future internet

MDPI

Article

Structuring Reference Architectures for the Industrial Internet of Things

Sebastian R. Bader [1,*], Maria Maleshkova [2,*] and Steffen Lohmann [1]

[1] Fraunhofer IAIS, Schloss Birlinghoven, 53757 Sankt Augustin, Germany
[2] University of Bonn, Endenicher Allee 19a, 53115 Bonn, Germany
* Correspondence: sebastian.bader@iais.fraunhofer.de (S.R.B.); maleshkova@cs.uni-bonn.de (M.M.)

Received: 15 June 2019 ; Accepted: 2 July 2019; Published: 8 July 2019

Abstract: The ongoing digital transformation has the potential to revolutionize nearly all industrial manufacturing processes. However, its concrete requirements and implications are still not sufficiently investigated. In order to establish a common understanding, a multitude of initiatives have published guidelines, reference frameworks and specifications, all intending to promote their particular interpretation of the Industrial Internet of Things (IIoT). As a result of the inconsistent use of terminology, heterogeneous structures and proposed processes, an opaque landscape has been created. The consequence is that both new users and experienced experts can hardly manage to get an overview of the amount of information and publications, and make decisions on what is best to use and to adopt. This work contributes to the state of the art by providing a structured analysis of existing reference frameworks, their classifications and the concerns they target. We supply alignments of shared concepts, identify gaps and give a structured mapping of regarded concerns at each part of the respective reference architectures. Furthermore, the linking of relevant industry standards and technologies to the architectures allows a more effective search for specifications and guidelines and supports the direct technology adoption.

Keywords: industrial internet of things; data exchange frameworks; reference frameworks

1. Introduction

The expected disruptive developments collectively referred to as the Internet of Things (IoT) have drawn significant attention in many industries, disciplines and organizations. While the concrete benefits and requirements are still not sufficiently clear, the general agreement on its relevance and impact is undeniable. As a result, a large number of initiatives and consortia from industry and research have been formed to all set the de facto standards and best practices.

Especially the manufacturing industry is actively involved in numerous activities related to this topic. Organizing this area and enabling effective discussions and design decisions are the targets of several standardization efforts. Many of them provide reference frameworks and architecture models. Reference frameworks in this context provide the necessary structure to transform the combined experiences and best practices, the opportunities of available technologies and the expected implications into understandable guidance for the involved stakeholders [1].

As a common understanding has not yet been reached, the current situation is characterized by the variety of proposed models and frameworks, created by groups of experts from different countries and domains. Whereas the goal of each approach is to overcome the current confusion, the huge amount of published models is again becoming a source of heterogeneity and misunderstanding. Newcomers and non-experts are overwhelmed by the amount of published recommendations and suggestions, contradicting terminology, inconsistent structuring and proposed best practices. The uncountable efforts intended to structure the domain have by now created another dimension of complexity.

The thereby created barriers aggravate the adaption of crucial developments and decelerate further progress. Moreover, the rising difficulty to find and classify relevant information undermines the further propagation of the core principles.

Therefore, a consistent alignment of the different frameworks and a structured organization of the main concepts are a pressing need, in order to create a sufficiently complete picture of the current state of the specification processes. Following the assumption that a single model can not cover all requirements, we annotated and interlinked the frameworks and models of the most influential initiatives, which cope with the digitization of the manufacturing domain. An openly available knowledge graph with self-defined and both human and machine-readable concepts, serves as the representation of the derived facts. Based on this grounded mapping of discovered relations, variances and commonalities we illustrate the different scopes and strengths.

This paper contributes to the mentioned challenges by:

1. Providing a methodology to structure, align and compare the various reference frameworks;
2. Presenting a collection of relevant concerns, their hierarchical structure and relationships;
3. Providing configurable visual views of the characteristics and relations between the concerns and the reference frameworks (http://i40.semantic-interoperability.org/sto-visualization/);
4. Offering an analysis of the thereby gained insights, for example, frequently covered areas or inconsistencies, which need further attention from the community.

The remainder of this paper is structured as follows: Section 2 gives an overview of other approaches to structure the observed frameworks and of surveys of the IIoT domain. The used methodology and data model is introduced in Section 3, followed by a description how the IIoT reference frameworks have been selected (Section 4) and an introduction of the most relevant ones in Section 5. We discuss the limitations of our approach in Section 6, followed by an outline of the findings and outline research gaps in Section 7 and conclude with our lessons learned and future activities (Section 8).

2. Related Work

In the following, the definitions as collected by Reference [2] are used. The terms 'Industrial Internet' (as defined by Reference [3]), 'Industry 4.0' (as defined by Reference [4]), 'Industrial Internet of Things' (as defined by Reference [2]) or even 'Cyber-physical Systems' (as defined by Reference [5]) all have different variations. In the following, in order to increase readability, we will stick to 'Industrial Internet of Things' and 'IIoT' as the unifying terms.

Several works aim to create a framework for software architecture descriptions. ISO/IEC 42010 [6] proposes Architecture Descriptions structured by a list of so-called *concerns* being addressed by several *architecture views*. An architecture view is a projection and therefore a simplification, of the abstract architecture in order to describe specific topics. For instance many IIoT reference architectures cover both interoperability and security related aspects. Though there are many inter-dependencies, describing both concerns in one view decreases readability and significantly increases the complexity. In contrast to the general agreement on the classification into views, only a minority explicitly states the regarded concerns and the followed conventions throughout the presented views. Therefore, it must be stated that the proposed structure of ISO 42010 is not followed—a development, which significantly hampers the comprehension of core aspects and limits effective comparisons. Nord et al. [7] further strengthen this fact. They also demand a first-class treatment of stakeholders and their concerns.

Boyes et al. provide taxonomies for the industry sector and its various domains and subdomains [2]. Additionally, the authors create hierarchies for connectivity, characteristics of IT, IIoT devices and user interactions. However, the proposed terms are not connected with the frameworks, which are currently developed. Therefore, the proposed taxonomies can be seen more as parallel activities and less as compliant to the prominent IIoT reference architectures.

A number of surveys on IIoT and related architectures have been published recently. Weyrich and Ebert [8] provide a concise overview of the most relevant frameworks and initiatives. While outlining the main approaches from an industry-based view, an in-depth analysis is missing. Sethi and Sarangi [9] outline a collection of IIoT topics, mentioning key drivers and enabling technologies but lack the link to guidelines how to use those. Even though a short wrap-up on lessons learned is outlined, the important organizational players especially for industrial standardization are not covered.

Zhong et al. outline the key requirements and technologies for Industrie 4.0 applications [10]. They present the relations between IoT-enabled manufacturing, cyber-physical systems, cloud manufacturing and intelligent manufacturing mainly through AI applications. They briefly compare the main efforts from the US, Germany/EU, Japan and China and argue for an agent-based, generic framework covering all previous frameworks. However, they do not present a unifying framework that could fulfill this demand.

Thoben et al. group the developments and discussions in their review mainly according to smart manufacturing and Industrie 4.0. In addition to Reference [10], they also discuss human-machine interaction with a special focus on safety and the prevention of hazards for the involved workers. Furthermore, they draw the conclusion that the description of the "variety of technical standards from various disciplines" [11] requires clear, widely-known reference models. However, the authors only refer to the Reference Architecture Model for Industrie 4.0 but do not make the link to other ones.

Similarly to the previously mentioned reviews, Strange and Zucchella highlight comparable issues and implications as the others—for instance cyber-security and data privacy as new challenges. However, in contrast to the others, Strange and Zucchella examine the IIoT from business-focus view. They emphasize less on the connectivity and interoperability topics but outline the effects on inter-organizational and international cooperations. In this context, they forecast the continuous decentralization of IT networks but also of supply chains and production networks in general. Unfortunately, they also finish their discussions on the thereby created new business-models by pointing to the IIoT reference architectures and do not further elaborate this point [12].

More innovative approaches for security aspects in the IoT domain are presented by Aloqaily et al. The authors show how deep learning can detect intrusion attacks in the highly dynamic area of connected smart vehicles [13]. The gained insights are also transferable to the manufacturing domain as the general setting of high numbers of dynamically interconnected devices is one important characteristic of the IIoT. In a similar direction go Otoum et al. [14]. They outline an hybrid intrusion detection approach using Restricted Boltzman Machines. However, these works focus on very specific security concerns and need to be combined with a set of communication, encryption and authentication mechanisms in order to achieve a sufficient level of end-to-end security.

Visions of new forms of orchestration through Smart Web Services [15] and Virtual Representations [16] promote the introduction of Web concepts into the manufacturing domain. Cooperations between autonomous devices have been analyzed by Kotb et al. [17]. The authors model workflows as Petri-Nets and demonstrate the benefits of cooperative behavior in distributed settings. The sharing of resources and dynamic negotiation of services optimizes the overall performance. Similarily, Al-khafajiy et al. promote a cooperative load-balancing model for fog computing [18]. The gained autonomy in the network and the cooperative aspect hardens the system regarding local overloads and federates the computational requirements among the IIoT network.

While a vast amount of literature examines the necessary technologies and implications for the Industrial Internet of Things, we regard the industrial initiatives as the key players for the actual realization of IIoT concepts. Although the ongoing developments are considered by the respective literature, a comprehensive overview of the relevant frameworks and guidelines is still missing.

3. Methodology for Aligning Reference Architectures

In order to create a comprehensive picture of the IIoT domain, a unifying foundation is necessary. A common way to do so would be to create yet another new framework, aiming to cover all existing

ones. However, the domain itself is highly dynamic and comprises nearly an uncountable amount of different interpretations and views. Consequently, no model or framework can sufficiently capture all aspects. We therefore present a schema and a data model to only structure the amount of information and collect the main perspectives and intentions. This is done through a Linked Data-based knowledge graph. This graph serves as the basis for the later analyses and contains both descriptions of the regarded IIoT frameworks, their layout and characteristics but also shows the various connections and relations between them. These links can be further extended, updated and maintained in future evolvements of the available data.

In order to create the data foundation for the later analysis, the process shown in Figure 1 was created. The collecting and filtering of relevant IIoT frameworks (Section 4 is followed by the iterative identification of IIoT-specific requirements and concerns (Section 3.2), which are then inserted into the knowledge graph. Furthermore, similarities and matches in the structure of the identified reference frameworks are encoded through alignment relations (Section 4.1) between the respective graph nodes. Additional meta-data, such as links to external information sources and annotations including title, short descriptions and references to the original documents are provided. The Linked Data approach supports the native presentation of such information in the form of typed HTTP links and an extendable RDF schema.

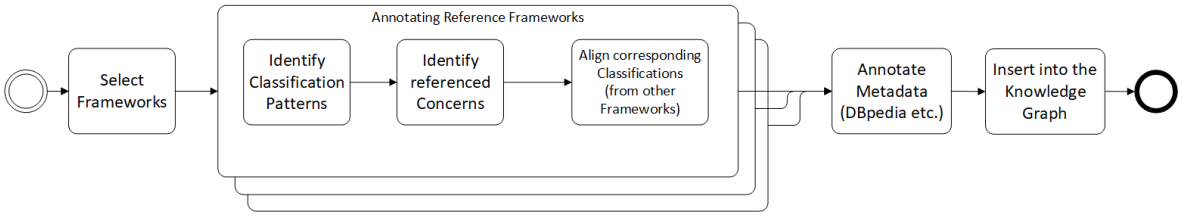

Figure 1. Processing steps to insert reference frameworks into the knowledge graph.

The actual analysis of the collected and integrated information is then conducted using two main visualization patterns. Venn diagrams are used to compare frameworks with each other by plotting their respective coverage of concerns. Thereby, concerns are plotted according to the frameworks referring to them. The intersections contain the concerns targeted by two or more reference frameworks, while the ones on the outside are exclusively mentioned by only one. This comparison method allows the identification of specific scopes but also overlaps between the frameworks. The co-occurrence matrices connect two classes. In this approach they present the connections between the frameworks or—more fain grained—their classifications towards their coverage over all identified concerns. This type of visualization allows the discovery of most suitable frameworks for specific requirements. For instance, a system architect should focus more on the ones having more coverage of security-related concerns if secure data transmission is crucial in his use case. More configurations and plots are available online (https://i40-tools.github.io/StandardOntologyVisualization/).

3.1. Structuring the IIoT Domain

Following the terminology of ISO/IEC 42010 [6], we decided to use three basic categories for IIoT-related entities, namely *concerns*, *frameworks* and *classifications*. A *concern* is a requirement, a challenge or an issue a certain stakeholder can have regarding an IIoT system. As such, both the goals and scope of reference architectures as the intentions of IIoT implementers are regarded as a set of concerns. For instance, a system architect integrating a heterogeneous set of production facilities might be more interested in interoperability and secure communication than aspects of data analytics and AI. *Frameworks* are the actual IIoT reference models. In general, the published guidelines of standardization, industry and community groups present their contributions and proposals according to a supplied model of the domain. This model is usually depicted as a graphical architecture with several layers, perspectives or other building blocks as part of one main document. We put these reference frameworks into the center of our data model. Classifications represent the parts and

sections of IIoT frameworks. Similarly to ISO/IEC 42010, we state that a classification ('viewpoint' in ISO/IEC 42010 terminology) *frames* several concerns, with potential overlaps of framed concerns between different classifications. In contrast to ISO/IEC 42010, we merge viewpoints and the originally separated "view" class to classifications in order to achieve a cleaner data layout (see Figure 2).

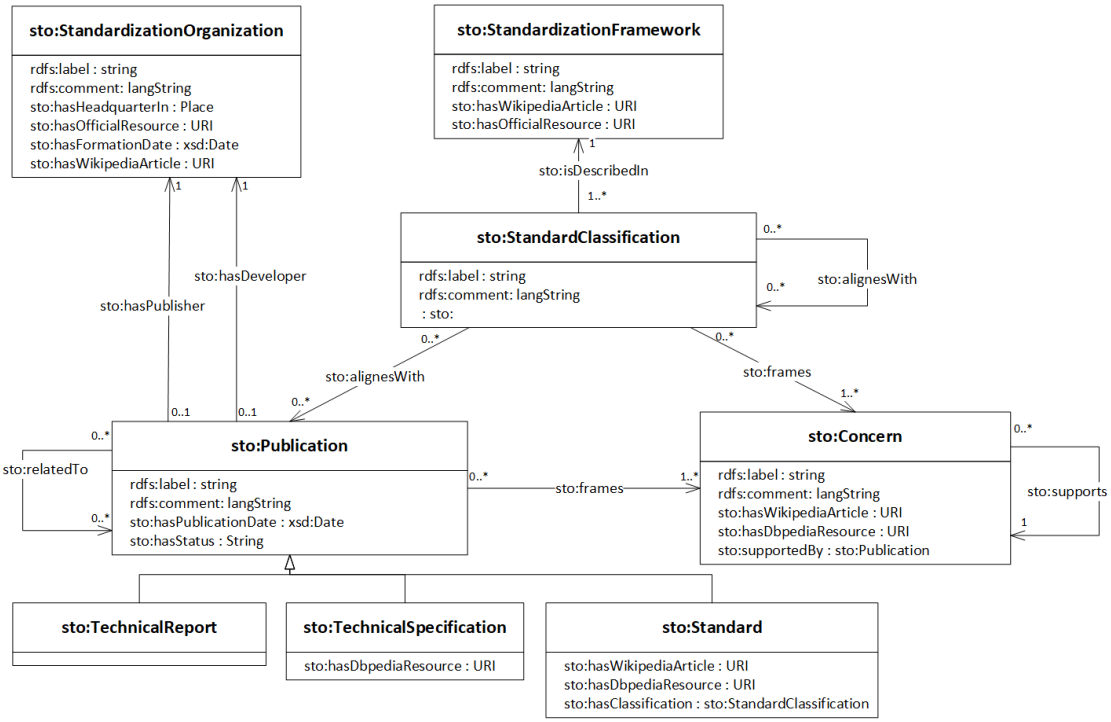

Figure 2. Structure of the IIoT knowledge graph. The original scheme [19] is extended by the set of concerns and architecture frameworks.

Relying on these three categories, a publicly available knowledge graph (accessible at https://i40-tools.github.io/StandardOntology/) was created as an extension of the RDF knowledge graph originally created by Grangel-Gonzalez et al. [19]. Relevant entities are encoded with unique URIs and inserted into the graph as nodes, whereas relations between entities are encoded by typed links, also encoded as HTTP URIs. This approach is a typical way to represent ontologies in the Web and follows the W3C recommendations and conventions for publishing Linked Data [20].

3.2. Considered Concerns

This section briefly outlines the subset of collected concerns, based on Reference [21,22], categorized in a hierarchy with interoperability, trustworthiness and business related concerns as the top level entities. Following ISO/IEC 42010, concerns are the aspects or challenges of an IIoT system that are covered by a certain section of a reference framework. A comprehensive list of relevant concerns allows the identification of blank spaces but also to outline different definitions and scopes of reference frameworks. The hierarchy of concerns creates a taxonomy-like structure. Lower level concerns influence a higher level one in terms of supporting its satisfiability. For instance, having a system with secure communication, this fact indicates a higher level of security and therefore trustworthiness of the system. Modeling such relations explicitly outlines previously intangible connections. Furthermore, formalizing information in the graph enables automated reasoning processes to further populate facts and extend the contained facts. The thereby created network supplies a defined vocabulary, which is used to match the distinct terminology of the various frameworks and to map their assertions. In addition, the formalized relations between the concerns themselves enable the precise assignment of contributions of very specific, lower-level concerns to more general, higher-level ones. To the best of our knowledge, no other work contains a comparable

structure of IIoT concerns and their respective interconnections or applies its structuring of the domain based on a formalized dimensions like ours.

In the following, the most central concerns with a selection of their direct sub-concerns are introduced. *Interoperability* or connectivity is the fundamental building block for enabling IIoT ecosystems (see Figure 3). Two IIoT components are interoperable when they can work together without any restrictions or additional adjustments. In this sense, interoperability contains integration aspects as endpoint descriptions and communication patterns. Therefore, both syntactic and semantic interoperability have to be established. *Syntactic interoperability* characterizes all aspects in order to exchange data, for example, network protocols and data formats. *Semantic interoperability* targets a shared understanding of the meaning of the data, for example, by information models.

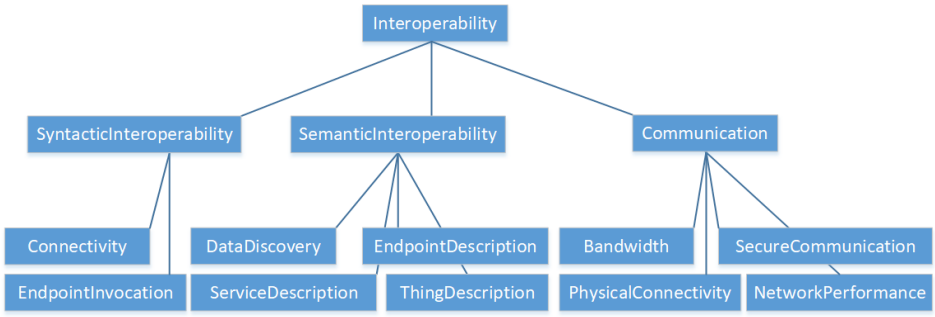

Figure 3. Interoperability-related concerns. Lower level concerns influence the fulfillment degree of higher ones.

Trustworthiness and the highly related *security* of data exchange ecosystems determine the ability to prevent unintended or unauthorized access, change or destruction and therefore behave as expected. *Access control*, *provenance tracking*, *identity management* and *authorization* but also *reliability*, *availability* and *resilience* influence security and are required for a trustworthy system (see Figure 4). Access control frames all methods necessary to ensure data exchange only for entitled parties. Assigning the rights is part of an *authorization* process by defining roles or policies. Provenance tracking denotes any mechanism to document the source of a data object and any kind of transformation or modification. Identity management faces the challenge of supplying unambiguous identifier and mechanisms for third parties to verify an identity claim (authentication). As IIoT also interacts with the physical world, functional *safety*, as a system's ability to prevent physical damage is an important requirement. Any productive IIoT system must have security concerns at its core. Therefore, security related concerns are judged more and more as non-optional but fundamental for any ecosystem.

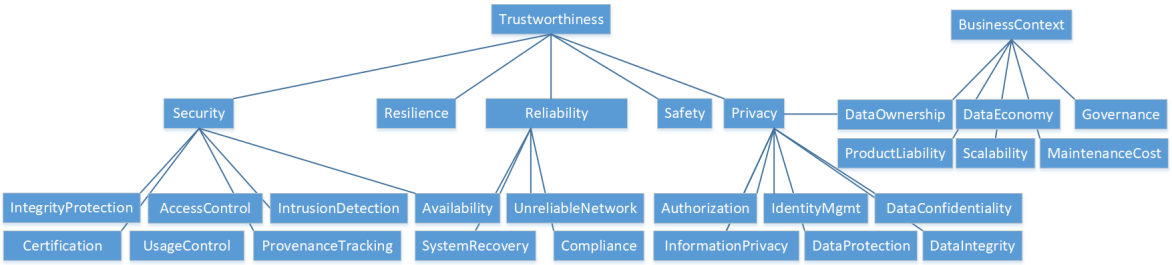

Figure 4. Selected extract of trust- and business-related concerns. Only the first two hierarchy levels are presented.

Business-related concerns outline, for instance, requirements around *data economics* and *governance* and value-adding features. As the IIoT reference frameworks face significant influence from the network and communication communities, technical concerns generally surpass economic considerations in quantity and level of detail. Nevertheless, reliable business models facing actual needs and future economic opportunities are essential building blocks for any reference architecture.

This list gives only a rough impression. In total, 186 concerns have been defined and grouped into a cycle-free, typed hierarchy as an integral axis of the knowledge graph. The complete set of concerns with explanations, their sources and further links to additional web resources is provided as instances of the class *Concern* (see Figure 2).

4. Selecting the Reference Architectures

The selection of noteworthy reference frameworks needs to be based on the interest of the target groups from the industry and research. One way to quantify this interest is based on the number of searches done via internet search engines, mainly Google. The following assumptions underlies the process of determining this interest: (a) Only broadly known reference frameworks are able to create the necessary impact and (b) the interest in the respective framework is more accurately indicated by the name of the publishing organization (for instance 'Industrial Internet Consortium') rather than the name of the reference architecture ('Industrial Internet Reference Architecture'). In particular the second assumption is based on a previously conducted literature search and results in a higher precision. 'Plattform Industrie 4.0', 'Industrial Internet Consortium', 'Industrial Data Space' and 'Industrial Value Chain Initiative' were the seed searches. The other approaches were iteratively added during the literature research and as returned by the named search engines.

Table 1 gives an estimation of the impact on the research community and the overall interest. Google Scholar statistics give a rough impression of the influence based on mentions in research publications. The collected dimensions are reflecting the mentioning of the respective terms in the whole indexed literature and in the papers published from April 2018. In addition, the total amount of citations of the main reference architecture publication have been counted wherever possible. The aggregated rank (Table 1) equally reflects the academic relevance through references and citations, on the one hand and the popularity in the Google Trends list on the other. One can easily recognize that the more industry-driven architectures have significantly less citations but tend to be more popular in terms of web searches.

Table 1. Ranking of selected IIoT reference frameworks ranked by Google Scholar (research relevance) and Google Trends (public interest) appearance.

Framework	All Time References	(Rank)	References Since 2018	(Rank)	Main Publication	Citations	(Rank)	Research Rank	G. Trends Rank	Overall Rank
OpenFog	558,000	(5)	17,600	(5)	[23]	23	(6)	3	2	1
IIC	181,000	(7)	12,300	(7)	[3]	74	(2)	1	7	2
Plattform Industrie 4.0	17,000	(10)	4340	(9)	[24]	57	(3)	5	6	3
IDS	4,480,000	(2)	101,000	(1)	[25]	14	(8)	2	10	4
x-Road	3340	(14)	288	(15)	[26]	46	(4)	10	3	5
FIWARE	2740	(15)	566	(13)	[27]	18	(7)	12	1	5
Industrial Value Chain	4,590,000	(1)	22,100	(3)	[28]	3	(12)	8	8	7
Industrie du Futur	125,000	(8)	5130	(8)	[29]	0	(13)	13	4	8
IoT-Architecture	6680	(11)	2540	(11)	[30]	239	(1)	4	13	8
Open Connectivity Foundation	1,330,000	(4)	19,200	(4)	[31]	9	(9)	6	11	8
BDVA	4,150,000	(3)	32,300	(2)	[32]	4	(11)	7	12	11
Edgecross	5950	(12)	330	(14)	[33]	0	(13)	15	5	12
Arrowhead Framework	37,900	(9)	3490	(10)	[34]	36	(5)	9	13	13
Piano Industria 4.0	5570	(13)	691	(12)	[35]	7	(10)	14	9	14
Alliance of Industrial Internet	291,000	(6)	16,500	(6)	[36]	0	(13)	11	13	15

The combination of the outlined measures indicates the impact and importance of the respective frameworks. The noted overall rank, therefore, supplies a rough impression of the significance of a framework in relation to the other frameworks. The interested user can better estimate the value of the provided specifications in terms of its innovative potential but also the possible community impact. This is especially important in the IIoT domain where only the early detection of new best practices guarantees future-proven and therefore sustainable solutions.

4.1. Reference Architecture Alignment Process

Relying on this knowledge graph, we align the most popular IIoT reference architectures regarding their overlaps and unique features (see Figure 1). We supply a qualitative comparison complemented with configurable visualizations. System architects can use the visualizations to find according proposals related to their problems. Creators of architectures can find corresponding specifications from different initiatives. Decision makers can use the knowledge graph to get overview on covered domains.

We compare the different reference *frameworks* by visualizing the respective concerns of their *classifications* (see Figures 8–10) and the relations (alignments) between them. Therefore, a comprehensive set of relevant and suited concerns needs to be formulated. We reach this list by extracting explicitly stated topics and challenges in the collected reference publications. The core set of concerns is additionally based on the Unified Requirements list collected by the IoT-A project [30], extended by our analysis of the various architecture descriptions and other publications of the IIoT domain in general. While some concerns are essential for most architecture descriptions, like describing interoperability between devices, services and applications, others are only relevant in a specific context, for example, the ability to have clear data provenance across a system architecture or only specified by a single source, for example, the ability to control the transmitting power in wireless networks. A mentioned concern is added to the list if either more than one architecture description specifies its relevance or if it is proposed as a crucial concern by at least one prominent publication. A complete spreadsheet with all concerns, explanations and references is publicly available (https://github.com/sebbader/architecturecomparison/blob/master/IoT-A%20Requirements.xlsx).

Each selected IIoT reference framework was analyzed according to its coverage of each concern. Their mentioned categories are stored as entities of the classification class and annotated with additional meta information. For instance, short textual descriptions, links to their official resources and, if existing, links pointing to DBpedia are added. DBpedia is the open knowledge graph representing the structured information in Wikipedia and plays a central role for the Linked Open Data Cloud (https://lod-cloud.net/). Therefore, additional look-ups and the discovery for further information for all entities is directly provided (see Figure 2).

We link a classification or framework to a concern if there is at least some coverage of the related aspects of the respective concern (lowest common denominator approach). The alignment enables the traversal of links in the graph. Starting from one view, related specifications and definitions can be discovered by following the links to other frameworks with related foci. Classifications with nearly no alignment relations may present an unique perspective on the IIoT whereas highly connected nodes most probably address fundamental and widely regarded topics. Both cases contain valuable insights and are presented in Sections 5 and 7.

The explained relations between the frameworks presented in Section 5 are represented as formal links between the respective classification nodes in the knowledge graph.Classifications with high degrees of incoming or outgoing links indicate a broader coverage, for instance the IIRA Information domain (center) and the RAMI Functional Layer (bottom). More focused and target-oriented classifications, like the IVI Activity View (bottom left) are reflected by less connections. While the interested reader will find more overview information in the higher connected sections, the less-connected entities provide usually more in-depth discussions and guidelines.

5. Considered Reference Architectures

Various organizations have published IoT reference architectures, focusing on different aspects and environments. However, most share a set of implicit assumptions and overlaps. The network layer can be identified as the common ground for any specification, relying on IP-based data exchange (the 'internet' part in IIoT). The differences result from views influenced by different industries, disciplines, challenges and technologies. Consequently, a comprehensive and unified picture on IIoT architectures is still missing. This chapter briefly introduces the major reference architectures and outlines common propositions but also identifies the significant distinctions. In order to gain an effective and comprehensive comparison, the propositions of the Industrial Internet Consortium and the Plattform Industrie 4.0 serve as reference points. Characteristics and distinct features of the other approaches are aligned with both reference architectures where possible.

5.1. Industrial Internet Reference Architecture

The Industrial Internet Reference Architecture (IIRA) published by the IIC aims at a comprehensive model of the industrial internet, independent of specific domains and industries. The wide scope results in a broad coverage of topics whereas concrete implementation guidelines are only partly provided.

The main IIRA categorization is based on the aforementioned ISO/IEC 42010, introducing the four viewpoints Business, Usage, Functional and Implementation. Nevertheless, IIRA lacks an explicit set of addressed concerns. While major concerns can be extracted by analyzing the viewpoint descriptions, a specific allocation of concerns to viewpoints is not given. This results in a certain vagueness of requirements for IIoT implementations. Therefore, various IIoT architectures can be compliant to IIRA requirements while interoperability or data exchange is not possible as a matter of heterogeneous implemented patterns.

IIRA groups its guidelines related to interoperability and data exchange in the Functional Viewpoint, further separated into multiple domains. While the main aspects of IIoT are discussed as parts of the Functional Viewpoint, key aspects like connectivity [37] and security [38] are discussed in separate documents. Figure 5 presents the relations between these central classifications by showing their overlaps of concerns. The Venn diagrams organize the framed concerns regarding the coverage of the certain classifications. The grouping takes place according to the relations as provided by the knowledge graph. Visualizing the data in form of Venn diagrams and co-occurrence matrices (Section 7) hides the complexity of the graph and allows any interested user to directly work with the information. Further views and configurations are possible at the website and available for any user. One can see the extent of the Functional Layer as the key part of the IIRA as it also relates to nearly all concerns from the others. Even though the visualization only supply *quantitative* comparison of concerns, the content is intuitively plotted in order to make it easy to understand. A quantitative presentation means in this context that only the bare number of concerns are compared. The impact and relevance of each single one is explicitly not taken into account. An additional *qualitative* analysis, also regarding the importance of specific concerns, would require a deep understanding of each individual use case and therefore cannot be achieved with a generic approach like presented here. Consequently, the main concepts and most important insights are outlined by the Functional Viewpoint section of the IIRA.

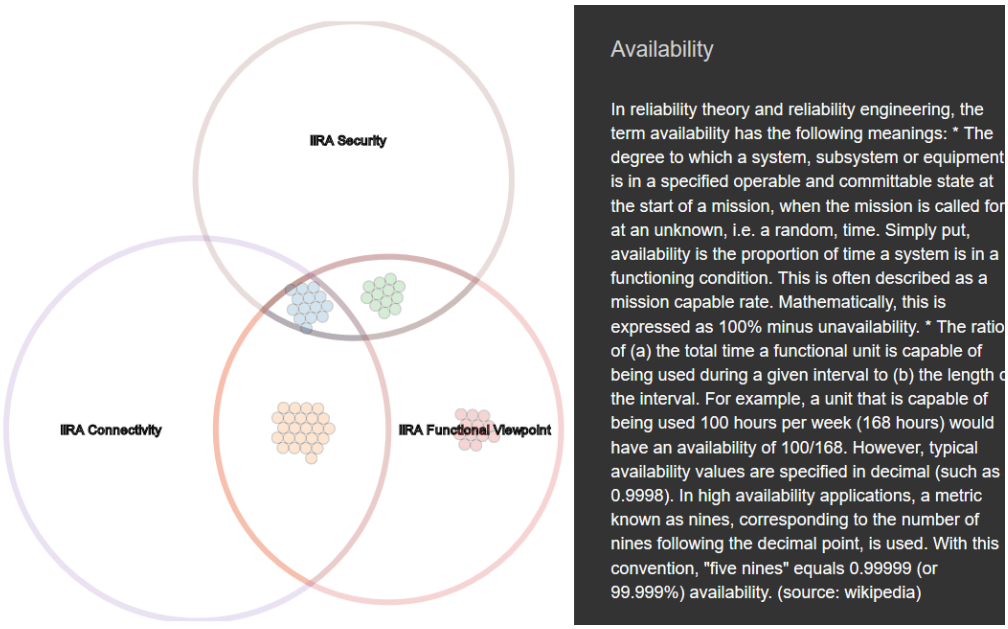

Figure 5. Concerns as framed by the IIRA sections on connectivity and security (http://i40.semantic-interoperability.org/sto-visualization/views/venn_cls_concern.html).

5.2. OpenFog Consortium

The American OpenFog Consortium (https://www.openfogconsortium.org/) targets the area between cloud and edge computing. Fog computing in these terms brings cloud computing capabilities closer to the edge of the network. The OpenFog Reference Architecture [23] is not primarily focused on industrial use cases but also discusses scenarios of smart buildings and interconnected traffic orchestration.

The core principles of their framework are explained according to so-called pillars supporting fog computing, for example security or scalability of fog architectures. The pillars actually depict the concerns of the framework, which are then explained through the viewpoints, views and perspectives of the reference architecture. Similar to the IIRA, the OpenFog Reference Architecture is inspired by ISO/IEC 42010. Noteworthy is also the recently announced merging of the OpenFog Consortium with the IIC, which most probably will lead to a further alignment of the IIRA and the so far developed OpenFog Reference Architecture.

5.3. Reference Architecture Model Industrie 4.0 (RAMI4.0)

The proposed architecture of the German Plattform Industrie 4.0 provides a framework for the interoperability in the manufacturing domain. The focus is on the integration of physical assets from the shop floor with services and applications in the office floor. It serves as a strategic framework highlighting relevant aspects and outlining a common understanding on requirements, dependencies and relations.

The model does not propose detailed technical implementation patterns but outlines according standards for the manufacturing domain, which have been extracted and analyzed in detail by Grangel et al. [19]. The core specification is published as DIN SPEC 91345 [24] and extended towards Linked Data practices [39]. IIC and the Platform Industry 4.0 compared their reference architectures and published the results as a whitepaper [40], therefore a replicating analysis is not conducted as part of this review.

5.4. Industrie du Futur

The French Alliance Industrie du Futur (http://www.industrie-dufutur.org/) aims to develop and define the appearance of the next generation of Franc' production domain. Similar to the Plattform

Industrie 4.0, Alliance Industrie du Futur shall bring industrial, research and governmental actors together. However, despite the aspiration of creating international impact [29], most publications are only available in French. Noteworthy international activities are the collaboration with the German Plattform Industrie 4.0 and the Italian Piano Industria 4.0 in order to align the respective requirements and to define several use cases for all frameworks.

5.5. Piano Industria 4.0

The Piano Industria 4.0 (https://www.mise.gov.it/index.php/it/industria40) is highly influenced by the German Platform Industrie 4.0. As stated before, this initiative is also part of the collaboration between the Alliance Industrie du Futur and the Plattform Industrie 4.0. Analog to its French counterpart, the Piano Industria 4.0 main target group are the national industrial and governmental actors [35], explaining why the vast majority of supplied publications are only written in Italian.

5.6. FIWARE

The FIWARE Foundation promotes an open-source software stack to accomplish interoperability also beyond IoT use cases. The Next Generation Service Interface (NGSI) is a standardized Web API for the IoT restricted to RESTful interactions. Any IoT protocol can be connected by suitable agents or wrappers, providing data towards the Orion Context Broker as the intermediary component for data and command transformation and translation. The currently specified NGSI-LD [41] provides a semantically annotated JSON syntax for context modeling and guidelines to interact with the respective resources.

The FIWARE reference architecture provides documentation for developers and system architects on cloud computing and how Big Data possibly enhances IIoT architectures on the higher network levels instead of regarding physical assets where concepts from for example, RAMI4.0 or IIRA are more detailed. In addition to HTTP serving as the suggested protocol with specified bindings FIWARE defines protocol-agnostic methods and context representations [41].

The strong orientation on HTTP and RESTful interaction patterns at the level of NGSI interfaces and the delivery of software libraries puts its emphasis on the different platform character of FIWARE. Whereas IIRA and RAMI4.0 comprise reference frameworks to categorize IIoT architectures, FIWARE proposes certain patterns and interfaces based on a RESTful integration layer.

As a consequence of the more software-focused view, the architecture directly illustrates certain components and specify necessary interaction patterns. Similar to other IIoT frameworks, IIRA and RAMI4.0 view HTTP as a possible communication protocol among others, whereas FIWARE puts it in the center of its integration and (user) interaction process.

5.7. International Data Space (IDS)

The IDS focuses on secure and trustworthy data exchange patterns in the manufacturing domain. The IDS Reference Architecture Model [25] (IDS-RAM) consists of five layers to establish interoperability and three crosscutting perspectives for reaching its main target, namely to ensure end-to-end data sovereignty of the data owner. The syntactic interoperability is accomplished by the IDS Connectors with their standardized interfaces and exchange protocols.

The Viewpoints of the IIRA map only to a limited extent to the IDS Layer model. The scope of the IDS leads to a stronger focus on configuration, modeling and integration aspects mainly regarded from a system integration point of view. The IIRA scope includes more stakeholders resulting in several ‘Viewpoints’. In general, the aspects of IDS Reference Architecture are mentioned in the IIRA’s Functional Viewpoint. The layers and perspectives of the IDS-RAM can—to some extent—be mapped to the IIRA domains of the mentioned Functional Viewpoint.

RAMI4.0 outlines a comprehensive view of manufacturing related aspects in an IoT landscape. Its focus is on the Asset and its digital representation, the Administration Shell, as its first class citizen. In contrast to that, IDS focuses on the data and data exchange while RAMI4.0 mainly specifies the

integration of shop floor and office related components. Each architecture therefore targets different challenges of industrial IoT. This observation is also presented in Figure 6 where the purple colored concerns depict the issues of physical objects and the description of data entities. Concerns of security, authentication but also deployment of digital components (mainly found in the blue-colored intersection) are less covered. One can also notify that interoperability-related concerns (green) are relevant for the RAMI4.0, the IIRA and the IDS Reference Architecture Model. In addition, RAMI4.0 has a stronger view on physical objects (part of purple) and IDS-RAM on data and usage control (part of brown).

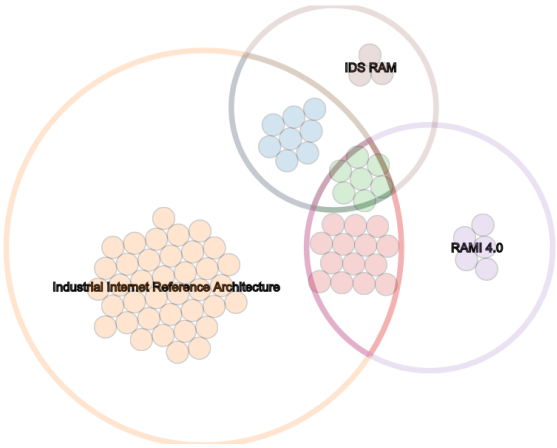

Figure 6. Comparison of RAMI4.0, IDS-RAM and IIRA by considered concerns.

Obvious similarities are the Business and Functional Layers in both reference models. Disregarding the same terminology, IDS and RAMI interpret the meaning differently. In the context of RAMI4.0, the Business Layer contains organizational and economic aspects as monetary conditions and legal regulations. On the other hand, IDS-RAM considers business related aspects, as for example, the role of a participant in the data exchange network.

The Functional Layer in terms of the IDS comprises its core functional requirements and considerations, mainly data sovereignty, trustworthy interactions and supported data exchange. In contrast, RAMI defines its Functional Layer as a view regarding and describing abstract capabilities and *functions* of assets and data workflows.

Network and integration related topics as defined by the RAMI Layers Communication and Integration are combined in the IDS System Layer. The different focus of the IDS considers a suitable communication level through internet standards as a precondition. RAMI, targeting also non-IP-capable devices, defines fine-grained views on connection patterns but also on representing and identifying real-world objects as digital entities. The Asset Layer further strengthens the viewpoint by defining and providing the physical entity. In contrast, a physical object is only regarded by its digital representation in the context of the IDS.

The major differences between both models is the emphasis on the cross cutting perspectives (IDS) and life cycle and hierarchy dimensions (RAMI). In order to enable a cross-organizational data exchange, security, certification and governance are the key consideration at all levels for the IDS. RAMI's focus on the integration of physical objects and manufacturing plants take these aspects for granted. The IDS instead lacks specific life cycle and organizational structures.

5.8. Alliance of Industrial Internet

One part of the Chinese government's program 'Made in China 2025' is the Alliance of Industrial Internet (AII) (http://aii-alliance.org/). While the more prominent announcements about 'Made in China 2025' have drawn attention in international media, the low international interest as shown is Table 1 is remarkable. One reason certainly is the, for instance in comparison with IIC activities,

low visibility of the Alliance of Industrial Internet in English-speaking events and publication channels. However, Reference [36] illustrates the general scope.

Mainly driven by the focus on data-driven interactions at the sensors and actuator level, production data analytics level and the exchange of enterprise data, the AAI reference framework outlines the various necessary communication channels between the next generation of information technology (IT) systems for the office floor and operational technology (OT) systems for the production facilities.

5.9. Internet of Things-Architecture IoT-A

The EU flagship project 'Internet of Things-Architecture' (IoT-A) [30] delivered an unified vision and guidance for transforming existing isolated solutions into an integrated IoT. The outlined Architecture Reference Model presents an extensive list of requirements on many aspects of IoT architectures, allowing a structured categorization of technologies, protocols and best practices according to the defined layers and perspectives. With its focus on achieving interoperability in means of communication and information exchange, the IoT-A Architecture Reference Model serves as major step towards internet-based technical integration of heterogeneous systems.

The IoT-A project aims to pave the way for a common understanding of IoT architectures. The IoT Reference Architecture Model (IoT ARM) provides generic terms and relations [30] for the IoT. Abstract concepts, such as *Phsyical Entities*, *Service* or *Users* provide the foundation for a consistent description of IoT architectures. An additional significant contribution of IoT-A is their list of reference requirements [21] for IoT scenarios. We extended this list and transferred the proposed items into the knowledge graph as concerns.

Although mainly discussing IoT topics and connectivity of physical objects and devices, the insights outlined by IoT-A are highly relevant for both the IDS and any other data-driven integration platform. Figure 7 shows the various overlaps with other frameworks and the big coverage of its architecture. IIRA addresses nearly all concerns also framed by the RAMI4.0 and IoT-A while the later provide more specific and detailed guidelines. Especially the asset and component related suggestions on the lower layers serve as a framework that the IDS further specifies and implements in order to reach a seamless data exchange (see Figure 8). The comprehensive explanations on functional and communication topics by the IoT-A project are extended by the IDS with in deep considerations on data security, privacy and governance. In addition, the IDS defines a more detailed data model and interaction patterns especially for security and authentication procedures. Therefore, the IDS can be regarded as an IoT-A compliant architecture with extended specifications but also concrete implementations for a secure and trustworthy data exchange.

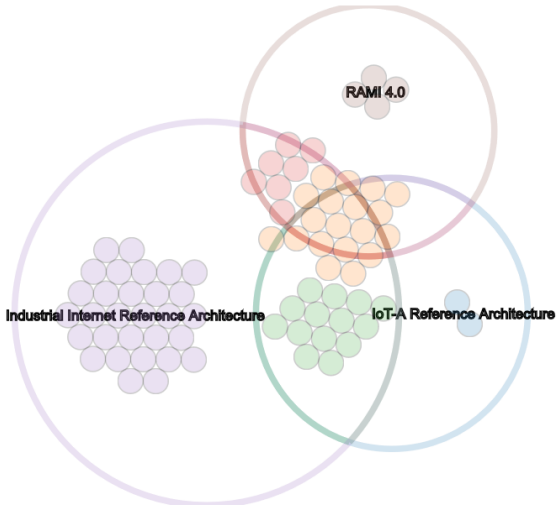

Figure 7. Coverage of IIRA, RAMI4.0 and the IoT-A Reference Architecture.

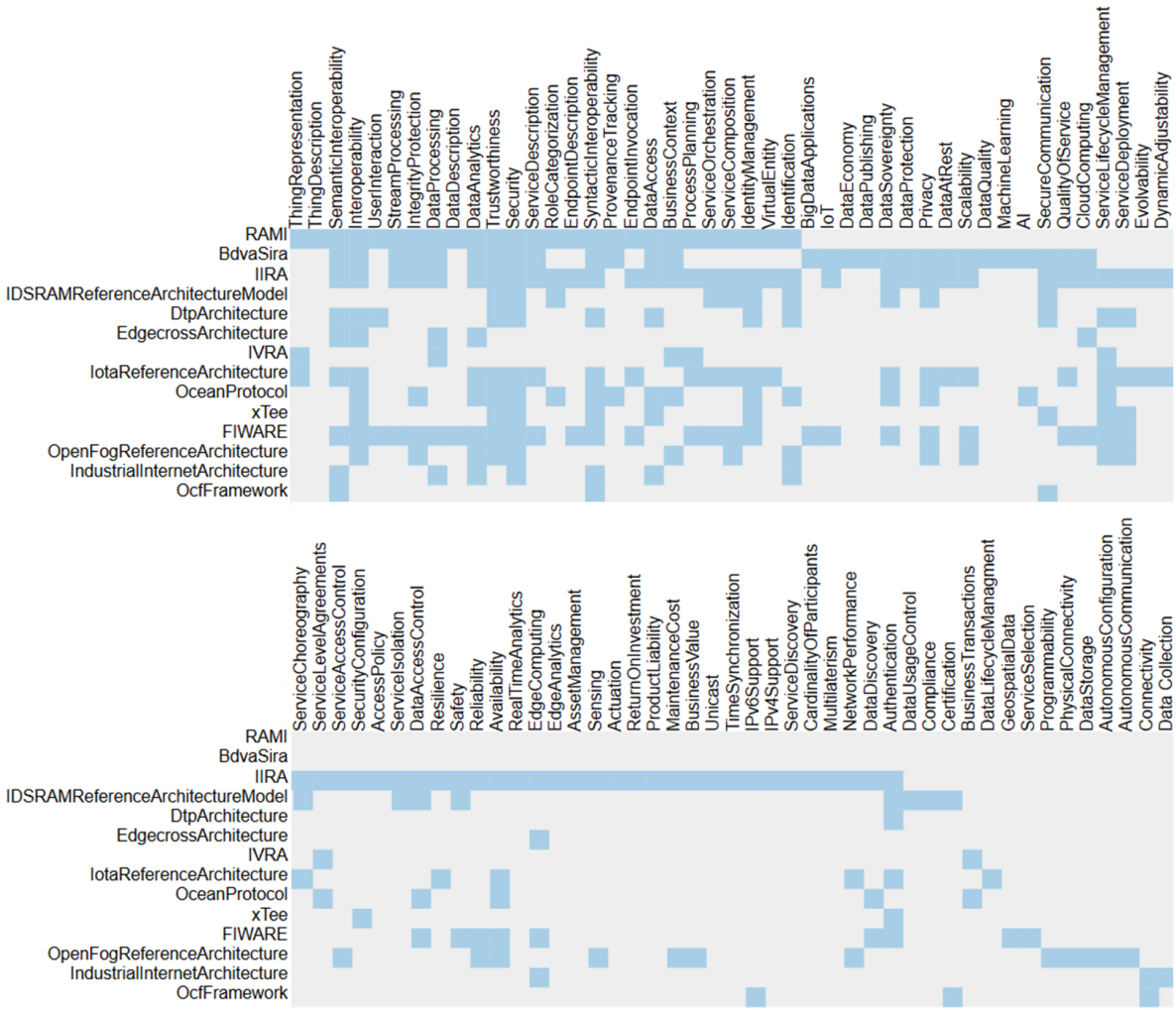

Figure 8. Concerns addressed by the frameworks as a co-occurrence matrix (http://i40.semantic-interoperability.org/sto-visualization/views/matrix_fw_concern.html).

5.10. Big Data Value Strategic Research and Innovation Agenda

The Big Data Value Association (BDVA) aims to provide frameworks and tools for data-driven applications in the context of a European Big Data initiative. As part of the Strategic Research and Innovation Agenda (BDV SRIA), a reference architecture for Big Data applications has been published that also covers some IIoT aspects [32].

Topics in the BDVA reference model are organized according to one vertical and one horizontal dimension. While the later forms a data management stack, the former contains crosscutting aspects and challenges. The mentioned topics and concerns are briefly defined on a business and process oriented level. The target group are decision-makers in companies and politics, therefore technical definitions are limited to the mentioning of according initiatives and organizations.

The big data scope of BDVA leads to a focus on data provisioning, processing and hosting related concerns. Interoperability, security or composition are only mentioned to a limited extend. The BDVA reference model provides a clear and comprehensive overview of concerns at the intersection of big data and cloud platforms. IIoT is one use case among others but not the major focus. In contrast to the other concerns, BDVA specifically distinguishes between static and dynamic data. A comparable view is neither part of RAMI4.0 nor IIRA, even though both discuss the impacts of data streams and stream processing. BDVA goes further and analyzes current gaps and challenges for dynamic data and formulates a list of necessary advancements.

BDVA concerns generally align with higher positioned layers and viewpoints. Data access and device integration are not considered whereas BDVA determines the effects of data volume, variety and velocity on applications, architectures and user interactions.

5.11. Arrowhead Framework

The EU Arrowhead Project (http://www.arrowhead.eu/) started in 2013 and is in the form of the succeeding project Productive4.0 still ongoing. The resulting framework [34] consists, similar to FIWARE, of several central roles (service registry, orchestrator, authorization). The open-source components form a SOA-based architecture in five example domains: Production (process and manufacturing), Smart Buildings and infrastructures, E-Mobility, Energy production and Virtual Markets of Energy.

5.12. Open Connectivity Foundation

The American-based OCF (https://openconnectivity.org/) is an international standardization organization. It strong focus on IoT topics and (industrial) connectivity are explained in the OCF Core Specification [31]. The Core Specification combines the reference nature of for instance the IIRA or RAMI4.0 with detailed specifications up to the structure of URIs. The OCF therefore is less a general overview about IIoT but rather a technical standard for system architects and developers.

5.13. Edgecross

The 2017 founded Japanese Edgecross Consortium [33] proposes guidelines and a reference architecture at the intersection of IIoT and cloud computing. The consortium states that the computation and aggregation of IIoT data needs to be achieved close to the device. Therefore, Edgecross focuses on guidelines and specifications for data processing and aggregation for cloud-based applications, regarded from an IIoT perspective.

The outlined challenges and described strategies target integration and interoperability aspects. Whereas the name ('edge...') raises expectations on computation close to the data source at the edge of the network, the major concerns are data modeling, their validation and the preprocessing of information to higher-level services. The investigations by the Edgecross Consortium outline the relevance of the integration challenge but provide limited further insights how to tackle it, especially as most documents are only available in Japanese.

5.14. Industrial Value Chain

The Industrial Value Chain Initiative (IVI) [28] defines a framework for industrial components and services. Independent Smart Manufacturing Units (SMU) serve as atomic building blocks for further integration and collaboration between the physical world on the one hand and the virtual world on the other. This view on 'things' corresponds to the concept of administration shells as propagated by RAMI4.0 (Asset Layer). In contrast to RAMI4.0, the IVI reference architecture also models the exchange of every resource of interest by Portable Loading Units (PLU). A PLU can contain a physical thing or product but also data and transaction information, therefore creating a general bracket for any transaction in both the physical and the virtual world.

The strong focus on the combined modeling of physical, real-world objects and the activities happening to them underlines the perspective of the Industrial Value Chain. Similar to the Platform Industrie 4.0, the Industrial Value Chain Initiative examines how to connect the various implicit aspects of IIoT into describable and exchangeable SMUs. The proposed considerations concern in particular the industrial purpose of assets (see also RAMI4.0 Business Layer) and rather their virtual characteristics and connectivity mechanisms. In contrast to for example, the Industrial Internet Consortium, data security and interoperability methods are less prioritized in comparison to the modeling and description of processing activities and operations.

The generically defined specifications allow the classification of very heterogeneous settings in terms of IVI, which at the same time implies a limited degree of expressed details. The Industrial Value Chain Reference Architecture aligns therefore mainly with the upper-level layers of other IIoT architectures, for example, the business- and function-related layers and viewpoints. Other frameworks can nevertheless be used to further specify connectivity or security concerns, as for example, the Industrial Data Space or FIWARE.

5.15. X-Road

Estonia's X-Road data exchange framework and the underlying X-tee integration [26] layer are certainly one of the most successful, if not the most successful, data sharing approaches for governance data at the moment. It has become the central infrastructure for information access for nearly the majority of Estonian government services and enables the digital information exchange between the government and its citizen. The target-oriented frameworks like x-Tee define selected, very specific requirements of connectivity (see Figure 8). IIRA covers a broad range of topics while RAMI4.0 focuses more on aspects regarding physical entities ('Things').

The main components are so-called Security Server, which act as gateways between the local databases and the other x-road components. The communication itself utilizes SOAP multipart messages, combining the data payload with security-related metadata. Service endpoints and offered RPC methods are described with WSDL files, supporting the integration process.

X-Road is, in contrast to other outlined approaches, not a fully decentralized environment. Central server provide identity information and enable the maintenance and control of the network as a whole. As its purpose is the exchange of government-related data, controlling the network by an official agency is therefore a strict requirement. At the same time, this characteristics hampers its applicability for other scenarios where equal partners need to communicate. In addition, the technical specifications regarding the used protocols and security roles are rather strict and inflexible, suitable for frequent and stable data exchange but less for ad-hoc communication or automated network configurations. Furthermore, the used set of technologies and description patterns hamper an automated integration and require human developers for providing interoperability and maintenance.

6. Limitations

The modeling of relations between reference frameworks, concerns, technologies and standards in the knowledge graph provides a flexible format for the modeling of the various relevant dimensions and dependencies. Nevertheless, the selected model has several disadvantages. First of all, the presented graph is by its nature incomplete. The amount of publications in the IIoT domain, considering its velocity and variety, do not allow a complete coverage. Therefore, the non-existence of an entity or a link between two entities must not be interpreted as though the two nodes are unrelated. For instance, not having an 'aligendWith' relation between classification A and B does not imply that A and B are not aligned. Nevertheless, the application of the so-called Open World Assumption inherent to ontology-based reasoning allows the application of machine supported knowledge graph completion. The number of explicitly stated facts can thereby automatically increased from more than 15,000 to up to 24,000.

Second, the detailed characteristics of a single relation cannot be presented, that is, there is either a relation or not instead of having, for instance strong and weak relations. For example, a reference architecture such as the IDS views usage control as at its main scope whereas the IIRA merely mentions it. As a matter of readability and simplicity and restricted by the expressiveness of the RDF model, the gradations of this relation and other potentially relevant features are not part of the graph. The knowledge graph model solely allows qualitative statements of relations (relation exists or not). Consequently, a link between two entities states that a relation between these entities exists but says nothing about the nature or degree of this relation. Applying automated logical reasoning, this restriction makes it hard to depict whether one statement 'is stronger' or 'has more support' than

another or which degree of uncertainty is included. Other approaches, in particular property graphs, have aligning capabilities but, in general, lacks the web-based nature of the RDF graph.

Furthermore, the chosen graphical representations are limited to two dimensional relations. While the knowledge graph itself is a highly interconnected and non-planar structure, the visualizations in the form of Venn diagrams and co-occurrence matrices limit the comparisons to a maximum of two dimensions. For instance, frameworks can be plotted in relation to concerns, their classifications or their alignments to other frameworks but not in the same view. Extending the existing plotting options for more-dimensional presentations including more kinds of attributes will increase the amount of information presented to the user.

7. Findings and Best Practices

Two major trends can be identified throughout most of the considered reference architectures. First, nearly all promote cyber-security as one of the key IIoT requirements as the IIoT will disable the isolation of critical infrastructure and devices behind restrictive firewalls or even in separated networks. However, the scope is usually limited to overview descriptions while concrete specifications are missing. For instance, the Security Framework provided by the IIC [38] adopts the categories confidentiality, integrity and availability for a more fine-grained definition of cyber-security. Still, the level of coverage is generally not further examined. We identified additional, more detailed security-affecting concerns. Amongst the previously mentioned, these are certification processes, provenance tracking, network security and process isolation, which have to be regarded at all levels of affected levels. Respective measures need to be outlined starting with embedded devices, over edge/fog/cloud computing, to vast distributed systems. While the reference architectures claim to guide the interested reader, implementation details about using which method or technology at which position of the architecture are generally missing. For instance, security concerns and requirements of IIoT systems regarding a network-wide detection of intrusion attempts for instance outlined by Reference [42]. The unifying approach behind the presented architecture should further promote such best practices in order to reach common patterns and a broader adoption.

Especially regarding security concerns, we identified a considerable demand and effort by the IIoT community. This is reflected in the remarkable amount of security- and trust-related concerns referenced by nearly all frameworks. In addition, the congruent usage of the same terms indicates an already reached common understanding. However, this is contradicted by the low level of detail provided by the considered frameworks. While certain practices have gained wide acceptance in the web-based communities and also new, innovative approaches—like flexible intrusion detection systems for IIoT networks [13] or data usage control in dynamic settings [43]—are available, the majority of IIoT frameworks does not explain which specific recommendations are appropriate in the industrial IoT domain.

The second relevant trend is the repeated reference to a set of core technologies, which have the potential to shape the IIoT. While at the beginning of the IIoT discussions mainly RFID and real-time analytics dominated (for instance in Reference [10,30,36]), later 5G and AI are more prominently presented [11,32,37] as the major developments for IIoT. While the mentioning of these technologies is certainly justified, their actual disruptive impact can only be estimated. Still, the seamless substitution of technology terms indicates an unclear vision of the real requirements and objectives to be met. In particular, it seems that a general shared understanding of the medium layers of the architectures has been established, while the resulting business workflows and the, therefore, necessary applications—being artificial intelligence, big data analytics or even Blockchains—are taken for granted. Moreover, the upper-level layers related to business and usage aspects are less elaborate in order to enable real end-to-end IIoT application networks.

In this direction are also the frequently mentioned Service Level Agreements (SLA) and Quality of Service (QoS) measurements. Reference [44] argues, however, that a Quality of Experience (QoE) approach is more feasible. Ad-hoc vehicular clouds can provide exemplary scenarios for mobile edge

nodes with on-the-fly connections and outline routing algorithms with high-velocity [44]. Quality of Experience has been discussed in various IoT scenarios mainly for smart cities by References [44–46]. New implications regarding the upcoming IoT technologies in smart cities are also reviewed by Lemayian and Al-Turjman [47]. The work outlines the consequences of the emerging IoT and discusses the requirements and implications for the truely connected city.

In addition to the already provided visualized relations between the reference frameworks, several outstanding commonalities can be identified. On the technical implementation level, most reference architectures promote the usage of container-based—mainly Docker—deployment methods. The advantages of having unified modules in the regarded distributed and heterogeneous environments has reached a common agreement. Moreover, the provisioning of APIs following the REST paradigm can be seen as a default baseline for endpoint interaction. While a significant ratio of use cases requires different interaction methods, for instance in event- and streaming-based interactions, RESTful APIs are a central building block of nearly every proposed reference architecture. In particular for automated deployment and configuration tasks of middleware services and the fast connectivity of external components.

Another example for a commonly shared agreement in the used solutions is supported by the repetitive mentioning of certain technologies. In particular, OAuth for authorization, HTTP for basic data exchange and MQTT for publish/subscribe applications present widespread building blocks. For the industrial internet, OPC-UA becomes one of the de facto standards for machine-to-machine communication.

Furthermore, certain areas of interest can be identified. While the IIoT-related architectures extensively describe technical and syntactical integration techniques, the higher-level processes and especially the consuming applications are only roughly described (see Figure 8). Since naturally the focus of IIoT is on the handling of the ‘thing’, the full application stack is able to exploit the potential. Commonly referred analytical services working with artificial intelligence are usually not further enriched with best practices and remain mostly a black box.

One can also notice a difference in the prioritization between the different domains and communities. While the rather IIoT-focused approaches present in detail data security mechanisms, the data exchange approaches provide more details on data privacy and usage control. Aspects concerning connectivity are widely covered and are discussed by nearly every reference architecture. More visualizations supporting this finding are also available at the website. However, the blank spots, for instance the unambiguous description of things, devices and endpoints, are only slightly discussed. While not one single framework needs to cover all of this, references to certain well-defined specifications between the frameworks can express a better overview. Stronger and explicitly stated differentiation to other works will speed up the progress in the field and prevent inefficiencies.

Furthermore, the focus on connectivity and security does not reflect the overall potential of the IIoT. While the industrial community currently examines the interlinking and communication between IoT devices, their implications are only roughly realized. Self-controlled devices, in combination with flexible edge and cloud computing architectures [17,47], need to adjust and act autonomously in order to achieve the necessary scalability and robustness. However, the main target is still the achievement of interoberability between heterogeneous systems rather than a real new design of future IIoT networks. The already existing complexity in terms of device variety, velocity and volume will further increase with the ongoing deployment of more and more connected IIoT systems. Therefore, simply following existing coordination and orchestration patterns for the quickly growing number of digital components will not be sufficient.

An overview on the different scopes and priorities is given in Figure 8. The co-occurrence matrix shows that the more generic concerns, for instance interoperability, security or data analytics, are covered by many frameworks while more specific challenges, like data access and the certification of IIoT systems. The Figures 9–11 show the same content on the level of classifications. This allows the interested reader to quickly gain insights into the available material and to effectively discover

and select the most suited guidelines. All presented views are available on the website and can be configured interactively. The provided graphs are always created at request time and illustrate the latest state of the knowledge graph and its content.

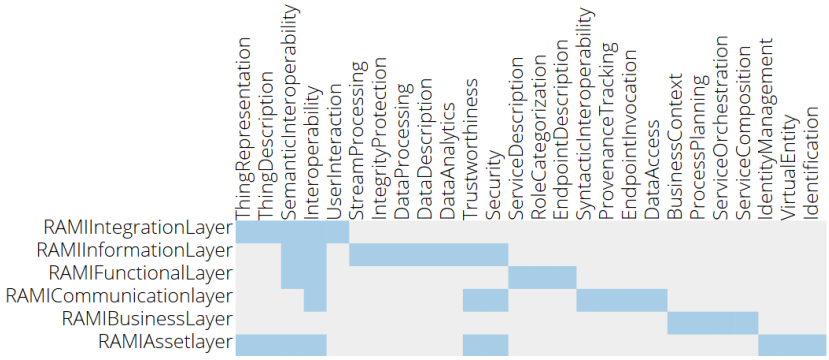

Figure 9. RAMI4.0 Layers with related concerns.

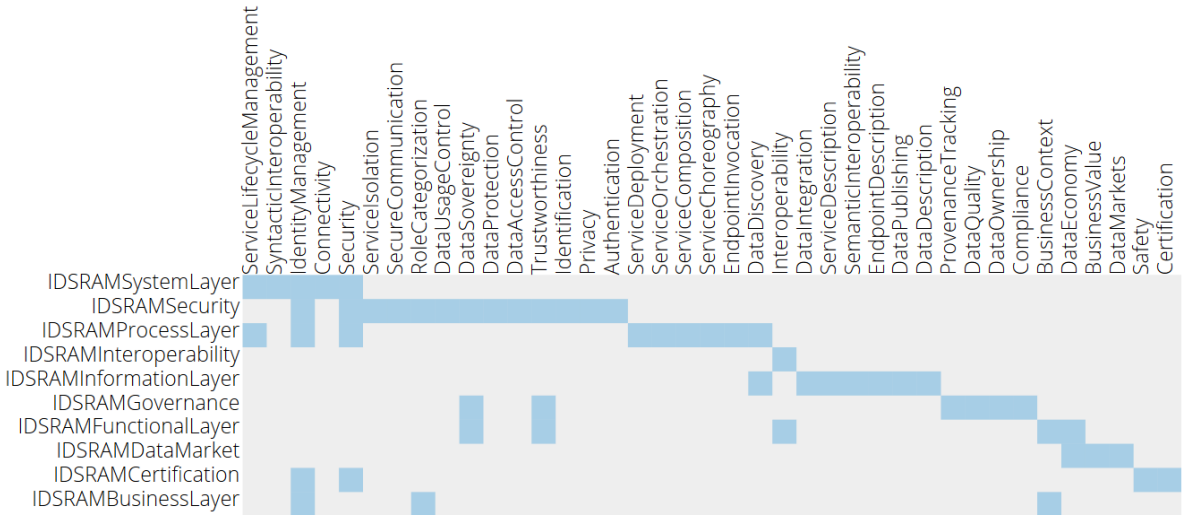

Figure 10. IDS Classifications with related concerns.

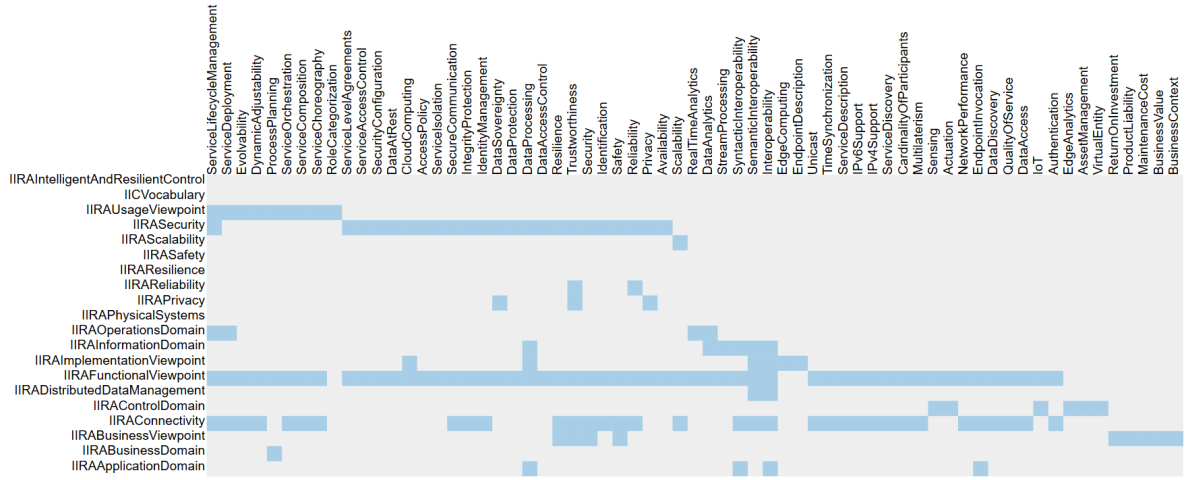

Figure 11. Concerns as referenced by the Industrial Internet Reference Architecture (IIRA).

A major drawback of nearly all outlined specifications is the lack of negative examples in terms of specifications, which scenarios and settings are disregarded. Valuable knowledge can be provided by outlining why certain commonly used paradigms or techniques are perceived as bad practices and

help to gain better insights. Making such intangible assumptions explicit helps the IIoT implementer to better understand the respective scope.

8. Lessons Learned and Outlook

Despite the multitude of works on the topic, there is still no widely adopted scheme for creating and illustrating IIoT reference frameworks. Although the referenced norms in this paper deliver guidelines, the heterogeneity of published architectures both in content but also format is significant. The different presentation patterns, arrangements and terminology hide similar requirements, assumptions and considerations and therefore make it very difficult to grasp a common ground. This work explicitly does not intend to provide yet another (meta-) IIoT framework but instead it aims to increase the applicability of the existing ones.

The currently missing transparency of the various frameworks and standardization activities leads to several, severe drawbacks. The interested reader is hampered in the attempt to understand the respective contributions as the heterogeneous terminology, structures and conventions add unnecessary complexity. Consequently, the introduction of sophisticated techniques and patterns is slowed down. On the other hand, the developer of reference architectures themselves can benefit from a structured and coherent overview on already existing approaches to avoid repeating and therefore ineffective, efforts.

In this paper, we propose a common ground in the form of a hierarchy of IIoT concerns in order to describe, index and interlink the various frameworks. As a matter of fact, the list is and will always be incomplete and not being able to cover all use cases. Nevertheless, explicitly mentioning a regarded subset of concerns at all architecture sections significantly increases transparency and comparability and therefore creates the foundation for achieving further progress. The interested reader is invited to use the interactive web views for his investigation. The provided knowledge graph gives an overview of the current scope of the most popular proposals, enabling the various stakeholders to discover and select reference points more efficiently. Automated reasoning further extends the manually inserted facts by nearly 50%.

In the future, we will further enhance our knowledge graph with more reference frameworks. In addition, we plan to introduce more of the automatically derived relations and formalize axioms for automated reasoning techniques. This will increase the number of links between the entities of the graph and create a better foundation for future analysis. In particular, we want to provide quantifiable measures on the relatedness of reference architectures and automatically propose suitable extensions. Further aspects of this work, which will be taken into account are the priorities and the mutual relations of concerns, for example, security and identity management. The core challenge is still the intuitive presentation of the supplied information and their interconnections. We will further search for better visualization schemes in order to quickly discover relevant insights and to use our approach as an index for IIoT frameworks.

Author Contributions: Conceptualization, S.R.B.; methodology, M.M.; software, S.R.B.; visualization, S.R.B. and S.L.; writing—original draft preparation, S.R.B.; writing—review and editing, M.M. and S.L.

Funding: This research was funded by the German Federal Ministry of Education and Research grant number 01IS17031 and Fraunhofer Cluster of Excellence "Cognitive Internet Technologies" (CCIT).

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

References

1. Muller, G. A Reference Architecture Primer, White paper. 2008. Available online: http://www.gaudisite.nl/ReferenceArchitecturePrimerSlides.pdf (accessed on 8 October 2018).
2. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The Industrial Internet of Things (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [CrossRef]

3. Lin, S.W.; Miller, B.; Durand, J.; Joshi, R.; Didier, P.; Chigani, A.; Torenbeek, R.; Duggal, D.; Martin, R.; Bleakley, G.; et al. Industrial Internet Reference Architecture. Industrial Internet Consortium (IIC), Tech. Rep. 2015. Available online: https://www.iiconsortium.org/IIRA.htm (accessed on 14 December 2018).
4. Hermann, M.; Pentek, T.; Otto, B. Design Principles for Industrie 4.0 Scenarios. In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; IEEE Computer Society: Washington, DC, USA, 2016; pp. 3928–3937.
5. Baheti, R.; Gill, H. Cyber-physical Systems. *Impact Control Technol.* **2011**, *12*, 161–166. Available online: http://www.gaudisite.nl/ReferenceArchitecturePrimerSlides.pdf (accessed on 8 October 2018).
6. IEEE: ISO/IEC/IEEE 42010: 2011-Systems and Software Engineering—Architecture Description. Technical Report. 2011. Available online: https://www.iso.org/standard/50508.html (accessed on 5 July 2018).
7. Nord, R.L.; Clements, P.C.; Emery, D.; Hilliard, R. Reviewing architecture documents using question sets. In Proceedings of the 2009 Joint Working IEEE/IFIP Conference on Software Architecture & European Conference on Software Architecture, Cambridge, UK, 14–17 September 2009; pp. 325–328.
8. Weyrich, M.; Ebert, C. Reference Architectures for the Internet of Things. *IEEE Softw.* **2016**, *33*, 112–116. [CrossRef]
9. Sethi, P.; Sarangi, S.R. Internet of Things: Architectures, Protocols, and Applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 1–25. Available online: https://www.hindawi.com/journals/jece/2017/9324035/ (accessed on 1 October 2018). [CrossRef]
10. Zhong, R.Y.; Xu, X.; Klotz, E.; Newman, S.T. Intelligent Manufacturing in the Context of Industry 4.0: A Review. *Engineering* **2017**, *3*, 616–630. [CrossRef]
11. Thoben, K.D.; Wiesner, S.; Wuest, T. "Industrie 4.0" and Smart Manufacturing—A Review of Research Issues and Application Examples. *Int. J. Autom. Technol.* **2017**, *11*, 4–16. [CrossRef]
12. Strange, R.; Zucchella, A. Industry 4.0, global value chains and international business. *Multinatl. Bus. Rev.* **2017**, *25*, 174–184. [CrossRef]
13. Aloqaily, M.; Otoum, S.; Al Ridhawi, I.; Jararweh, Y. An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Netw.* **2019**, *90*, 101842. [CrossRef]
14. Otoum, S.; Kantarci, B.; Mouftah, H.T. On the Feasibility of Deep Learning in Sensor Network Intrusion Detection. *IEEE Netw. Lett.* **2019**, *1*, 68–71. [CrossRef]
15. Maleshkova, M.; Philipp, P.; Sure-Vetter, Y.; Studer, R. Smart Web Services (SmartWS)—The Future of Services on the Web. *IPSI BgD Trans. Adv. Res.* **2016**, *12*, 15–27.
16. Bader, S.R.; Maleshkova, M. Virtual Representations for an iterative IoT Deployment. In Proceedings of the Ninth International Workshop on Web APIs and Service Architecture, Lyon, France, 23–27 April 2018; pp. 1887–1892.
17. Kotb, Y.; Al Ridhawi, I.; Aloqaily, M.; Baker, T.; Jararweh, Y.; Tawfik, H. Cloud-Based Multi-Agent Cooperation for IoT Devices Using Workflow-Nets. *J. Grid Comput.* **2019**, 1–26. [CrossRef]
18. Al-khafajiy, M.; Baker, T.; Al-Libawy, H.; Maamar, Z.; Aloqaily, M.; Jararweh, Y. Improving Fog Computing Performance via Fog-2-Fog Collaboration. *Future Gener. Comput. Syst.* **2019**, *100*, 266–280. [CrossRef]
19. Grangel-Gonzalez, I.; Baptista, P.; Halilaj, L.; Lohmann, S.; Vidal, M.E.; Mader, C.; Auer, S. The Industry 4.0 Standards Landscape from a semantic Integration Perspective. In Proceedings of the 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus, 12–15 September 2017; pp. 1–8.
20. Heath, T.; Bizer, C. *Linked Data: Evolving the Web into a Global Data Space*; Synthesis Lectures on the Semantic Web: Theory and Technology; Morgan & Claypool: San Rafael, CA, USA, 2011; Volume 1, pp. 1–136.
21. IoT-A. IoT-A Unified Requirements List. 2016. Available online: https://web.archive.org/web/20160322053934/http://www.iot-a.eu/public/requirements (accessed on 25 September 2018).
22. Yaqoob, I.; Ahmed, E.; Hashem, I.A.T.; Ahmed, A.I.A.; Gani, A.; Imran, M.; Guizani, M. Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. *IEEE Wirel. Commun.* **2017**, *24*, 10–16. [CrossRef]
23. OpenFog Consortium Architecture Working Group. Openfog Architecture Overview. *White Paper OPFWP001* **2016**, *216*, 35. Available online: https://www.openfogconsortium.org/ra/ (accessed on 5 December 2018).
24. Adolphs, P.; Berlik, S.; Dorst, W.; Friedrich, J.; Gericke, C.; Hankel, M.; Heidel, R.; Hoffmeister, M.; Mosch, C.; Pichler, R.; et al. DIN SPEC 91345: Reference Architecture Model Industrie 4.0. *DIN SPEC* **2016**, *4*. Available online: https://webstore.ansi.org/Standards/DIN/DINSPEC913452016 (accessed on 13 November 2018).

25. Otto, B.; Lohmann, S.; Auer, S.; Brost, G.; Cirullies, J.; Eitel, A.; Ernst, T.; Haas, C.; Huber, M.; Jung, C.; et al. *Reference Architecture Model for the Industrial Data Space*; Fraunhofer-Gesellschaft: Munich, Germany, 2017.
26. Freudenthal, M.; Hanson, V.; Nõgisto, I.; Kromonov, I.; Annuk, S. X-Road Architecture. Cybernetica. 2015. Available online: https://www.ria.ee/riigiarhitektuur/wiki/lib/exe/fetch.php?media=an:x-tee_kohtumised:arc-g_x-road_arhitecture_1.2_y-879-3.docx&usg=AOvVaw3fhwi5k_UEfnpBMsjJov5V (accessed on 5 October 2018).
27. Glikson, A. Fi-ware: Core Platform for Future Internet Applications. In Proceedings of the 4th Annual International Conference on Systems and Storage, Haifa, Israel, 30 May–1 June 2011 .
28. Industrial Value Chain Initiative. Industrial Value Chain Reference Architecture (IVRA). 2016. Available online: https://iv-i.org/wp-test/wp-content/uploads/2017/09/doc_161208_Industrial_Value_Chain_Reference_Architecture.pdf (accessed on 8 October 2018).
29. Faure, P.; Darmayan, P. Le plan français Industrie du futur. *Annales des Mines Réalités Industrielles* **2016**, *2016*, 57–60.
30. Bassi, A.; Bauer, M.; Fiedler, M.; Kramp, T.; Kranenburg, R.V.; Lange, S.; Meissner, S. *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*; Springer: Heidelberg, Germany, 2013.
31. Park, S. OCF: A new open IoT consortium. In Proceedings of the 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, 27–29 March 2017; pp. 356–359.
32. Big Data Value Association. European Big Data Value Strategic Research and Innovation Agenda. 2017. Available online: http://www.bdva.eu/SRIA (accessed on 23 September 2018).
33. Edgecross Consortium. Edgecross Consortium to Address Edge Integration in IIoT-enabled Architectures. 2018. Available online: https://www.edgecross.org/ja/data-download/pdf/Edgecross_Consortium_WP(E).pdf (accessed on 29 September 2018).
34. Delsing, J. *IoT Automation: Arrowhead Framework*; CRC Press: Boca Raton, FL, USA, 2017.
35. Tiraboschi, M.; Seghezzi, F. Il Piano nazionale Industria 4.0: una lettura lavoristica. *Lab. Law Issues* **2016**, *2*, 1–41.
36. Alliance of Industrial Internet. Industrial Internet Architecture, White Paper. 2016. Available online: http://en.aii-alliance.org/uploadfile/2017/0307/Industrial.pdf (accessed on 29 March 2019).
37. Joshi, R.; Didier, P.; Jimenez, J.; Carey, T. The Industrial Internet of Things Volume G5: Connectivity Framework. IIC. 2018. Available online: https://www.iiconsortium.org/IICF.htm (accessed on 2 August 2018).
38. Schrecker, S.; Soroush, H.; Molina, J.; LeBlanc, J.; Hirsch, F.; Buchheit, M.; Ginter, A.; Martin, R.; Banavara, H.; Eswarahally, S.; et al. Industrial Internet of Things Volume G4: Security Framework. IIC. 2016. Available online: https://www.iiconsortium.org/IISF.htm (accessed on 2 August 2018).
39. Bader, S.R.; Maleshkova, M. The Semantic Asset Administration Shell. In Proceedings of the 15th International Conference on Semantic Systems, Crete, Greece, 3–7 June 2018.
40. Lin, S.W.; Murphy, B.; Clauer, E.; Loewen, U.; Neubert, R.; Bachmann, G.; Pai, M.; Hankel, M. Architecture Alignment and Interoperability—An Industrial Internet Consortium and Plattform Industrie 4.0 Joint Whitepaper. 2017. Available online: https://www.iiconsortium.org/pdf/JTG2_Whitepaper_final_20171205.pdf (accessed on 24 July 2018).
41. Fonseca, J.; Guillemin, P.; Bauer, M.; Frost, L.; Privat, G.; Abbas, A.; Li, W.; Fernández, D.; Fisher, M.; Wright, A.; et al. *Context Information Management (CIM); NGSI-LD API*; ETSI: Valbonne, France, 2018.
42. Sadeghi, A.R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In Proceedings of the 52nd Annual Design Automation Conference—DAC '15, San Francisco, CA, USA, 7–11 June 2015; pp. 1–6.
43. Schütte, J.; Brost, G.S. A data usage control system using dynamic taint tracking. In Proceedings of the 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland, 23–25 March 2016; pp. 909–916.
44. Cao, Y.; Chen, Y. QoE-based node selection strategy for edge computing enabled Internet-of-Vehicles (EC-IoV). In Proceedings of the Visual Communications and Image Processing (VCIP), St. Petersburg, FL, USA, 10–13 December 2017; pp. 1–4.
45. Otoum, S.; Kantarci, B.; Mouftah, H.T. Mitigating False Negative intruder decisions in WSN-based Smart Grid monitoring. In Proceedings of the 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 153–158.

46. Huang, X.; Xie, K.; Leng, S.; Yuan, T.; Ma, M. Improving Quality of Experience in multimedia Internet of Things leveraging machine learning on big data. *Future Gener. Comput. Syst.* **2018**, *86*, 1413–1423. [CrossRef]
47. Lemayian, J.P.; Al-Turjman, F. Intelligent IoT Communication in Smart Environments: An Overview. In *Artificial Intelligence in IoT*; Springer: Cham, Switzerland, 2019; pp. 207–221.

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).