YEARBOOK OF UNWE (2021), PUBLISHING HOUSE – UNWE
ISSN (print): 1312-5486; ISSN (online): 2534-8949; http://unwe-yearbook.org/en/
DOI: https://doi.org/10.37075/YB.2021.2.07

A CONCEPTUAL APPROACH FOR INDUSTRIAL INTERNET OF THINGS ASSESSMENT

Luben Boyanov[1]
e-mail: lboyanov@unwe.bg

Abstract

The Industrial Internet of Things (IIoT) is a new paradigm that fundamentally changes the current patterns and activities in industry. The new Digital revolution transforms all sectors of human activities and production. IIoT has numerous architectural, business, technological, social and consumer perspectives. This paper looks at some reference architectures, connectivity issues, business aspects and security topics of IIoT. Those domains are looked at with their most important subdomains into a framework that can allow an architect or end user to make a quantitative assessment of a IIoT. The proposed approach uses expert evaluation of the main domains and subdomains from a reference IIoT architecture, which are then used to obtain an overall IIoT assessment.

Key words: Industrial Internet of Things, reference architectures, connectivity, assessment methodology, security

JEL: C69, O32, L63, L86

Introduction

Internet of Things (IoT) is a modern paradigm that describes the connection of almost every "thing" to Internet. IoT looks not only in the way of connecting RFIDs, sensors and other objects to the global digital network but also the effects and outcomes of those connections. The model allows for the measurement of physical values such as temperature, humidity, pressure, etc. form sensors and tags attached to goods, vehicles, even to living beings. Objects, things and connected devices become "smart" providing new functions and utilities. Areas of human activities involved in this lead to the creation of smart industry, smart agriculture, smart healthcare, finance, transport, logistics, education, environment, power supply, etc. The big variety of objects and activities creates huge opportunities for new applications and approaches to make people's lives easier and more effective. Costs, resources and waste are reduced by improving efficiency. Deliveries are perfected, services to end users are accelerated, with an improved visibility of the product chain from the factory to the recipient. Industry is part of this revolutionary world phenomenon of "things", having its own terminology

[1] Assoc. Prof., PhD, Information Technologies and Communications Department, Applied Informatics and Statistics Faculty, University of National and World Economy

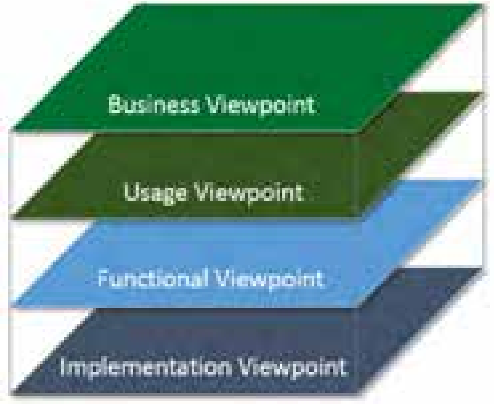
and pillars – Industry 4.0 and Industrial IoT (IIoT). One of the key concepts in Industry 4.0 is connectivity – it enables manufacturing to be ‘smart’. The new paradigm helps the production process in industrial environments and supports the improvement of planned preventive machine maintenance. The high-tech strategy Industry 4.0 has been proposed and shaped by the German government (Federal Ministry for Economic Affairs and Energy of Germany, 2021). Industry 4.0 plays an important role for many industries, organizations and governments that have adopted its main directions. The framework, proposed by the German ministry looks at important areas, in addition to the connectivity of RFIDs and sensors – it raises challenges related to energy efficiency, real-time productivity, coexistence, interoperability, security and privacy (Sisinni et al., 2018). The focus of Industry 4.0 is on the optimization of industrial processes through intelligent devices and data-driven analytics. Digitalization and advanced IT products in Industry 4.0 and IIoT are used for data-driven solutions. The mass connectivity of industrial machines, robots and devices, and the continuous transmission and collection of data from them are used to both increase efficiency and enhance security – two of the key tasks and requirements in IIoT and Industry 4.0.

IIoT is a very broad topic – not only because it covers a wide variety of industries (many of them having nothing in common), but also because each industry has numerous sectors with big variations amongst them. There have been a number of initiatives, concepts, approaches and structures related to IIoT. Reference architectures, connectivity, business view, analytics and security are all important with numerous implementation options and hurdles for their adoption. We look at those five topics and propose a methodology for an overall IIoT assessment.

Reference architectures

The term reference architecture (RA) is about defining a prototype approach and using common terms within a certain domain of activities/products. Essentially, an RA is a set of patterns, or one defined architectural model, for use in business and technical contexts. In industry, the development of standards, approaches and models is of great importance. With the implementation of Industry 4.0 and the use of IoT, the reference model for the Industrial Internet of Things is becoming increasingly important. As some authors argue: “The big need for reference architectures in industry has become tangible with the fast-growing number of initiatives working toward standardized architectures. These initiatives aim to facilitate interoperability, simplify development, and ease implementation” (Weyrich and Ebert, 2016, p. 113).

The Industrial Internet Reference Architecture (IIRA) is both an architectural approach and a standards-based methodology (Industrial Internet Consortium, 2021). Using the IIRA model and approach, system architects can create their products that follow the set frameworks and concepts. An important point here is that the developers can use the same RA in various IIoT implementations. IIRA was created in 2014, as a result of the efforts of experts and representatives from AT&T, Cisco, General Electric, IBM, and Intel, aiming support of Industrial IoT applications. An important aspect of IIRA is that it defines business, usage, functional and implementation points of view – Figure 1. Thus IIRA follows business goals, vision and recommendations. IIRA integrates the links between different perspectives – in addition to the business one, it also considers the scope of an application and the system life cycle process. The latter varies and should be tailored to each industrial sector.

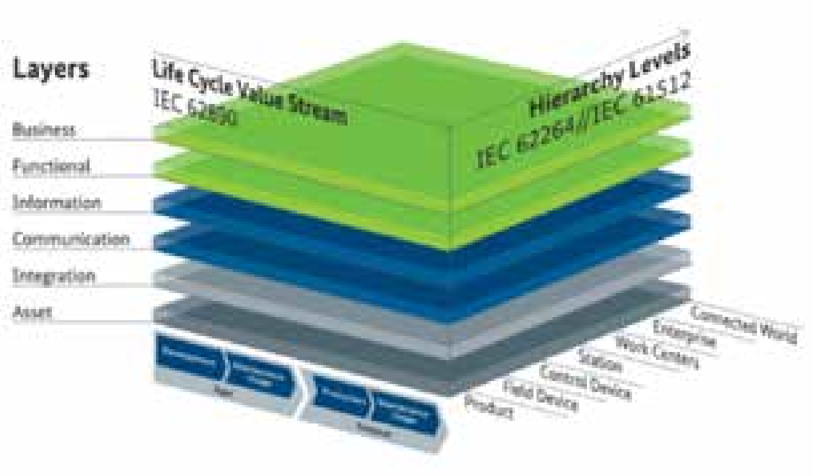


Source: Industrial Internet Consortium (2021).

Figure 1: IIRA viewpoints

Another Industrial RA is the Reference Architectural Model Industry 4.0 (RAMI 4.0) (Lydon, 2021)

This service-oriented architecture supports the digital transformation of present manufacturing. It unifies the elements and technology components into a layered, lifecycle model. RAMI 4.0 transforms complex processes into easy-to-understand sets. The latter include topics like data privacy and IT security. The model is viewed as 3D and factory is the first dimension. The second one is the product lifecycle. The third is the architecture. The architectural layers: business, functional, information, communication, integration and asset are given in Figure 2.



Source: Lydon (2021).

Figure 2: RAMI 4.0.

Another service-oriented architecture is the Arrowhead framework (Arrowhead, 2017). It has been developed in the framework of an EU research project on IoT automation. This architecture is based on local automation tools in five industrial domains – manufacturing (production, processes and energy), smart buildings and infrastructures, electro-mobility, energy production and virtual energy markets.

Other existing reference IIoT architectures are IDS (IDS RAM, 2021), OpenFog (OpenFog Consortium, 2017) and more, related to testing, benchmarking, middleware and services, smart factories, etc. A well-structured analysis of existing reference frameworks and their classifications is given in (Bader et al., 2019). Our work is based on the main topics in IIRA – business, connectivity, security and analysis.

Business topics

The IIoT business context refers to the opportunities through which business is advanced and innovations created. Consideration of the market context, strategies, business models and ways of evaluating business cases are of great importance to the IIoT. They determine the technologies and capabilities for creating and developing new industrial and consumer products. IIoT solutions have a tremendous potential to increase the diversity of business channels for enterprises, create more opportunities for customers, and achieve meaningful societal benefits.

Market Context

The changes to existing business models brought about by the IIoT, create numerous new opportunities in all markets. It is very important for enterprises to innovate and make their business strategies and operating models more efficient, in order to remain competitive in national, regional and global markets.

Strategy

Businesses must also define their strategies and goals within IIoT. This can provide clarity on the speed of transformation, the balance of risks associated with the market and the risks associated with the speed of product innovations. In creating effective IIoT strategies, it is important to create alliances and business partnerships. Many enterprises create and follow plans for the production of various IIoT applications. This requires defining and clarifying initiatives and also drafting documents like application roadmaps and budgets.

Business model innovation

During the periods of transformation with IIoT, business models need to comply with existing internal elements. Transformations should include all new opportunities. IIoT affects not only operations but also product creation, marketing, increased customer value – the entire business value chain. Adaptation of business models is of utmost importance to achieving the goals of an enterprise.

Best practices and platforms

The IIoT concepts are new and different from previous enterprise activities. They could introduce or extend initiatives that follow best practices and platforms in the IIoT field. This could be done with an internal Centre of excellence using the help of experts to guidance in modern activities. Such Center of excellence can be useful for many companies. A unified IIoT strategy can be created and managed within an organization. This also provides the opportunity to effectively share best practices and platforms across the organization.

Connectivity

The concept of a smart industrial environment, where sensors efficiently transmit data, using communication technologies such as WiFi, BLE, ZigBEE and 5G, allows dynamic and adaptable to changing circumstances data collection. The seven layer OSI model and the four layer Internet TCP/IP model do not correspond to all IIoT requirements for industrial device connectivity. There is a requirement for special attention to industrial sensors, controllers, gateways and communication devices. IIRA proposes a five layer connectivity stack model for IIoT, with layers (from bottom – up) – physical, link, network, transport and framework.

Connectivity standards

Connectivity technologies in the IIoT have to integrate with existing communications. The choice of a connectivity standard should allow present technologies to be integrated within an application area. Most commonly, a connectivity standard is typically created with specific functionality in mind. Gateways are used to connect different technologies as well as to connect a certain domain to others. Examples of connectivity standards used in the IIoT are LPWAN, NB-IoT, LTE-M, 5G, Wi-Fi 6, and Bluetooth 5.

Connectivity functions

The most important connectivity functions include: data resource model; publish-subscribe and request-reply data exchange patterns; data quality of service; data security, and programming API. Other communication issues and functions to be considered are: data resource model; addressing; data type; data resource lifecycle and exception handling.

Transport layer

Transport layer considerations include endpoint addressing (the messaging protocol), modes of communication (unicast, multicast and broadcast), connectedness (connection-oriented or connectionless), prioritization (critical or non-critical data), timing and synchronization (NTP- or PTP-based time, GPS clocks), topology, span and segmentation.

Connectivity framework

Connectivity framework standards include Data distribution service (DDS), Hypertext Transfer Protocol (HTTP); OPC Unified Architecture; oneM2M; Constrained Application Protocol (CoAP); MQTT; well-known fieldbus protocols like Profibus (Profinet), EtherNet/IP, Modbus & Modbus/TCP, HART & HART wireless.

Security

The key security features of IIoT are safety, security, resilience, risk management, monitoring, configuration and management. These topics are considered of high importance for an IIoT in order to build a proper degree of trust in an industrial system. The interrelationship between safety, security, robustness and reliability are a prerequisite for the reliable operation of the employed system.

Safety

Safety is considered a state of the IIoT system, and includes safety assessment techniques. This property should perform security analysis of threats and examine what capabilities are available for its enhancement.

Security

This feature concerns the protection of the system from inadvertent or unauthorized access, modification or destruction. Security defines the degree of protected behaviour and refers to the elements responsible for the security of information and its system assets.

Resilience

This feature refers to the system design, which must be completed in a way that failures do not occur at the same time.

Risk management

Risk is about the uncertainty related to objects and intentions that looks at the likelihood of an event, occurring together with the impact of that event. Risk management can be viewed as Risk avoidance, Risk mitigation, Risk transferal, Risk acceptance and Residual risk.

Security monitoring, configuration and management

Security monitoring is accountable for capturing data with regard to the overall state of the system – from its endpoints to the connectivity traffic. Security configuration and management are responsible for the control of changes to both operational functionality of the system (including reliability and safety behaviour) and security controls that ensures its protection.

Analytics

Analytics is the ultimate goal in the quest for making processes and products better and more efficient for each business and industry. It leads to new insights and intelligence that are able to improve a lot decision-making for the product-creation. Analytics can further enhance the intelligence of operations, which in turn can improve the transformation of major business outcomes and social values.

Business Usage

Business analytics aims at creating business value. The process identifies performance bottlenecks at various stages in order to remove them. This is done by using analytical strategies, system's operational states, identifying performance and assessing the environment. Analytics also intends to identify and examine emerging information patterns. It assesses industrial systems under varied conditions.

Implementation

The implementation is concerned with the technologies which are used to implement the functionality of a product or process. It also realizes connectivity schemes and lifespan management.

Big Data

Big data has the objective to provide input to analytics in IIoT systems in regard to operation optimization, malfunctioning and preventive processes. Big data comes from various sources – sensors, RFIDs, legacy databases, websites, historical records, etc. The big data analytics platform must address and maintain the processing of input data from all possible sources.

Artificial Intelligence

Artificial Intelligence (AI) can increase the performance of IIoT systems. Machine learning (ML), which is a subset of AI, can enable organizations to gather a big number of insights in an industrial process or product. Using either structured or unstructured data, ML can extract better value from existing data compared to traditional business intelligence solutions. Using AI tools, machines and programs can be "trained" with big data. Then they can use tools/programs that have "learned" in order to overcome situations, unexpected conditions or even make predictions.

Methods and Modelling

Analytics can be of a streaming or batch type. Streaming analytics is performed in real or almost real time for the flow of data. This kind of analytics must be fast and have high data throughput and low latency. Batch analytics is not constrained to fast answers/processing and has better accuracy. It can be periodically updated with new input data. Analytics models can be descriptive, predictive or prescriptive. ML or deep learning algorithms can be used for each of these three models.

System Characteristics

System characteristics are important for the provision of various dependencies and requirements, which are used to collect, store and communicate data in an industrial processes. Safety is an important characteristic in IIoT because in industry, the most important critical issues are human injury of loss of life. Security mechanisms in IIoT should be applied to ownership, authentication and authorization. Data management is another system characteristic. Data can be collected in a raw, integrated, cleaned or meaningful form. Connectivity within one domain is considered to be more reliable (and so is data, obtained from it) than connectivity between two or more domains. Also using various communication protocols and standards affect speed and hence – the ability to process data in real time.

An assessment approach

Our approach is based on the use of the main topics of IIRA. Each of them can be listed as a domain – business, connectivity, security and analytics. For each domain, we take the most important subdomains. An expert opinion and evaluation for a subdomain can be given in the range between 0 (if the subdomain is irrelevant in a IIoT) and 6 (max score – the subdomain is best applied/supported). The values are given as a general assessment for a feature and should be not closely linked to the assessed IIoT. For example, using best known and highest ranked safety features/network/framework, an expert can give a value of 6. When using weak security monitoring, configuration and management, the expert gives a value of 1. Next comes the assessment of the importance (or as given bellow – weight) of a subdomain for the particular IIoT. The weight value is in the range between 1 (low importance to the system) and 5 (very high importance). These values are provided by the management, top executives or company and designers of the assessed IIoT on the basis of their considered importance for the system. An example of assessment of an IIoT system is given in Table 1.

Table 1: Assessment of an Industrial Internet of Things system

Domains	Assessment of:	Value (0-6)	Weight (1-5)	Total value
Business	Market Context	4	5	20
	Strategy	3	5	15
	Business model innovation	4	5	20
	Best practices and platforms	5	5	25
Connectivity	Connectivity standards	2	5	10
	Connectivity functions	5	4	20
	Transport layer	3	3	9
	Connectivity framework	2	4	8
Security	Safety	6	4	24
	Security	2	2	4
	Resilience	4	2	8
	Risk management	5	3	15
	Monitoring, configuration and management	1	3	3
Analytics	Business usage	2	2	4
	Implementation	4	3	12
	Big data	1	3	3
	Artificial intelligence	3	2	6
	Methods and modelling	2	2	4
	System characteristics	3	3	9
Total assessment				219

The table above demonstrates how a IIoT system can be assessed in a quantified manner. The maximum IIoT assessment/mark is equal to 19 * 30 = 570 for an industrial system, employing the maximum scores for all domains. The chosen values (from experts) and weights (from system management) for an example IIoT system, presented above, make the overall system assessment equal to 219.

Conclusion

The paper looks at the significance of IIoT and makes a short review of existing reference architectures for them. IIRA is such an architecture – probably the most elaborate and carefully designed one. It was developed by representatives of some of the biggest companies in the field and for this reason was chosen as a basis for our assessment methodology. The main domains and subdomains of IIRA are briefly presented. The methodology of creating a value for IIoT architecture is based on expert and management quantitative assessment. Other works have presented the quantitative assessment of features like trustworthiness and robustness (Wu et al., 2021), security requirements (Tange et al., 2019), security, privacy and trust (Chen et al., 2021), etc. but no overall assessment for an IIoT has been found in scientific papers. The presented approach can be modified to include more domains or subdomains, but can also be simplified whereby some of the subdomains can be removed. Further work on the application of this methodology can be considered.

References

Arrowhead. (2017). Eclipse Arrowhead Framework, available at: https://www.arrowhead.eu/eclipse-arrowhead/this-is-it/ (accessed 2.14.21).

Bader, S. R., Maleshkova, M., Lohmann, S. (2019). Structuring Reference Architectures for the Industrial Internet of Things, Future Internet 11, 151. https://doi.org/10.3390/fi11070151

Chen, L., Ye Zh., Jin S. (2021). A Security, Privacy and Trust Methodology for IIoT. Technical Gazette, Tehnicki vjesnik 28, 898–906.

Federal Ministry for Economic Affairs and Energy of Germany. (2021). What is Industrie 4.0?, available at: https://www.plattform-i40.de/PI40/Navigation/EN/Industrie40/WhatIsIndustrie40/what-is-industrie40.html (accessed 2.14.2021).

IDS RAM. (2021). Reference Architecture, International Data Spaces, available at: https://internationaldataspaces.org/use/reference-architecture/ (accessed 9.22.2021).

OpenFog Consortium. (2017). OpenFog Reference Architecture for Fog Computing, available at: https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf

Lydon, B. (2021). RAMI 4.0 - Reference Architectural Model for Industrie 4.0, International Society of Automation, available at: https://www.isa.org/intech-home/2019/march-april/features/rami-4-0-reference-architectural-model-for-industr (accessed 9.21.2021).

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., Gidlund, M. (2018). Industrial Internet of Things: Challenges, Opportunities, and Directions, IEEE Transactions on Industrial Informatics 14, pp. 4724-4734, https://doi.org/10.1109/TII.2018.2852491

Tange, K., De Donno, M., Fafoutis, X., Dragoni, N. (2019). Towards a systematic survey of industrial IoT security requirements: research method and quantitative analysis, in Proceedings of the Workshop on Fog Computing and the IoT, IoT-Fog '19, Association for Computing Machinery, New York, NY, USA, pp. 56-63, https://doi.org/10.1145/3313150.3313228

Industrial Internet Consortium. (2021). The Industrial Internet Reference Architecture v 1.9, available at: https://www.iiconsortium.org/IIRA.htm (accessed 2.25.2021).

Weyrich, M., Ebert, C. (2016). Reference Architectures for the Internet of Things, IEEE Software 33, pp. 112-116, https://doi.org/10.1109/MS.2016.20

Wu, X., Wang, J., Wang, P., Bian, Z., Huang, T., Guo, Y., Fujita, H. (2021). Trustworthiness assessment for industrial IoT as multilayer networks with von Neumann entropy, Applied Soft Computing 106, 107342, https://doi.org/10.1016/j.asoc.2021.107342