
330	Product lifecycle management - How to adapt PLM to support changing product develo	Bitzer, M. and Vielhaber, M. and K	2016	Scopus	EC1	Rejected	

331	Product lifecycle management and digital manufacturing technologies in the era of clo	C. {Holligan} and V. {Hargaden} an	2017	IEEE	EC2	Rejected	
332	Product lifecycle management enabled by industry 4.0 technology	Ferreira, F. and Faria, J. and Azeve	2016	Scopus	EC1	Rejected	
333	Promoting Trust in Interoperability of Systems-of-systems	Allian, Ana Paula	2019	ACM	EC1	Rejected	
334	Protocol interoperability of OPC UA in service oriented architectures	Derhamy, H. and Ronnholm, J. and	2017	Scopus	EC2	Rejected	
335	Realising Interoperability between OPC UA and OCF	Cavalieri, S. and Salafia, M.G. and	2018	Scopus	EC2	Rejected	
336	Real-Time Wireless Data Plane for Real-Time-Enabled SDN	P. A. {Ribeiro} and L. {Duoba} and I	2019	IEEE	EC4	Rejected	
337	Reference field for research and development of novel hybrid forms of human machine	Zeidler, F. and Bayhan, H. and Ven	2017	Scopus	EC2	Rejected	
338	Requirements analysis for machine to machine integration within industry 4.0	Salles, R.M.D. and Coda, F.A. and S	2019	Scopus	EC2	Rejected	
339	Resilient ontology support facilitating multi-perspective process integration in industry	Kaar, C. and Frysak, J. and Stary, C	2018	Scopus	EC2	Rejected	
340	REST based OPC UA for the IIoT	R. {Schiekofer} and A. {Scholz} and	2018	IEEE	EC2	Rejected	
341	RESTful IoT Authentication Protocols	Nguyen, H.V. and Lo Iacono, L.	2016	Scopus	EC1	Rejected	
342	Robotic internal audit - Control methods in the selected company	Hradecká, M.	2019	Scopus	EC1	Rejected	
343	Role models and lifecycles in IoT and their impact on the W3C WOT thing description	Blank, M. and Kaebisch, S. and Lah	2018	Scopus	EC2	Rejected	
344	Runtime reconfiguration of time-sensitive networking (TSN) schedules for Fog Comput	Raagaard, M.L. and Pop, P. and Gu	2018	Scopus	EC1	Rejected	
345	Safety-Related Wireless Communication via RF Modules for Industrial IoT Applications	Telawi, S. and Hayek, A. and Börcs	2018	Scopus	EC1	Rejected	
346	Scientific discussion: Open reviews of “arti reference architecture – PROSA revisited”	Borangiu, T. and Cardin, O. and Ba	2019	Scopus	EC1	Rejected	
347	Selection of a data exchange format for industry 4.0 manufacturing systems	R. S. {Peres} and M. {Parreira-Roch	2016	IEEE	EC2	Rejected	
348	Semantic communication between components for smart factories based on oneM2M	A. {Willner} and C. {Diedrich} and I	2017	IEEE	EC4	Rejected	
349	Semantic data integration for industry 4.0 standards	Grangel-González, I.	2017	Scopus	EC1	Rejected	
350	Semantic degrees for industrie 4.0 engineering : Deciding on the degree of semantic fo	Cheng, C.-H. and Guelfirat, T. and	2015	Scopus	EC2	Rejected	
351	Semantic enrichment of product data supported by machine learning techniques	R. {Costa} and P. {Figueiras} and R.	2017	IEEE	EC2	Rejected	
352	Semantic interoperability for asset communication within smart factories	C. {Diedrich} and A. {Belyaev} and	2017	IEEE	EC2	Rejected	
353	Semantic Interoperability for Coalition Creation by Mobile Robots and Humans: an App	Smirnov, A. and Kashevnik, A.	2018	Scopus	EC1	Rejected	
354	Semantic Interoperability in Industry 4.0: Survey of Recent Developments and Outlook	Nilsson, J. and Sandin, F.	2018	Scopus	EC2	Rejected	
355	Semantic technologies for the modeling of condition monitoring knowledge in the fran	Cao, Q.	2018	Scopus	EC1	Rejected	
356	Semantic web of things for industry 4.0	Thuluva, A.S. and Anicic, D. and Ru	2017	Scopus	EC1	Rejected	
357	Semantic-based approach for low-effort engineering of automation systems	Thuluva, A.S. and Dorofeev, K. and	2017	Scopus	EC1	Rejected	
358	Service-Oriented Approach for Internet of Things	Moraes, E.C.	2018	Scopus	EC1	Rejected	
359	Service-oriented platform for smart operation of dyeing and finishing industry	Park, K.T. and Im, S.J. and Kang, Y.	2019	Scopus	EC2	Rejected	
360	Smart interoperable logistic environment innovation driver for modern technologies	E. {Forkel} and C. {Schumann}	2017	IEEE	EC2	Rejected	
361	Smart Interoperable Logistics and Additive Manufacturing - Modern Technologies for I	Forkel, E. and Baum, J. and Schum	2018	Scopus	EC1	Rejected	
362	Smart SysTech 2019 - European Conference on Smart Objects, Systems and Technologies		2019	Scopus	EC1	Rejected	
363	Smart Wearable System for Safety-Related Industrial IoT Applications	Hayek, A. and Telawi, S. and Klos,	2018	Scopus	EC1	Rejected	
364	Smart-troubleshooting connected devices: Concept, challenges and opportunities	Mauro Caporuscio and Francesco	2019	Sciencet	EC2	Rejected	
365	Social relationship paradigm applied to object interactions in industrial IoT	Bajic Eddy and Hajlaoui Oussama	2018	Sciencel	EC2	Rejected	
366	Software-defined networking to improve cybersecurity in manufacturing oriented inte	Fraile, F. and Flores, J.L. and Poler,	2019	Scopus	EC2	Rejected	
367	Standardisation connecting the initiative 'industry 4.0' and service life cycle	Freitag, M. and Zelm, M.	2015	Scopus	EC1	Rejected	
368	Study on the low energy consumption method for light-wight devices in IoT service env	Kim, Y.-H. and Kim, M.-S. and Park	2018	Scopus	EC2	Rejected	
369	Subject-oriented design of smart hyper-connected logistics systems	Neubauer, M. and Krenn, F.	2017	Scopus	EC2	Rejected	
370	Supporting a Cloud Platform with Streams of Factory Shop Floor Data in the Context of	W. M. {Mohammed} and B. R. {Fer	2018	IEEE	EC2	Rejected	
371	Sustainable Data Management for Manufacturing	Burow, K. and Franke, M. and Den	2019	Scopus	EC2	Rejected	
372	SustainaBLE: A power-aware algorithm for greener industrial IoT networks	Garrido-Hidalgo, C. and Hortelano	2017	Scopus	EC1	Rejected	
373	Syntactic translation of message payloads between at least partially equivalent encodi	Palm, E. and Paniagua, C. and Bod	2019	Scopus	EC1	Rejected	
374	System on chip generation for multi-sensor and sensor fusion applications	T. {Lieske} and B. {Pfundt} and S. {V	2017	IEEE	EC2	Rejected	
375	Testbed to verify interoperability among heterogeneous devices with OPC UA	Song, B. and Kim, H. and Lee, W. a	2017	Scopus	EC1	Rejected	
376	The adoption stages (Evaluation, Adoption, and Routinisation) of ERP systems with bus	Caetano Haberli Junior and Tiago	2019	Sciencet	EC2	Rejected	
377	The fourth industrial revolution (industry 4.0): Intelligent manufacturing	Hwang, J.S.	2016	Scopus	EC1	Rejected	
378	The global impact of telematics for health-care professionals	Healy, J.C.	1998	Scopus	EC1	Rejected	
379	The good, the bad and the ugly–the future of patent assertion entities in Europe	Thumm, N.	2018	Scopus	EC1	Rejected	
380	The Industrial Internet of Things as an enabler for a Circular Economy Hy-LP: A novel I	Hatzivasilis, G. and Fysarakis, K. an	2018	Scopus	EC1	Rejected	
381	The industry 4.0 standards landscape from a semantic integration perspective	Grángel-Gonzalez, I. and Baptista,	2018	Scopus	EC2	Rejected	
382	The new deal on data: A framework for institutional controls	Greenwood, D. and Stopczynski, A	2013	Scopus	EC1	Rejected	

383	The role of comprehensive function models in the management of heterogeneous indu	S. S. P. {Olaya} and M. {Wollschlae	2019	IEEE	EC2	Rejected	
384	The role of Information and Communication Technologies in healthcare: taxonomies, p	Giuseppe Aceto and Valerio Persic	2018	Sciencel	EC2	Rejected	
385	The Role of Interoperability in The Fourth Industrial Revolution Era	Liao, Y. and Ramos, L.F.P. and Satu	2017	Scopus	EC2	Rejected	
386	Toward Plug Play Cyber-Physical System Components	V. {Jirkovský} and M. {Obitko} and	2018	IEEE	EC2	Rejected	
387	Toward Plug&Play Cyber-Physical System Components	Jirkovsky, V. and Obitko, M. and K	2018	Scopus	EC1	Rejected	
388	Towards a knowledge-based framework for digital chain monitoring within the industr	Oussama Meski and Farouk Belkac	2019	Sciencel	EC2	Rejected	
389	Towards industrial Internet of Things: An efficient and interoperable communication fr	Eliasson, J. and Delsing, J. and Der	2015	Scopus	EC1	Rejected	
390	Towards integration between OPC UA and OCF	Cavalieri, S. and Mulè, S. and Salaf	2019	Scopus	EC1	Rejected	
391	Towards interoperability across digital manufacturing platforms	Wajid, U. and Bhullar, G.	2019	Scopus	EC1	Rejected	
392	Towards interoperability between OPC UA and OCF	Cavalieri, S. and Salafia, M.G. and	2019	Scopus	EC1	Rejected	
393	Towards the blockchain-enabled offshore wind energy supply chain	Keivanpour, S. and Ramudhin, A. a	2019	Scopus	EC1	Rejected	
394	Towards the shop floor app ecosystem: Using the semantic web for gluing together ap	Miclaus, A. and Clauss, W. and Sch	2016	Scopus	EC1	Rejected	
395	Trends in industrial communication and OPC UA	P. {Drahoš} and E. {Kučera} and O.	2018	IEEE	EC2	Rejected	
396	UH4SP: A Software Platform for Integrated Management of Connected Smart Plants	Santos, N. and Rodrigues, H. and P	2018	Scopus	EC1	Rejected	
397	Virtual Power Plant basic requirements for integration of Distributed Energy Resource	Nwauka, O. and Telukdarie, A. and	2018	Scopus	EC1	Rejected	
398	VSOMEIP - OPC UA Gateway Solution for the Automotive Industry	A. {Ioana} and A. {Korodi}	2019	IEEE	EC2	Rejected	
399	Warehouse development of ontology for providing semantic interoperability	Korneev, D. and Boichenko, A. and	2019	Scopus	EC1	Rejected	
400	Using a systems of systems modeling approach for developing Industrial Internet of Th	Morkevicius, A. and Bisikirskiene,	2017	Scopus	EC1	Rejected	

APPENDIX

B

SURVEY DOCUMENTATION

In this Appendix, we attached the survey we sent to the experts in Industry 4.0 and the first version of architecture drivers.

Architecture drivers for trustworthy interoperability in Industry 4.0

Hello!
If you have access to this form, it is because your opinion matter to us!
We need your expertise feedback to help us improve the main architecture drivers to enable trust Interoperable systems in the context of Industry 4.0.
To guide you, we divided this form in two main parts:
1) 3 questions about your professional experience;
2) 7 questions related to the main architectural drivers;
We thank you in advanced for this precious and reliable feedback!

We want to know more about you!

1. What role describes you best? Select the role that best characterizes your job.
    ( ) Software architect
    ( ) Software engineer
    ( ) Business analyst
    ( ) Project manager
    ( ) Requirements engineer
    ( ) Researcher
    ( ) Other: _____
    Years of experience: _____

2. How would you rate your experience with reference/enterprise architecture?
    1 2 3 4 5
    None ( ) ( ) ( ) ( ) ( ) Expert

3. How would you rate your experience with Industry 4.0?
    1 2 3 4 5
    None ( ) ( ) ( ) ( ) ( ) Expert

Questions about architecture drivers.

We designed 7 drivers that mainly encompass trust concerns for interoperable systems in the context of Industry 4.0. Please, give zoom in your browser to proper see the images.

Driver for Authentication

Driver Name	Authentication to the system	
Diver ID	AD.01 – SECURITY	
Description		**Quantification**
Environment	The application is installed on the system and has been started before at least once. The application is currently closed and waiting for authorized users/ devices to login.	The application starts at least once
Stimulus	His credentials are transmitted securely.	Secure authentication to the system
Response	Alternative a: The application accepts user's credentials and user authenticates in the system. Alternative b: The application does not accept user's credentials and user does not authenticate in the system.	Authentication <5s.

Is the architecture driver properly defined according to the Industry 4.0 context?

( ) The driver is approved and properly well defined.
( ) The driver is approved, but some details may require further refinement or elaboration.
( ) The driver is consolidate in some extents, but there are parts of the driver that need further elaboration.
( ) The driver is not well represented and must be redone.

What must be improved in the architecture driver?

_____

_____

Driver for Data Privacy

Name	Data privacy	
Diver ID	AD.02 – DATA PRIVACY	
Description		**Quantification**
Environment	Several industrial plants are interconnected and the control system is waiting for a proprietary material blueprint from one specific manufacturer.	Only 1 session per user/plant
Stimulus	The manufacturer uploads the proprietary blueprint to the control system.	Throughput <20KB/ms
Response	The control system activates the privilege access to attest the information will be read only by authorized users.	Only authorized users can have access to sensitive information

Is the architecture driver properly defined according to the Industry 4.0 context?

( ) The driver is approved and properly well defined.
( ) The driver is approved, but some details may require further refinement or elaboration.
( ) The driver is consolidate in some extents, but there are parts of the driver that need further elaboration.
( ) The driver is not well represented and must be redone.

What must be improved in the architecture driver?

_____

_____

Driver for Traceability and Auditability

Driver Name	Traceability and auditability of data	
Diver ID	AD.03	
Description		Quantification
Environment	Several industrial plants are interconnected and ready to send and receive data.	Only 1 session per user/plant
Stimulus	Information is being exchange between the control system, sensors, devices, and industrial partners.	Throughput <20KB/ms
Response	The control system records information regarding origin, state and location of materials, components and products, history and current status of data.	The system must keep track of data being transferred.

Is the architecture driver properly defined according to the Industry 4.0 context?

( ) The driver is approved and properly well defined.
( ) The driver is approved, but some details may require further refinement or elaboration.
( ) The driver is consolidate in some extents, but there are parts of the driver that need further elaboration.
( ) The driver is not well represented and must be redone.

What must be improved in the architecture driver?

_____

_____

Driver for Data Integrity

Driver Name	Data Integrity	
Diver ID	AD.04	
Description		Quantification
Environment	Several industrial plants are interconnected and the control system is waiting for sensors data reading.	Only 1 session per user/plants
Stimulus	During transmission of data from sensors to control system an electromagnetic radiation includes a random transmission error.	Throughput <20KB/ms
Response	The application initiates the integrity-protection mechanism to detect data errors.	No incorrect data can be transmitted.

Is the architecture driver properly defined according to the Industry 4.0 context?

( ) The driver is approved and properly well defined.
( ) The driver is approved, but some details may require further refinement or elaboration.
( ) The driver is consolidate in some extents, but there are parts of the driver that need further elaboration.
( ) The driver is not well represented and must be redone.

What must be improved in the architecture driver?

_____

_____

Driver for Availability

Driver Name	Availability	
Diver ID	AD.05	
Description		Quantification
Environment	An authorized user is logged in the system.	Only 1 session per user/plant
Stimulus	A peak of energy turns off the main server.	The main server must be restored in less than 1 hour.
Response	An alert window is presented and the connection is immediately reestablished with a backup server.	System available 99% of the time

Is the architecture driver properly defined according to the Industry 4.0 context?

( ) The driver is approved and properly well defined.
( ) The driver is approved, but some details may require further refinement or elaboration.
( ) The driver is consolidate in some extents, but there are parts of the driver that need further elaboration.
( ) The driver is not well represented and must be redone.

What must be improved in the architecture driver?

_____

_____

Driver for Scalability

Name	Scalability of data and services	
Diver ID	AD.06	
Description		Quantification
Environment	Several industrial plants are interconnected and are logged in the system	Only 1 session per user/plant
Stimulus	A new user send a request to be part of the system	
Response	Authorized users add and give grants for a new user to be part of the system.	# of different connections

Is the architecture driver properly defined according to the Industry 4.0 context?

( ) The driver is approved and properly well defined.
( ) The driver is approved, but some details may require further refinement or elaboration.
( ) The driver is consolidate in some extents, but there are parts of the driver that need further elaboration.
( ) The driver is not well represented and must be redone.

What must be improved in the architecture driver?

_____
_____

Driver for data consistency

Driver Name	Consistency of data	
Diver ID	AD.07	
Description		Quantification
Environment	Several industrial plants are interconnected and the control system is waiting for data to be transmitted.	Only 1 session per user/plant
Stimulus	The control system gets real time data via multiple sources and production feedback data.	
Response	A consistent mechanism automatically checks the real time data to avoid inconsistencies.	I/O fails after Timeout >20s

Is the architecture driver properly defined according to the Industry 4.0 context?

( ) The driver is approved and properly well defined.
( ) The driver is approved, but some details may require further refinement or elaboration.
( ) The driver is consolidate in some extents, but there are parts of the driver that need further elaboration.
( ) The driver is not well represented and must be redone.

What must be improved in the architecture driver?

_____
_____

Which architecture drivers are still missing?

_____
_____

APPENDIX

C

INTERVIEW DOCUMENTATION

In this Appendix, we present the consent form and the architecture drivers used during the interview with experts of Industry 4.0.

INTERVIEW CONSENT FORM

Research project title: Promoting Trust in the Interoperability of Industry 4.0
Research investigator: Ana Paula Allian
Research Participants name: xxxxxxxxxxx
Duration of the interview: One hour

Thank you for agreeing to be interviewed as part of the above research project. Ethical procedures for academic research require that interviewees explicitly agree to being interviewed and how the information contained in their interview will be used. This consent form is necessary for us to ensure that you understand the purpose of your involvement and that you agree to the conditions of your participation. Would you therefore read the accompanying information sheet and then sign this form to certify that you approve the following:

- the interview will be audio recorded and a transcript will be produced;
- the transcript of the interview will be analyzed by **Ana Paula Allian** as research investigator;
- access to the interview transcript will be limited to **Ana Paula Allian**;
- any summary interview content, or direct quotations from the interview, that are made available through academic publication or other academic outlets will be anonymized so that you cannot be identified, and care will be taken to ensure that other information in the interview that could identify yourself is not revealed;
- the actual recording will be destroyed after completing this work;
- all or part of the content of your interview may be used in academic papers.

By signing this form I agree that

1. I am voluntarily taking part in this project. I understand that I don't have to take part, and I can stop the interview at any time;
2. The transcribed interview or extracts from it may be used as described above;
3. I don't expect to receive any benefit or payment for my participation;
4. I can request a copy of the transcript of my interview and may make edits I feel necessary to ensure the effectiveness of any agreement made about confidentiality;
5. I have been able to ask any questions I might have, and I understand that I am free to contact the researcher with any questions I may have in the future.

Kaiserslautern, November 28, 2019.

_____
xxxxxxxxxxxxxxxxxx

_____
Ana Paula Allian

ARCHITECTURE DRIVERS, ARCHITECTURE SOLUTIONS AND ARCHITECTURE DECISIONS BASED ON BLOCKCHAIN

ARCHITECTURE DRIVER AUTHENTICATION

Driver Name	Authentication to the system	Quantification
Environment	• Application installed on the system with an authentication solution already implemented. • There is ever-changing system that needs to support addition and removal of new devices in an efficient way. • Digital Twins exists for each object in the production line.	• Number of objects.
Stimulus	• Devices and users need to authenticate into the application and credential token is acquired during authentication.	• Authentication token!=null.
Response	• **Alternative a:** The application accepts devices/users credentials and user authenticates in the system. • **Alternative b:** The application does not accept device/users credentials and user does not authenticate in the system.	• Number of objects authenticated to the system > 0.

ARCHITECTURE SOLUTION FOR DRIVER AUTHENTICATION

Decision Name	Certificate Authorities for Authentication to the system	
Steps	1. Application requires authorized access through certificate authorities (CA) using a public key infrastructure (PKI), since the solutions are distributed. 2. The user sends his certificate to the system. 3. The application checks the validity of the CA public key. 3.1 If connection is accepted, the user is successfully login in the system. 3.2 If connection is rejected, a warning message is presented to the user and data is saved in log files.	
Design decisions	DD.01.01	
Pros & Opportunities		**Cons & Risk**
• Verification of identity to prevents non-repudiation. • More secure and confidential for online transactions. • Integrity is guaranteed, as long as CA can be verified.		• Users must trust the CA in generating and managing their public keys. • Single point of failure, if the CA fails. • The management of the public keys by one centralized CA can be both expensive and inefficient.
Assumption & Quantifications		**Trade-Offs**
• The application starts at least once. • Secure authentication to the system. • Authentication at minimal time possible.		• Availability. • Performance.

ARCHITECTURE DECISION RATIONALE FOR DRIVER AUTHENTICATION

Decision Name	Authentication to the system with Blockchain-Based PKI Concept	
Design Decision ID	DD.01.01	
Explanation	Blockchain-based PKI is a distributed solution to promote trust based on the majority vote from parties.	
Pros & Opportunities		**Cons & Risk**
• No centralized point of failure. • No centralized authority. • Open source implementations.		• Hard to come up into an agreement of all parties in the majority vote. • More complex to be developed and maintained.
Assumption & Quantifications		**Trade-Offs**
• The application starts at least once. • Secure authentication to the system. • Authentication at minimal time possible.		• Performance.

ARCHITECTURE DRIVER DATA ACCESS CONTROL

Driver Name	Data Access Control	Quantification
Environment	• Supplier wants to pass profitable information to manufacturer, e.g. blueprint on his two product types. • The system has to manage a number of distinct stakeholders with different access rights.	• Stakeholders and devices >0.
Stimulus	• Supplier extracts information from the product, makes a package, and hands it over to the manufacturer. • Manufacturer has ordered the package might only have read permissions for sensors and devices.	• Number of data entries >0.
Response	• The control system activates the privilege access to attest the information will be read only by authorized users. • The information of the access control is retrieved from its Digital Twin, which uses access control application to manage access to data.	• ObjectID !=null

ARCHITECTURE SOLUTION FOR DRIVER DATA ACCESS CONTROL

Name	**Access authorization control to the system using ACL**
Steps	1. The application calls the authorization method to check the access control list (ACL) to determine the privileges of user or device. 2. The ACL specifies the access rights allowed, denied, or audited for that trustee access to a securable object. 3. The system checks the ACL in sequence until it finds one or more role that allow all the requested access rights, or until any of the requested access rights are denied.
Decisions	DD.02.01

Pros & Opportunities	**Cons & Risk**
• Confidentiality. • Centralized decision can control who access the system.	• Efficiency is a problem, because it uses homomorphic encryption, which is complex. • Difficult to scale with the massive amount of data processing required in the current networks. • ACL causes overhead in processing and managing the rules. • There is the need of a centralized decision to control who access the system.
Assumption & Quantifications	**Trade-Offs**
• Only authorized users can have access to sensitive information. • Maximum transfer rate. • Only 1 login per user/plant.	• Performance. • Scalability.

ARCHITECTURE DECISION RATIONALE FOR DRIVER DATA ACCESS CONTROL

Name	**Decentralized Authorization with Blockchain**
Decision ID	DD.02.01
Explanation	The Blockchain provide decentralized end-to-end data privacy through policies defined in smart contracts or on the data management messages.

Pros & Opportunities	**Cons & Risk**
• Data ownership and control are decentralized. • The user has full control to define its ACL. • Can combine smart contracts with ACL, and user has full control to define its ACL.	• Complex to develop, because it still needs to use the homomorphic encryption. • Scale better than the ACL technique, but scalability may still be a problem in big distributed systems.
Assumption & Quantifications	**Trade-Offs**
• Only authorized users can have access to sensitive information. • Maximum transfer rate. • Only 1 login per user/plant.	• Performance. • Scalability.

ARCHITECTURE DRIVER DATA PRIVACY

Name	Driver for data privacy to protect intellectual property	Quantification
Environment	• Multiple devices and users exist and are offering a number of capabilities. • Digital Twins exist for each object of the production line. • Possible customers need to be able to access certain data such as the status of their current production line and products, but they must not be able to access data from other customers.	• Number of devices.
Stimulus	• One manufacturer transmits anonymously industrial secrets data that is under jurisdiction protection through the system. • The sensitive data is target as anonymous before sending to authorized users.	• Product blueprint as Digital Twin.
Response	• The information of the product is retrieved from its Digital Twin, which has control access regulations implemented. • The production is scheduled on a private particular plant for only authorized users to have access.	• Processing state of new product = scheduled.

ARCHITECTURE SOLUTION FOR DRIVER DATA PRIVACY

Name	Protection of data Privacy with Encrypted data	
Steps	1. Definition of security needs. 2. Select an encryption protocol and tool. 3. Implement the encryption strategy. 4. Implement decryption.	
Decisions	DD.03.01	
Pros & Opportunities		**Cons & Risk**
• Encrypting sensitive data can add to an organization's ROI in security. • Encryption protects and isolates data between users, companies and third-parties with access to the data.		• Need a data-centric encryption.
Assumption & Quantifications		**Trade-Offs**
• Stakeholders and devices >0. • Number of data entries >0. • ObjectID !=null.		• Availability.

ARCHITECTURE DECISION RATIONALE FOR DRIVER DATA PRIVACY

Name	Protection of data Privacy based on Blockchain and pseudonymise all personal data	
Decision ID	DD.03.01	
Explanation	Blockchain can encrypt all sensitive data and separate it into segments that would be accessible to authorized parties at any time. These segments are also known as pseudonymisation, personal identifiers are maintained off the Blockchain, with some mechanism to link back to the chain.	
Pros & Opportunities		**Cons & Risk**
• Enhances privacy by replacing most identifying fields within a data record by one or more artificial identifiers. • Sensitive data are no longer available on the chain.		• If the identifiers from off-Blockchain are deleted, the on-chain data will be anonymised.
Assumption & Quantifications		**Trade-Offs**
• Stakeholders and devices >0. • Number of data entries >0. • ObjectID !=null.		• Availability.

ARCHITECTURE DRIVER FOR TRACEABILITY AND AUDITABILITY OF DATA

Driver Name	Traceability and auditability of data	Quantification
Environment	• Several industrial plants are interconnected and ready to send and receive data. • Arbitrary transactions between objects are possible. • Multiple devices and users exist and are connected to the system.	• Number of devices. • Number of users / plants.
Stimulus	• Plant needs to be assigned, be maintained, and be reconfigured for new products. • The plant engineer and autonomous decision engine initiates the configuration of devices.	• New time stamp Value!=Old time stamp value.
Response	• The system records every step in a process chain, from raw material to the final product, tracking what was changed, in which way, and who did the changes. • The systems provide immutability of data and tamper-resistant records to support stakeholders during decision rational.	• The working production continues.

ARCHITECTURE SOLUTION FOR DRIVER TRACEABILITY AND AUDITABILITY OF DATA

Name	**Traceability and auditability of data with Provenance-Aware Storage Systems**	
Steps	1. The application uses Provenance-Aware Storage Systems (PASS), a provenance approach to tracks files in a distributed system for further auditability. 2. PASS collects and maintains information about the operations done at the system level. 3. The data is collected in a centralized fashion and verified by centralized users.	
Decisions	DD.04.01	
Pros & Opportunities		**Cons & Risk**
• It helps the network administrators in detecting any access violation or any malicious operation. • Increase availability of data and confidence of data.		• Distributed systems have several layers of interoperability, which make the logging techniques inefficient. • Complexity, because distributed systems provide load balancing. • Lack of privacy if encryption is not implemented. • Centralized controller is needed to monitor the system.
Assumption & Quantifications		**Trade-Offs**
• Only 1 session per user/plant. • Minimum possible Throughput. • The system must keep track of data being transferred.		• Privacy. • Performance.

ARCHITECTURE DECISION RATIONALE FOR DRIVER TRACEABILITY AND AUDITABILITY OF DATA

Name	**Traceability based on Blockchain**	
Decision ID	DD.04.01	
Explanation	Blockchain provides the data provenance service by recording the evidence of the data originality and the operations in the Blockchain transactions	
Pros & Opportunities		**Cons & Risk**
• Provides non-reputability of data. • It is less complex, because it delegates the provenance service among nodes in the network. • No centralized controller.		• This system is more complex to be developed.
Assumption & Quantifications		**Trade-Offs**
• Only 1 session per user/plant. • Minimum possible Throughput. • The system must keep track of data being transferred.		• Performance.

ARCHITECTURE DRIVER AVAILABILITY OF PHYSICAL DEVICES

Driver Name	Availability of devices	Quantification
Environment	• The Production line is working with at least one product scheduled. • There are at least two objects with redundant capabilities in the production line, such as the primary object and its redundancy. • The primary device is processing at least one product workpiece.	• Number of devices. • Number of products.
Stimulus	• An unexpected event happened and turns off the main device. • The primary device with defects is identified by the plant supervision system.	• An error alert is presented in the primary device.
Response	• Status of workpiece is retrieved from its Digital Twin, which calculates the capacity of the device to process the product workpiece. • If capacity is available on the device redundancy, the workpiece is rescheduled to it. • The workpiece is automatically or manually removed from the physical primary device. • The production continues in the redundant device.	• Number of not completed workpieces = zero. • State of the process P=producing. • Number of reschedules = one.

ARCHITECTURE SOLUTION FOR DRIVER AVAILABILITY OF PHYSICAL DEVICES

Decision	Availability of devices
Steps	1. The applications operate by using groups or clusters. 2. When a HW/SW faults, cluster immediately starts the application in another system, without requiring administrative intervention. 3. The controller activates the group servers, which can be utilized with a minimal amount of downtime when a server node fails.
Decision	DD.05.01

Pros & Opportunities	Cons & Risk
• No single point of failure.	• Not all software applications support clustered environment. • Cost is high, since the cluster needs good hardware. • Scalable performance. • Relies on a centralized controller, which could do whatever it wants with data.
Assumption & Quantifications	**Trade-Offs**
• Only 1 session per user/plant. • The main server must be restored as quickly as possible.	• Consistency. • Performance. • Scalability.

ARCHITECTURE DECISION RATIONALE FOR DRIVER AVAILABILITY OF PHYSICAL DEVICES

Decision Name	Availability of devices based on Blockchain
Decision ID	DD.05.01
Explanation	Blockchain ledger with distributed databases to allow the registration of data and transactions on the chain without losing the tamper-evident benefits brought by the Blockchain technology.

Pros & Opportunities	Cons & Risk
• Blockchain data is distributed across a large network of computers. • Blockchain is resilient against data loss and infrastructure failures. • Data is immutable.	• Distributed systems ledgers can grow very large over time.
Assumption & Quantifications	**Trade-Offs**
• Only 1 session per user/plant. • The main server must be restored as quickly as possible.	• Performance. • Scalability.

ARCHITECTURE DRIVER AVAILABILITY OF DATA

Driver Name	Driver for availability of data	Quantification
Environment	• The Production line is working with at least one product scheduled. • The manufacturer have obligation to document and make available the production line process.	• Number of devices. • Number of years to keep documents recorded.
Stimulus	• The primary device is processing at least one product workpiece. • Designated representatives of manufacturing production require the verification of data related to a specific technical requirement (i.e., temperature and bombing pressure in a specific time of production line).	• New time stamp Value != Old time stamp value.
Response	Documents records are retrieved from its Digital Twin according to specific time.	New time stamp Value != Old time stamp value.

ARCHITECTURE SOLUTION FOR DRIVER AVAILABILITY OF DATA

Decision	Availability of data and services
Description	Digital twins are replicas of physical devices in a production line. They naturally are develop to replicate each objective and diagnose problems.
Steps	1. The applications loads the Digital Twin. 2. The higher-layer application accesses the Digital Twin to retrieve the data. 3. Digital twins diagnose a problem and automatically send warning alert of error.
Decision	DD 06.01

Pros & Opportunities	**Cons & Risk**
• Standardized structure that can be used for simulation	• Collect irrelevant data just because it is possible. • Relies on a centralized controller, which could do whatever it wants with the data.
Assumption & Quantifications	**Trade-Offs**
• Only 1 session per user/plant • State of assets are measured	• Overhead

ARCHITECTURE DECISION RATIONALE FOR DRIVER AVAILABILITY OF DATA

Decision Name	Availability of data based on Blockchain
Decision ID	DD 06.01
Explanation	Blockchain ledger with distributed databases to allow the registration of data and transactions on the chain without losing the tamper-evident benefits brought by the Blockchain technology.

Pros & Opportunities	**Cons & Risk**
• Blockchain data is distributed across a large network of computers. • It is resilient against data loss and infrastructure failures. • Immutable of data.	• Distributed systems ledgers can grow very large over time.
Assumption & Quantifications	**Trade-Offs**
• Only 1 session per user/plant. • The main server must be restored as quickly as possible.	• Performance. • Scalability.

ARCHITECTURE DRIVER COMPATIBILITY OF DATA AND SERVICES

Name	Compatibility of data and services	Quantification
Environment	• The Production line is working with at least one product scheduled. • Many devices offering several capabilities must exchange data. • Digital twins exist for each object.	• Number of devices. • Number of products.
.Stimulus	• A new product line is added to the manufacturing system. • New digital twins for each object from the product line exist.	• Number of products ordered increases > 0
Response	• The system loads Digital Twins of new product line to understand their main components without human intervention. • The system supports the new production line integrating them into a unified enterprise architecture layer.	• Number of new digital twins = number of real objects from the new product line

ARCHITECTURE SOLUTION FOR DRIVER COMPATIBILITY OF DATA AND SERVICES

Name	Compatibility of data based on middleware	
Steps	1. The application implements middleware. 2. The middleware provides a collection of coupled services to garner support across wide array of platforms and devices. 3. Middleware can be used to add or remove entities as needed.	
Decisions	DD.07.01	
Pros & Opportunities		**Cons & Risk**
• Integration of different protocols. • Homogeneous communication. • Integration of legacy devices.		• Hard to ensure real-time compliance with the physical communication buses. • Security issues (harder to maintain transaction secure)
Assumption & Quantifications		**Trade-Offs**
• Elements navigating in the VAB are available through the type property of every Property element. • # of different connections		• Privacy. • Performance.

ARCHITECTURE DECISION FOR DRIVER COMPATIBILITY OF DATA AND SERVICES

Decision Name	Compatibility of data and services based on consortium Blockchain	
Decision ID	DD.07.01	
Explanation	A consortium Blockchain and Smart contracts to define common semantic standards based on standards used by industrial environment. These standards should be agreed in advance by the consortium of organizations in a Blockchain network	
Pros & Opportunities		**Cons & Risk**
• Facilitates the inclusion of nodes and new participants to work in the same infrastructure.		• Block size can be big. • Response time can be longer. • Higher costs.
Assumption & Quantifications		**Trade-Offs**
• Only 1 session per user/plant. • Any change in the system must be agreed by all authorized users. • # of different connections.		• Performance.

APPENDIX

D

LIST OF CODES

In this Appendix, we attached the complete list of codes from interviews with experts of Industry 4.0.

Categories	Codes	Amount
Authentication	Describe better public key	6
Authentication	Tradeoff must be well defined	3
Authentication	Blockchain may not bring benefits	12
Authentication	Quantification in authentication needs precise information	6
Authentication	Majority vote is difficult to be applied	2
Authentication	Traditional solution solves the problem for authentication	9
Authentication	Blockchain may bring benefits	8
Authentication	Blockchain needs a central authority	10
Authentication	Blockchain could provide self authorization companies.	4
Authentication	Performance is a tradeoff with Blockchain	4
Authentication	Authentication driver describe high level user authentication	6
Authentication	Blockchain can help to bring transparency in the whole chain	2
Authentication	Blockchain allows to synchronize changes to every participant	1
Authentication	Decentralized solution is good to identify people	2
Authentication	Authentication driver should follow regulations	1
Authentication	The production process should authenticate	2
Authentication	Blockchain is not mature for authentication	2
Data Privacy	Quantifiation in Privacy needs precise information	3
Data Privacy	Data integrty is not solved with driver privacy	2
Data Privacy	Tradeoff is inconsistent for Privacy	3
Data Privacy	Decentralized solution is a good option for I4.0	2
Data Privacy	Privacy of data should follow some regulation	19
Data Privacy	Blockchain should be combined with traditional techinologies	13
Data Privacy	Blockchain should ensure protection of data	2
Data Privacy	Blockchain enables transparency to Privacy	2
Data Privacy	Privacy driver is too generic	1
Data Privacy	There is the need to trust in the whole configuration	2
Data Privacy	Continuous communication is needed	2
Traceability	Traceability is well defined	1
Traceability	Tradeoff is inconsistent for Traceability	5
Traceability	Traceability can not garantee consistency of data	2
Traceability	Quantification in traceability needs precise information	3
Traceability	Blockchain does not support big amount of data	2
Traceability	Blockchain must be combined with traditional technology	13
Traceability	Blockchain cannot help traceability to restore the data	2
Traceability	Blockchain cannot guarantee security	1
Traceability	Blockchain decrease performance if used to encrypt documents	1
Traceability	External authorities must trust in the data	1
Traceability	Blockchain can store data immutable way	4
Traceability	Blockchain allows to put hash value	4
Traceability	Blockchain keeps track of data	8
Traceability	Blockchain allows to share data beteween companies	1
Traceability	The best solution is always connected to standards	3
Traceability	Traceability driver is too generic	3
Availability of Data	Quantification in Availability needs precise information	12
Availability of Data	Physical twins support availiabity of data	1
Availability of Data	Blockchain must be combined with traditional solutions	8
Availability of Data	Blockchain is not a good solution for availability of data	7
Availability of Data	This driver describes redundancy of data	3
Availability of Data	Traditional solutions can support availability of data	14
Availability of Data	Bockchain holds the hash value, but not the data	6
Availability of Data	Tradeoff should be well defined	3
Availability of Data	Blockchain can help identify the data is not corrupted in the process	1
Availability of Data	Blockchain depends on the application domain	1
Availability of Data	Distributed systems allow replication of data	3
Compatibility	Tradeoffs is inconsistent for Compatibility	2
Compatibility	Blockchain is not a good solution for compatbility	15

Compatibility	Quantification for compatibility is not well defined	5
Compatibility	Blockchain Offchain might help in compatibility	1
Compatibility	Traditional solutions solve the problem for Compatibility	8
Compatibility	Compatibility is the system prepared for some extension	2
Compatibility	Compatibility should have mechanism to change the facilities	3
Compatibility	Smart contracts would assume what devices and how to be compatible.	2
Compatibility	Compatibility should be better described	1
Compatibility	Performance is not a tradeoff for compatibility	1
Access Control	Access control driver should control devices and users	23
Access Control	Access control list should be better described	13
Access Control	Access control based on multiple roles or attibutes	4
Access Control	Scaling is not a tradeoff for Access Control	2
Access Control	Decentralized access control is a good solution for I40	4
Access Control	Partners may need a centralized decision	10
Access Control	Quantification in access control should be better defined	3
Access Control	Access control list should be stored somewhere	2
Access Control	Blockchain might not be a good solution for access control	1
Access Control	Blockchain may be a good solution for acess control	1
Access Control	Blockchain could be good for transparency	1
Access Control	Blockchain solution should be detailed	4
Access Control	Traditional approaches could solve problems to access control	5
Access Control	Scalability is a tradeoff for traceability	2
Access Control	Performance is a tradeoff for Blockchain	3
Access Control	Availability is a tradeoff for Access control	1
Availability of devices	Describe better solution for availabiiy of devices	3
Availability of devices	Redundancy availabity of devices is needed	14
Availability of devices	Quantification of availability of devices should be better described	11
Availability of devices	Blockchain is not a good solution for availability of devices	15
Availability of devices	Traditional solution solve availability of devices	4
Availability of devices	data should be centralized	1
Availability of devices	Availabilty of device is related to a better quality of service	6
Availability of devices	Cost is a tradeoff for availability of devices	1
Availability of devices	Performance is not a tradeoff for availability	2
Availability of devices	Scalability is not a tradeoff for availability	1
Availability of devices	Replication is not transparent process	1
Availability of devices	Availability is related to maintainability	3

APPENDIX

E

DECLARATION OF ORIGINAL AUTHORSHIP AND LIST OF PUBLICATIONS

I, Ana Paula Allian, declare that this thesis and the work presented in it are my own and has been generated by me as the result of my own original research. I confirm that this work was done wholly or mainly while in candidature for a degree at the University of São Paulo. Where I have consulted the published work of others, this is always clearly attributed. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself. Excerpts of this dissertation have been either published or submitted for the appreciation of editorial boards of journals, conferences, and workshops, according to the list of publications presented below.

Publications resulting from this thesis

During the conduction of this PhD project, the following works were published in international conferences and journals:

- **ALLIAN**, A. P., Schnicke, F., Antonino, P. O., Rombach, D., Nakagawa, E. Y. (2020). Architecture Drivers for Trustworthy Interoperability in Industry 4.0.

  Journal: IEEE System Journal. 1-10. *(Approved for publication)*

  Level of contribution: High – the PhD candidate is the main investigator.

- **ALLIAN**, A. P. : Promoting trust in interoperability of systems-of-systems.

  Conference: European Conference on Software Architecture (ECSA) 2019: 67-70. DOI: 10.1145/3344948.3344953

Level of contribution: High – the PhD candidate is the main investigator.

- **ALLIAN**, A. P., Schnicke, F., Antonino, P. O., Rombach, D., Nakagawa, E. Y. (2020). Can Blockchain assure Trustworthy Interoperability in Industry 4.0?

  Journal: Journal of Industrial Information Integration (IF = 10.615).Pages 1–10. *(Submitted on October, 2020)*.

  Level of contribution: High – the PhD candidate is the main investigator.

- **ALLIAN**, A. P., Schnicke, F., Antonino, P. O., Rombach, D., Nakagawa, E. Y. (2020). TIBA - Trust Interoperability Architecture for Industry 4.0. Pages

  Journal: International Journal of Computer Integrated Manufacturing (IF = 2.861). Pages 1–12. *(Will be Submitted on December, 2020)*.

  Level of contribution: High – the PhD candidate is the main investigator.

- **ALLIAN**, A. P.; Oliveira, E.; Capilla, R.; Nakagawa, E. Y. Have Variability Tools Fulfilled the Needs of Software Industry?

  Journal: Journal of Universal Computer Science, 1-16, 2020. *Approved for publication*

  Level of contribution: Medium – the PhD candidate is the main investigator.

- **ALLIAN**, A. P., CAPILLA, R., and NAKAGAWA, E. Y. (2019). Observations from variability modelling approaches at the architecture level.

  Book chapter: In Software Engineering for Variability Intensive Systems - Foundations and Applications, pages 41?56. Taylor and Francis. DOI: 10.1201/9780429022067-2

  Level of contribution: Medium – the PhD candidate is the main investigator.

- **ALLIAN**, A. P.; SENA, B., NAKAGAWA, E. Y. Evaluating variability a the software architecture level: an overview.

  Conference: Symposium on Applied Computer SAC 2019: 2354-2361. DOI: 10.1145/3297280.3297511

  Level of contribution: Medium – the PhD candidate is the main investigator.

- **ALLIAN**, A. P.; OliveiraJr, E.; Nakagawa, E. Y. Variability in Software Product Lines. 1–13

  Book chapter: UML-based Software Product Line Engineering with SMarty *(To be submitted)*

  Level of contribution: High – The PhD candidate participated in the research conduction and paper writing.

Other related publications

- SENA, Bruno ; Garces, Lina ; **ALLIAN**, Ana Paula ; Nakagawa, Elisa Yumi . Investigating the applicability of architectural patterns in big data systems.

  Conference: Pattern Languages of Programs (PLoP). PLoP 2018, Estados Unidos. 2018. p. 1-8. DOI: 10.5555/3373669.3373677

  Level of contribution: Medium – The PhD candidate participated in the research conduction and paper writing.

- SENA, B.; **ALLIAN**, A. P.; Nakagawa, E. Y.. Characterizing Big Data Software Architectures: A Systematic Mapping Study.

  Conference: Brazilian Symposium on Software Components, Architectures, and Reuse (SBCARS). Fortaleza, Ceará, Brazil. p.1-10, 2017. DOI: 10.1145/3132498.3132510

  Level of contribution: Medium – The PhD candidate participated in the research conduction and paper writing.

- Nakagawa, E. Y.; **ALLIAN**, A. P.; Oliveira, B.; Sena, B.; Paes, C.; Lana, C. et al.,. Software architecture and reference architecture of software-intensive systems and systems-of-systems: contributions to the state of the art.

  Conference: European Conference on Software Architecture (ECSA). Canterbury, United Kingdom, p.4-11, 2017;

  Level of contribution: Medium – The PhD candidate participated in the research conduction and paper writing. DOI: 10.1145/3129790.3129822

- Fioravanti, M. L.; Sena. B.; Paschoal, L. N.; Silva L. R.; **ALLIAN**, A. P.; Nakagawa, E. Y.; Souza, R. R. S.; Isotani, S.; Barbosa, E. F.. A Project Based Learning Approach for Software Engineering Teaching: An Experience Report.

  Conference: Special Interest Group on Computer Science Education (SIGCSE) Baltimore, Maryland, USA. p 1-6. 2017. DOI: 10.1145/3159450.3159599

  Level of contribution: Medium – The PhD candidate participated in the research conduction and paper writing.

- KASSAB, M., NETO, V., **ALLIAN**, A. P: Investigating quality requirements from a human perspective in IoT-based software architectures for education.

  Conference: European Conference on Software Architecture (ECSA) 2019: 241-244. DOI: 10.1145/3344948.3344978

  Level of contribution: Low – The PhD candidate participated in the research.

- VOLPATO, T., **ALLIAN**, A. P, NAKAGAWA, E. Y.: Has social sustainability been addressed in software architectures?

  Conference: European Conference on Software Architecture (ECSA) 2019: 2019: 245-249. DOI: 10.1145/3344948.3344979

  Level of contribution: Low – The PhD candidate participated in the research.

- Nakagawa, E. Y.; **ALLIAN**, A. P.; Guessi, M.; Galster, M.; OliveiraJR, E.; FERA: An Lightweight Approach to Evaluate Architectural Description of Reference Architectures, TOSEM,

  Journal: Transactions on Software Engineering and Methodology (TOSEM). p. 1-35, 2020. *(To be submitted)*

  Level of contribution: Medium – The PhD candidate participated in the research conduction and paper writing.

- Guessi, M; Garces, L; **ALLIAN**, A. P.; Lana, C. A.; Felizardo, K. R.; Navarro, E.; Nakagawa, E. Y. Women Representativeness in the Software Architecture Community: a Systematic Mapping.

  Journal: Journal of Informetrics, p. 1-32, 2020. *(To be submitted)*

  Level of contribution: Medium – The PhD candidate participated in the research conduction and paper writing.

- Sena, B.; Garces, L.; **ALLIAN**, A. P.; Nakagawa, E. Y. KE-SoS: A Process for Knowledge Extraction from Systems-of-Systems.

  Conference: International Workshop on Software Engineering for Systems-of-Systems (SESoS), p.1-8. *(To be submitted)*

  Level of contribution: Medium – The PhD candidate participated in the research conduction and paper writing.


ICMC
USP
SÃO CARLOS