2019 International Conference on Networked Systems (NetSys)

Secure Real-time Communication and Computing Infrastructure for Industry 4.0 – Challenges and Opportunities –

Erich Zielinski, Julius Schulz-Zander
Fraunhofer Heinrich Hertz Institute, Berlin, Germany

Marc Zimmermann, Christian Schellenberger
Technische Universität Kaiserslautern, Germany

Alejandro Ramirez, Florian Zeiger
Siemens AG, Munich, Germany

Mathias Mormul
Universität Stuttgart, Germany

Felicitas Hetzelt, Felix Beierle
Technische Universität Berlin, Germany

Harald Klaus
Deutsche Telekom AG, Germany

Hanspeter Ruckstuhl
Nokia, Munich, Germany

Alexander Artemenko
Robert Bosch GmbH, Renningen, Germany

***Abstract*—In this experience paper, we summarize the analysis of key technologies that are prerequisite for a secure real-time communication and computing Infrastructure in the smart factory, which supports flexible and reconfigurable production assets with a real-time digital representation. A broad range of Industry 4.0 use cases is evaluated – jointly with industrial application partners - and a set of basic requirements is derived from them.**

These challenges need to be addressed by available and upcoming ICT technologies in the domains of cloud computing in an industrial environment, virtualization and industrial Edge Computing, 5G radio and network, analytics with big and fast data, and Artificial Intelligence / Machine Learning technologies. The analysis includes mechanisms for secure and reliable connectivity in production, secure wireless communication and secure processes, massive sensor data analysis, and (virtual) network elements like secure gateway. Challenges and opportunities for new applications in production are described in the following.

***Index Terms*—Industry 4.0, Distributed Industrial Clouds, Industrial Edge Computing, Security, Virtualization, SDN, 5G**

I. Introduction and Vision

The digitization of industrial production, which combines manufacturing capabilities with new information and communication technologies, is seen as a way to reduce CAPEX and OPEX and increase the flexibility towards lot size one to meet today's customer needs for individual products. Moreover, the trend towards the smart factory will enable new use cases and business models (referred to as Industry 4.0).

Implementing this vision requires a holistic view of the underlying infrastructure taking into account technical possibilities adapted to industrial requirements. Such an industrial communication infrastructure enabling platforms and applications becomes an important economic factor. This will bring tremendous benefits:

This work is partially supported by German national funding under support grant no. 01MA17008 (IC4F).

978-1-7281-0568-0/19/$31.00 ©2019 European Union

- Boosting the performance of production facilities due to tight monitoring and configuration of equipment (e.g., condition monitoring, predictive maintenance, digital twin in real-time).
- Close alignment of production and business processes through flexible (re)-configuration of production facilities.
- Connectivity of all objects in a heterogeneous environment and supporting both, standard and proprietary interfaces.
- Improved collaboration across the value chain by quality-assured, secure and in-time connectivity, within and across factory premises boundaries.

More insight into the economic drivers and challenges is obtained from an analysis of the underlying industrial application scenarios (use cases) [1]. This encompasses new, innovative use cases representing a trend in the field of Industry 4.0., as well as use cases with demanding industrial requirements to communication technologies beyond the state-of-the-art. As a result, generic requirements that will drive technology selection and architecture for industrial networks can be derived. The results are summarized in Chapter II. For each of the generic requirements, technology options need to be considered which fulfill the boundary conditions of the use cases. The challenges and opportunities to enable Industry 4.0 use cases are presented in Chapter III.

II. Key Drivers in Industrial Communication

Key drivers for industrial communication were derived from the analysis of the use cases as describe above. They can be viewed as a set of generic requirements, which will drive technology selection and architecture for industrial networks.

Everything gets Connected: A high degree of automation is already state of the art in factories. However, Industry 4.0 adds the ability to seamlessly exchange data between the factory network and the rest of the enterprise. Ubiquitous connectivity,

and easy data exchange and access will be established between the Internet, the Intranet, and the shop floor.

Shop Floor goes Wireless: A close interlock between business and production processes requires that a factory can adapt to different business needs also in the physical world. For a new product launch, the production needs to be executed by flexible robots creating a new production island on demand, instead of restructuring a whole static factory line. To exploit the possibilities of seamless communication between machine control and business process, physical flexibility on the shop floor is necessary, allowing free flow of production equipment and material flow. From communication point of view, wireless connections should be used to avoid spatial constraints from fixed cabling.

High Bandwidth for Video: Visual inspection and recognition of mobile objects in the factory require high bandwidth in combination with low packet loss in particular in industrial mobile networks.

High Device Density for Sensor Networks: One goal of the industrial factory network is the ability to get deep insights into production process by gathering and analyzing data from many sensors. The number of sensors, which can be connected simultaneously, is an important performance parameter. Energy consumption of the wireless connection should be minimized to enable long battery lifetime. In this way, truly wireless sensors without wired power supply get feasible.

Fast and Reliable Communication for Machine Control: In factory automation, the amount of data to be transferred is typically low, but time between sending a message and reception of the message (latency) is of uttermost importance. Predictability of latency allowing constant cycle times within a production network is even more important than low absolute latency. With higher, but predictable latency, a production process can still operate on lower speed. In case of unpredictable latency, the entire production might be disrupted resulting, e.g., in the need for a safety stop of a machine. The ideal case of low and predictable latency is referred to as ultra-reliable low-latency communication. Besides factory automation, the experience and usability of tools using augmented reality (AR) strongly depends on low latency.

Hierarchical Infrastructure to Support Different Use Cases: Besides wireless transmission timing requirements of a use case also need to include data processing. If a use case requires low latency between event and action, the processing needs be executed as close to the wireless access as possible. Collocation of access node and compute resource is known as Edge Computing. It is used for communication and processing needs of objects connected to the same edge computing instance, i.e., only for a rather limited spatial area like a shop floor. Use cases utilizing data from objects distributed over a larger spatial area, require central processing in a central cloud.

Sharing Infrastructure between Use Cases and Tenants: In a real factory setup, several use cases owned and operated by different business entities and exhibiting different communication requirements will run on the same physical infrastructure. The difficulty in these multi-tenant scenarios is to optimize two contradicting properties. On the one hand, resources should be pooled ("shared") between different use cases and tenants to enable best possible resource utilization. On the other hand, resources should be isolated and dedicated allowing use case specific optimizations and to ensure that resources are available when needed. Virtualization techniques can be used for handling such resource partitioning problems.

Automated Deployment and Operations: A manifold of use cases resulting in different requirements, a rich choice of technology options, and various possibilities to deploy those on a virtualized hierarchical infrastructure need to be considered. These factors change over time and factory networks need to adapt to this. The employed ICT automation framework needs to consist of deployable ("virtualized") functions used to build the factory network, a deployment system pushing these functions on the infrastructure, and an orchestration framework generating the necessary communication links between these functions.

Security: With expansion of the internet to the cyber-physical domain, also attack scenarios known from the internet become relevant. Attacks might occur via a cloud system and corrupt or even hijack a production environment from outside. Therefore, security must be an integral part of an industrial network pursuing communication only between verified identities as well as applying end-to-end protection. Furthermore, a fine granular access management system needs to limit access to resources to only eligible entities.

III. Challenges and Opportunities

Distributed Industrial Cloud

The Distributed Industrial Cloud is an evolution of cloud computing, which brings unified compute, storage, networking and platform services to the industrial domain for hosting distributed applications on diverse factory, enterprise and public devices, geographically distributed across wide areas (see Figure 1).

Such Industrial Clouds represent a novel approach, very different from today's public clouds which centralize homogeneous hardware (compute servers, network and storage devices) in a few large data centers.

The distributed industrial cloud introduces compute resources (including hardware acceleration) very close to producers and consumers of the data and thus allows portable industrial application components to be placed virtually anywhere on the continuum from the factory floor to enterprise clouds or the data centers of global cloud providers - optimally aligned with the use case requirements such as latency, throughput, and reliability. Management and orchestration of this distributed industrial cloud supports the intelligent placement according to the different use case requirements. Placement strategies include:

- Remote monitoring and predictive maintenance applications are natural targets for a global cloud deployment because there is no need for a real-time response.

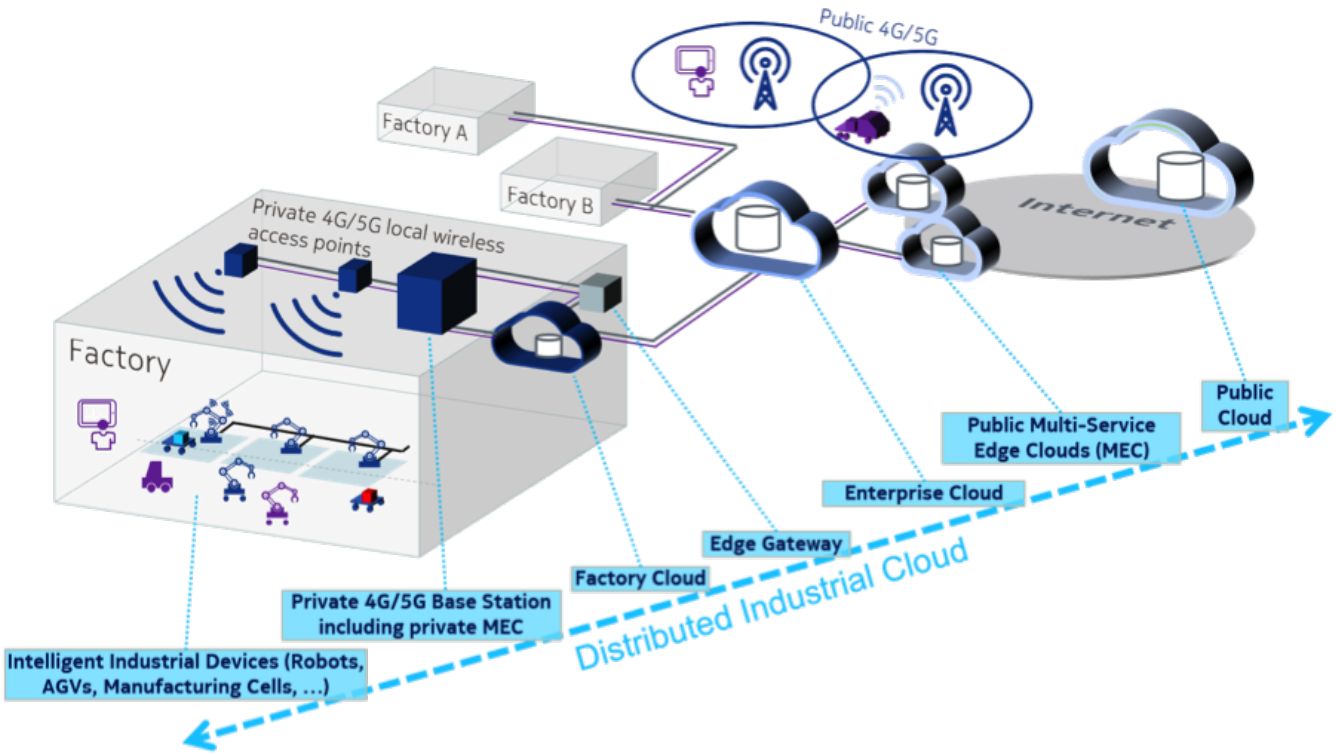

Fig. 1. **Scope of the Distributed Industrial Cloud:** The distributed industrial cloud introduces compute resources (including hardware acceleration) very close to producers and consumers of the data and thus allows portable industrial application components.

- Factory clouds and edge gateways host services, which aggregate data from multiple assets, filter and pre-process this data before transmitting it to enterprise or global cloud resources.
- Real-time, low-latency actions for machine control are executed on the machine itself or near the machine on industrial edge computing components. Some low latency use cases allow for a convergence of industrial edge-computing resources and multi-access edge-computing (MEC) resources collocated with private 5G base stations.

Virtualization NFV/SDN

The distributed industrial cloud leverages well known concepts from the telecommunication space such as Network Function Virtualization (NFV) [2], Hardware Acceleration and MEC [3]. Virtualized Network Functions (VNFs) are hosted on a virtualized infrastructure which spans across diverse network elements and points of presence. Hardware acceleration and intelligent functions placement ensure that VNF based solutions can provide reliable and low latency networking services on a par with non-virtualized implementations. In future networks it is foreseen, that the distributed compute and networking resources are not only used by the communication service providers themselves but are offered to 3rd parties in the form of network slices thus allowing for efficient use of network infrastructures.

Network slicing (NS), e.g., via VLANs or MPLS, is a well known concept which is typically used in today's enterprise and operator networks. The goal of NS is the separation of traffic into different network domains with different performance guarantees. However, one of today's key challenges is to guarantee performance isolation between the different slices. Moreover, NS is one of the key features of *Software-Defined Networking* (SDN) which separates the control from the data plane to allow each to evolve independently from the other. SDN outsources the control of the data plane to a logically centralized control plane. This allows SDN applications running atop of the SDN control plane to programmatically control the data plane. Specifically, the applications leverage an north-bound API exposed by the controller. However, the challenge is to provide proper south-bound interfaces for the huge variety of different devices types in the data plane. For instance, while OpenFlow is well suited for standard Ethernet devices, it lacks the understanding for TSN.

Wireless 5G

The I4.0 era is characterized by ubiquitous connectivity: Everything is connected – sensors, actors, controllers, tools, machines, humans, digital twins, analytics, Artifical Intelligence (AI) / Machine Learning (ML) applications. Whilst the internet and enterprise Information Technology (IT) has long since converged on just three connectivity standards - 3GPP cellular, IEEE 802.1 Ethernet and IEEE 802.11 Wireless LAN – the industrial domain has only recently started to consolidate the many industrial wireline communication protocols with IEEE 802.1 Ethernet with time sensitive networking (TSN)

extensions [4]. For industrial wireless, the 3rd Generation Partnership Project (3GPP) has positioned its 5G standard for consolidating the many industrial wireless technologies in both the local and the wide area. This convergence on TSN Ethernet and 5G will facilitate the seamless integration of fixed and wireless industrial, enterprise and internet communication - a key enabler for "everything connected" and converged IT and Operations Technology (OT).

In the upcoming new releases of 5G New Radio (NR) the technical foundation will be laid for meeting the performance requirements of wireless time sensitive communication (TSC), compatible with TSN Ethernet, along multiple dimensions [5].

- Low Latency Communication with below 0.5ms one-way delay on the radio link is achieved by the scalable 5G numerology, which enables short Transmission Time Interval (TTI) and non-slot based scheduling, up-link (UL) grant free and down-link (DL) pre-emptive scheduling.
- High Reliability with a frame loss ratio below 10E-5 (while maintaining lowest latency) is expected to emerge with features such as increased micro-diversity with multiple input, multiple output (MIMO) antenna technology, pro-active data duplication, and multi-connectivity enhancements, which can eliminate interruption during handover.
- High bandwidths of 5Gbps in UL and 10Gbps in DL can be made possible by new spectrum options ranging from approx. 400 MHz potentially up to 100 GHz and up to 25% higher cell capacity, compared to Long Term Evolution (LTE - the 4th generation 3GPP standard), thanks to significantly improved MIMO operation with NR codebooks.
- Time synchronization with sub 1 µs precision across the air interface can be achieved employing the precision time protocol (IEEE 1588-2008) and 5G internal or external grand master clock.

The 5G Core (5GC) introduces a new Services Based Architecture (SBA) to implement control (e.g. Session Management, Authentication, Authorization, Accounting and Quality of Service (QoS) control) and software-defined networking (SDN) based control of user plane functions (e.g. the gateway to interface with a bridged TSN Ethernet) [6]. The SBA provides powerful service capabilities, can be extended with tailor-made industrial services, and allows arbitrary placement of control- and user-plane functions. Such flexibility lets the 5GC meet the requirements of diverse industrial applications and their underlying distributed industrial cloud:

- Following the SDN paradigm, the 5G User Plane Function (UPF) can be deployed separate from the control plane, e.g. collocated with base stations and edge computing for local processing of real-time critical industrial data or centrally in the factory cloud where non-real time data is consumed.
- The extended policy control framework allows programmatic configuration of network slices with user defined QoS. The enhancements mirror the NR capabilities and support the TSC features (e.g. time triggered transmission according to the cyclic communication requirements of distributed automation applications).
- Unlike earlier 3GPP standards, 5G should support broadcast and multicast natively, without a separate, complex middleware. The decision of using unicast or multicast on the air interfaces can be taken by the RAN avoiding the need for changing the transport in the core.

The standardization of 5G wireless industrial communication is a combined effort of communication equipment vendors, telecoms operators and industrial enterprises directed by the 3GPP. Given the complexity of this task, 3GPP has defined a phased approach. 3GPP Release 15 standards, completed 3Q2018, enable independent deployment of 5G (without need for LTE) and introduce the SBA for the core. Release 16 standards, scheduled for 1Q2020, will provide extended support for Ethernet and time sensitive communication capabilities. Finalization of the industrial wireless capabilities can be expected with Release 17.

Software Defined Radio (SDR)

A dynamic production environment will require the flexible deployment of different wireless communication standards, on-demand, depending on the current requirements. This should be installable per software, with no hardware swap being necessary. Each of the tenants may require a different wireless communication standard.

A Software Defined Radio (SDR) [7] building block will be able to provide the flexible connectivity on a per-tenant basis. A single hardware radio platform can be reconfigured by software, and the required signal processing is encapsulated on containers, which can be started or stopped on-demand. This simplifies the coexistence and management of the different standards and defines standard distribution mechanisms.

It is envisioned to add an app-store on top of the bare containers, which allows each tenant to download, install and uninstall different connectivity options.

Analytics in the Smart Factory

The digitization of the shop floor introduces a wide-ranging abundance of possibilities for analytics within the Smart Factory. Through data originating from a variety of different sensors on machines and workers, a detailed insight into operating procedures and process operations is possible. Use cases range from root cause analysis, where the goal is to detect the source of an erroneous behavior or state, up to predictive analytics, e.g., Predictive Maintenance, to predict future events. Different use cases might pose different requirements to the architecture of the system. For long term data analytics, e.g., Big Data requirements need to be addressed. (Near) Real-time analytics [8] require scalable software modules.

Big Data Analytics for Smart Factories presents new challenges since traditional approaches, such as data mining, may not be suited to fulfill all requirements of the manufacturing industry. Since data is the foundation for analytics, first, a scalable approach for data management and access must

exist. Using recent database concepts, such as data lakes and communication middleware, the access to historical and real-time data can be enabled. Second, these technologies as well as the data analytics platforms must support edge computing to fulfill requirements like security and constraints, such as low latency. Consequently, the distribution of data, applications, and technologies to edge and backend imposes a higher management complexity of the overall system and must be accompanied by new concepts and tools to simplify the use of analytics in Smart Factories and support small and medium-sized enterprises. Another problem resides in the data itself, as poor data quality can affect the results of analytics significantly [9]. Noise in sensor data, erroneous measurements, badly chosen sampling rates, and other influencing factors must be addressed by enhanced sensor technologies, measuring concepts or data analytics itself.

Secure Connectivity – End-to-end Security in Production

In the course of the Industry 4.0 paradigm, secure connectivity is a key success factor [10]. Industrial market player, especially SME's are still expressing their concerns with respect to security issues. Many stakeholders, in particular factory operators, connect their networks to the Internet or to Internet-connected networks for the sake of efficiency or maintenance consideration. However, the security model for these factory networks was that of a standalone, unconnected network, and they are often not yet prepared for security threats in the Internet. Furthermore, today's networks are usually "flat", which means no segmentation or traffic control is used, for simplicity and reliability. Accordingly, as soon as an attacker is inside the network, it can be easily compromised.

Implanting security within existing industrial businesses, secure connectivity services have to be designed to ensure that both, existing as well as new production facilities and components may take part in the industrial r/evolution of Industry 4.0. It was agreed within the IC4F project to follow a comprehensive approach that consists of a **secure connectivity gateway**, which extends the industry device physically (i.e., the connection between the gateway and industry device is secure) containing a **secure hardware anchor** in combination with a **public key infrastructure**.

The secure connectivity gateway provides a secure connectivity path to the industry device:

- A secure hardware anchor ensures that the complete software stack on the gateway is booted securely using advanced encryption and certification methods to prevent or detect manipulations on critical software components.
- Certificate- as well as role-based data handling will enable to provide (or to prevent) access to dedicated data. For example, machine maintenance may be performed using remote access to the production device via a 5G connection. The role-base access provided with the secure connectivity gateway provides access to specific maintenance data.
- The secure connectivity gateway enables security on application level, e.g. using the security mechanisms of the OPC-UA foundation.

Integrating new industrial devices, e.g., sensors, actors, gateways, production devices, into standardized and highly automated productions require a consistent certificate management from the early beginning. Assuming that each securely connected device is carrying an initial certificate, controlled certificate management processes based on a powerful public key infrastructure are needed along the whole life cycle.

Public key infrastructures have to be suitable for mass use and should be executable without manual administrative intervention if possible. As minimum configuration of an Industry 4.0 PKI the following services were considered within the IC4F consortium:

- Verification service with a very high availability and processing rate from worldwide incoming requests (enabling real-time verification of a digital identity)
- Revocation service (revocation of a digital identity)
- Service for creation of certificates (issuing digital identities in an automated procedure)
- Distribution service (enabling automated distribution of a digital identity)
- Registration service (authorization of the request to issue a digital identity in an automated procedure)
- Reporting service

For the conceptual establishment and operation of an Industry 4.0 PKI, the following points are going to be considered within the IC4F consortium, e.g.:

- Specification of the PKI hierarchy, starting with the Industry 4.0 Root-CA (Certification Authority)
- Specification of the number of possible manufacturer-related CA levels, including the defined content within the digital identity.
- Specification of the minimum requirements for the digital identity with regard to content to be used as well as the cryptography algorithms.
- Organizational frame concept that defines (amongst other issues) on which basis digital identities are issued, authorized, extended and disabled.
- Preparation of an authorization procedure, in which IoT/M2M devices or Industry 4.0 applications may be used on a case-by-case basis.
- Specification of an Industry 4.0 policy that determines the framework conditions for the issuing of CA and minimum requirements for device and implementation IDs.

Reliable Wireless Communication – Protect the new Medium

Reliable wireless communication is important due to time-critical processes in manufacturing [11]. Nowadays, the lack of reliability is often the deciding point for choosing wired communication solutions instead of wireless. Several approaches are introduced to improve the reliability of the communication between two components, independent of them being small sensors, production machines or moving vehicles.

- **Private cellular networks** are networks operating in locally licensed spectrum [12]. The user has to obtain the rights to use this spectrum, depending on local regulations, either from either a mobile network operator who owns the spectrum nationwide or the government directly. The benefit of private cellular networks is exclusivity in the spectrum. No other communication devices are allowed to communicate on the same frequency. This decreases the interferences on said frequency through other networks.
- **Using dedicated industrial wireless protocols in the ISM band:** Protocols that are specialized for industrial usage often use time slot based communication where every participant is guaranteed a certain slot for communication. Therefore, a conditional reliability can be promised but only if there are no other networks on the same frequency in the vicinity [13]. Because those protocols are usually used in the ISM bands where it is only allowed to access the medium if it is idle, interferences from other communications might still prohibit the access on the time slot which means that the device has to wait for the next slot. Those protocols are also sensitive for in band jamming that forces them to stay back and, therefore, the time-critical communication can be disrupted.
- **Securing commonly used protocols:** This approach is using protocols that are well known and understood and altering them to be better suited for industrial purposes or using supporting systems to minimize interferences. To achieve this, different mechanisms have to be used in the factory like a wireless communication monitoring and management system. With the help of the monitoring system, the communication of registered devices can be surveyed and potential communication breakdowns detected in early stages or at least fast enough to suggest countermeasure to overcome the situation. Additionally, the live coverage can be analyzed by dynamic radio mapping tools to find sources of potential interferences. To detect those interferences, data from infrastructure and dedicated sensor devices is needed and methods of machine learning can be applied to detect anomalies within this data. If an anomaly is detected, the management system can push new configurations, like a channel switch, to affected devices to mitigate the effect of the interferences which would otherwise lead to performance drops of the production process.

To have a sufficiently reliable communication, a combination of two or even all three approaches is recommended. A special industrial communication protocol can be applied within an exclusively used frequency band with additional monitoring and management to provide the highest possible reliability for time-critical communication. The recommended approach might also depend on the considered use case and for some less critical processes even one approach can deliver the required level of reliability.

IV. Conclusion

Following the above discussion, the challenges and opportunities can be grouped in three domains:

- The ICT infrastructure layer provides wireless or wired access to all kinds of objects on the shop floor and connects them with cloud resources in the different network domains.
- The Application and Data layer encompasses factory applications, data models, data management, data analytics and data visualizations, as well as AI/ML algorithms.
- An overarching security framework provides end-to-end security a secure hardware anchor in combination with a public key infrastructure and specific security concepts for wireless technologies.

As a result, a great variety of innovative use cases for new Industry 4.0 business models as well as use cases with demanding industrial requirements are enabled by the key technologies as described above. They can be viewed as technology building blocks and their choice guarantees the required industrial KPIs.

References

[1] IC4F Consortium, "White Paper, Building Blocks for a Secure Real-time Communication and Computing Infrastructure for Industry 4.0," Tech. Rep., 2018.

[2] ETSI GS NFV 002, "Network functions virtualization (NFV); architectural framework v1.2.1," Tech. Rep., ETSI, December 2014.

[3] ETSI GS MEC 003, "Mobile edge computing (mec); framework and reference architecture v1.1.1," Tech. Rep., ETSI, March 2016.

[4] "Time-sensitive networking (tsn) task group, published tsn standards: 802.1qbu, 802.1qbv, 802.1qca, 802.1qch, 802.1qci, 802.1qcc, 802.1qcp,," Tech. Rep., IEEE, 1015-2018.

[5] Z. Li, M. A. Uusitalo, H. Shariatmadari, and B. Singh, "5g urllc: Design challenges and system concepts," in *2018 15th International Symposium on Wireless Communication Systems (ISWCS)*, Aug 2018, pp. 1–6.

[6] ETSI TS 123 501, "5g; system architecture for the 5g system (3gpp ts 23.501 version 15.3.0 release 15)," Tech. Rep., ETSI, September 2018.

[7] J. Mitola, "The software radio architecture," *IEEE Communications Magazine*, vol. 33, no. 5, pp. 26–38, May 1995.

[8] H. Hromic, D. Le Phuoc, M. Serrano, A. Antonić, I. P. Žarko, C. Hayes, and S. Decker, "Real time analysis of sensor data for the internet of things by means of clustering and event processing," in *2015 IEEE International Conference on Communications (ICC)*, June 2015, pp. 685–691.

[9] Zhiting Song, Yanming Sun, Jiafu Wan, and Peipei Liang, "Data quality management for service-oriented manufacturing cyber-physical systems," *Computers & Electrical Engineering*, vol. 64, pp. 34 – 44, 2017.

[10] Bundesministerium für Wirtschaft und Energie (BMWi), "IT-Sicherheit für die Industrie 4.0. Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten.," Januar 2016.

[11] A. Frotzscher, U. Wetzker, M. Bauer, M. Rentschler, M. Beyer, S. Elspass, and H. Klessig, "Requirements and current solutions of wireless communication in industrial automation," in *2014 IEEE International Conference on Communications Workshops (ICC)*, June 2014, pp. 67–72.

[12] Bundesministerium für Wirtschaft und Energie (BMWi) - Bundesnetzagentur, "Anhörung zur lokalen und regionalen Bereitstellung des Frequenzbereichs 3.700 MHz bis 3.800 MHz für den drahtlosen Netzzugang," 2018.

[13] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, Oct 2009.

Additional Information

Bibliographic Data

E. Zielinski, J. Schulz-Zander, M. Zimmermann, C. Schellenberger, A. Ramirez, F. Zeiger, M. Mormul, F. Hetzelt, F. Beierle, H. Klaus, H. Ruckstuhl, and A. Artemenko, "Secure Real-time Communication and Computing Infrastructure for Industry 4.0 – Challenges and Opportunities," in *Proceedings 2019 Advanced Communication Networks for Industrial Applications (AIComNets) at NetSys 2019*. IEEE, 2019.

Pre-print from

https://beierle.de

Online at

https://ieeexplore.ieee.org/document/8854499

BibTeX

@inproceedings{Zielinski2019AiComNets,
title = {{Secure Real-time Communication and Computing Infrastructure for Industry 4.0 - Challenges and Opportunities}},
author = {Zielinski, Erich and Schulz-Zander, Julius and Zimmermann, Marc and Schellenberger, Christian and Ramirez, Alejandro and Zeiger, Florian and Mormul, Mathias and Hetzelt, Felicitas and Beierle, Felix and Klaus, Harald and Ruckstuhl, Hans and Artemenko, Alexander},
booktitle = {{Proceedings 2019 Advanced Communication Networks for Industrial Applications (AIComNets) at NetSys 2019}},
publisher = {IEEE},
year = {2019},
doi = {10.1109/NetSys.2019.8854499}
}

Copyright Note

IEEE Copyright Notice
Copyright (c) 2019 IEEE

Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.