INVITED PAPER

Coexistence Standardization of Operation Technology and Information Technology

By Max Felser, *Senior Member IEEE*, Markus Rentschler, *Senior Member IEEE*, and Oliver Kleineberg, *Member IEEE*

ABSTRACT | In factory automation (FA) and process control, networks and protocols of the operation technology are more and more merged with those of the information technology (IT). The requirements of operational technology (OT) and IT are different. Modern networks and protocols for communication in FA and process control systems must take care of the coexistence and convergence between the IT and OT worlds. Due to historical developments, the standards for OT were and remain defined by the International Electrical Commission. The IT, on the other hand, is the domain of the International Telecommunication Union and the International Standard Organization (ISO), which takes over most of the standards in the communication field from the IEEE Standard groups 802. This paper provides an overview of the standardization bodies involved and provides examples on how different requirements introduced by OT and IT can coexist. The merging of OT and IT on an Ethernet network with time-sensitive networking is the key technology for real-time applications in the factory floor. The adoption of the industrial protocol OPC UA provides secure connections from the factory floor to automation cloud infrastructures. IO-Link wireless, as new standard for sensors and actuators in OT, provides coexistence mechanisms toward wireless standards in IT applications such as IEEE 802.11. These examples show that there are possibilities to coexist and even to merge the standards and technologies of OT and IT in a successful way.

Manuscript received August 1, 2018; revised December 20, 2018 and February 4, 2019; accepted February 18, 2019. *(Corresponding author: Max Felser.)*

M. Felser is with Bern University of Applied Sciences BFH, CH-3400 Burgdorf, Switzerland (e-mail: max.felser@bfh.ch).
M. Rentschler is with the Institute for Intelligent Industrial Systems Balluff GmbH, 73765 Neuhausen, Germany (e-mail: markus.rentschler@balluff.de).
O. Kleineberg is with Hirschmann Automation and Controls GmbH, 72654 Neckartenzlingen, Germany (e-mail: oliver.kleineberg@belden.com).

Digital Object Identifier 10.1109/JPROC.2019.2901314

KEYWORDS | Information technology (IT); operation technology; real-time Ethernet (RTE); WLAN

I. INTRODUCTION

Networks and protocol specifications of factory automation (FA) and process automation (PA), as part of operational technology (OT), have been defined by the International Electrical Commission (IEC). The OT has developed its own culture of optimizing the availability, reliability, and longevity of the investments made to produce physical goods. By contrast, information technology (IT) requires prompt reactions to new requirements. The necessary long-term specifications for the IT are laid down by the International Standard Organization (ISO), based on the standards in the communication field from other standardization groups that work on an international or national level, such as IEC, the American National Standards Institute (ANSI), or the IEEE Standard groups 802. A technology could, for example, be standardized in IEEE 802. After this process has been completed, relevant standards can be adopted, for example, by ANSI or IEC and subsequently adopted by ISO. The Internet Engineering Task Force (IETF) also plays a significant role with their requests for comments (RFCs). One of these modern technologies adopted by IT is the "Cloud" technology (CT).

The total number of nodes in IT is much larger than in OT. This leads to the fact that the typical cost per node in IT is lower than that in OT. To further reduce costs, OT is in the process of adopting the same network technologies as defined in the IT world at an increasing rate. The two worlds begin to merge as shown in Fig. 1. It is also expected that the use of CT in favor of OT will make additional business models and automation structures possible and profitable. Combining these domains is often referred to as the "Industrial Internet of Things" (IIoT).

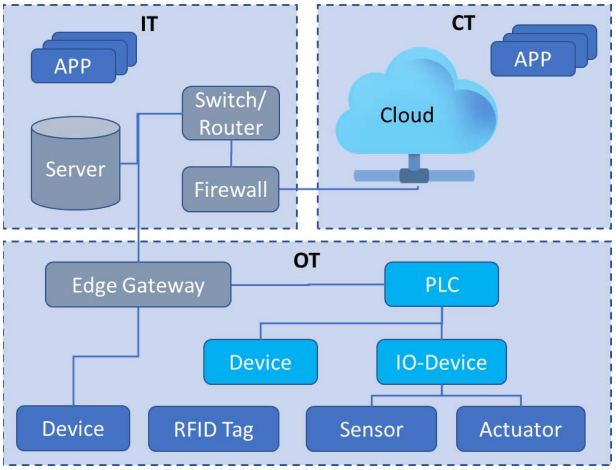

Fig. 1. ***Architectural overview of the IIoT domains Operation Technology, IT, and CT, and their relations.***

Adoption of the same networks in OT and IT may be useful on the cost level, but the requirements for applications in the field of OT and IT are different, which may lead to new types of challenges in bridging between different worlds with the same technology.

This paper provides an overview of the most important standardization bodies that are dealing with information and communication networks in the IIoT domain. Subsequently, it highlights the requirements from the OT and IT and the coverage of these requirements. In the third part, examples are given that illustrate how the different requirements of OT and IT can coexist.

II. STANDARDIZATION

National and international legislative bodies define laws and regulations which often have a binding nature and are always publicly accessible (Fig. 2). Since the founding of the EU, single-state laws have played a minor role in Europe because the EU Commission provides the binding rules for the member states. For telecommunication standardization in Europe, the European Telecommunications Standards Institute was founded by the European Conference of Postal and Telecommunications Administrations (CEPT) in 1988 and is officially recognized by the European Commission. Within CEPT, the Committee for International Telecommunication Union (ITU) Policy (Com-ITU) is responsible for the coordination of CEPT and ITU activities. The ITU is a specialized agency of the United Nations and intents to harmonize telecommunications standards worldwide.

In technical topics, the term "state of the art" is often used by the legislator to refer to recognized standards that are created by a self-regulated economy, consisting of standardization organizations and industry consortia. A differentiation can be identified between international standardization bodies with representations from different countries and interest groups or consortia of companies and industries with a common interest. Very often, the consortia groups are also open to individuals for participation. Usually, technical subjects and their details are defined in specifications and guidelines of these industrial consortia. Typically, a new technology is developed by consortia or interest group and subsequently brought up to an international standardization body to be published as a recognized standard, if a long-term stability is required for further implementation and market acceptance.

A. International Recognized Standardization Bodies

Regarding standards for information networks, the International Telecommunication Union, the International Organization for Standardization, and the International Electrotechnical Commission are the most important organizations that achieve worldwide acceptance.

1) International Telecommunication Union: ITU is the United Nation's specialized agency for information and communication technologies. The ITU allocates the global radio spectrum and develops the technical standards that ensure networks and technologies interconnected on a global level. It is structured in study groups, each of them comprising experts from both public and private sectors and designed to develop recommendations for an area of information and telecommunication technologies (ICTs). For example, the Study Group 20 is working on addressing the standardization requirements of Internet of Things (IoT) technologies, with an initial focus on IoT applications in smart cities and communities. One key reference for security standards, which is in use today in the IT world, for example, is "Recommendation ITU-T X.509 for electronic authentication over public networks." ITU-T X.509, based on public key infrastructure, is used in a wide range of applications; from securing the connection between a browser and a server on the web to providing digital signatures that enable e-commerce transactions to be conducted with the same confidence as in a traditional system. Without the wide acceptance of the standards specified by ITU, the rise of e-business would have been impossible.

2) International Organization for Standardization: ISO is an independent, nongovernmental international organization with a membership of 161 national standards bodies

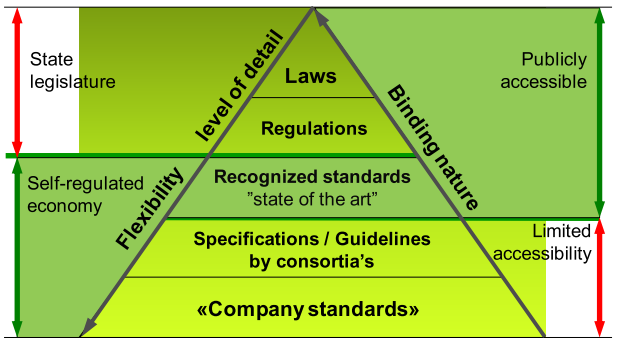

Fig. 2. ***Distinct levels of standards and their accessibility and legal status.***

with its central secretariat in Geneva, Switzerland. Members are the foremost standards organizations in their countries and there is one member per country only. Individuals or companies cannot become ISO members. National committees (NCs) such as ANSI, USA; Deutsches Institut für Normung (DIN), Germany; Bundesamt für Sicherheit in der Informationstechnik (BSI), U.K.; or Schweizerische Normen-Vereinigung (SNV), Switzerland, provide services to ISO and support different technical committees. ISO has published 22 215 international standards and related documents, covering almost every industry, from technology to food safety, to agriculture and healthcare. All local networks as used in the IT world are standardized in the ISO range of standardization. In addition, all device networks that are part of a machine or vehicle are also typically defined as ISO standards.

3) International Electrotechnical Commission: The International Electrotechnical Commission (IEC) is a not-for-profit, quasi-governmental organization that prepares and publishes International Standards for all electrical, electronic, and related technologies, with its headquarters located in Geneva. IEC members are organized in a single NC per country. Individuals participate in the IEC's work through the NCs such as ANSI, USA; BSI, U.K.; Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE), Germany; or electrosuisse, CH. Standardization regarding automation networks and engineering in relation to automation technology is done in different working groups (WGs) in IEC. The OT world is based on the technology defined in these standards [1], [2].

The "IEC/IEEE 60802 Time-Sensitive Networking (TSN) Profile for Industrial Automation" is a recent ongoing joint project between the IEC and the IEEE. It is referenced both at the IEEE 802 [3] as well as the IEC SC65C MT9 [4]. This joint standardization initiative seeks to provide, from the IEC side, a unified application profile to enable the use of the IEEE 802 TSN technology with IEC-specification-based automation technologies. This joint standardization activity is important to IT and OT convergence, as it bridges between the very OT-centric view of the IEC and its automation application profiles and the IT-centric view of the IEEE and its novel TSN network technology that is aimed at the use in mission-critical networks [5].

B. Standardization by Consortia's or Interest Groups

Different industry-driven consortia are supporting defined application domains or specific technologies for information networks and information handling.

1) International Society of Automation: The International Society of Automation is a nonprofit professional association that sets the standard by individual experts for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. ISA is accredited by the ANSI to develop standards following open participation rules. Most ISA standards are published as American National Standards, and many are submitted through ANSI to become international standards through the International Electrotechnical Commission.

Among ISA's standards that have gained international relevance are Enterprise-Control System Integration (ISA-95/IEC 62264) [6], Cybersecurity for Industrial Automation and Control Systems (ISA-99/IEC 62443), or Wireless Systems for Automation (ISA-100/IEC 62734). These existing standards are considered to deliver interoperability horizontally and vertically [7].

2) Internet Engineering Task Force: The IETF's mission is to make the Internet work better by producing technical documents that influence the way people design, use, and manage the Internet. IETF standards are built on the combined engineering judgment of participants, including individuals from academia, network operators, router vendors, and open-source projects. WGs are the primary mechanism for the development of IETF specifications and guidelines, many of which are intended to be standards or recommendations. There are typically over 100 active WGs at any given time. The IETF community uses RFCs documents as the main type of publication to create "Internet Standards." The IETF is the most relevant standardization body for network protocols in the IT domain. The Transmission Control Protocol (TCP)/Internet Protocol (IP) suite for IPv4 and IPv6 and supporting protocols were defined in a series of RFC documents. A range of these protocols has been adopted for OT purposes, such as Simple Network Management Protocol (SNMP) [RFC 1157] and DHCP [RFC 2131]. Network Time Protocol (NTP) [RFC 1305], Hypertext Transfer Protocol (HTTP) [RFC 2616], Extensible Messaging and Presence Protocol (XMPP) [RFC 6120], Constrained Application Protocol (CoAP) [RFC 7390], and JSON [RFC 4627] are also used in the IIoT domain [8].

3) Organization for the Advancement of Structured Information Standards: OASIS [9] as a global nonprofit consortium works on the development, convergence, and adoption of standards for security, IoT, energy, content technologies, emergency management, and other areas. Some of the standards maintained by OASIS could gain acceptance in IIoT, such as Message Queuing Telemetry Transport (MQTT) for publish/subscribe messaging and Advanced Message Queuing Protocol (AMQP) for point-to-point message exchange, both based on TCP/IP.

4) Institute of Electrical and Electronics Engineers: The IEEE scope of work extends far into different technology and application scenarios. On a global scale, IEEE is organized in both a regional and a technical structure. Since the IEEE origins lie in the United States, a specific IEEE-USA committee has been established, which focuses on the U.S. region. Other regional units are consolidated under the Member and Geographic Activity Board. An overview of the IEEE organizational structure is available on the IEEE Internet website in [10].

Table 1 IEEE Working Groups Relevant for IT and OT

IEEE 802 Working Group	Scope	Possible applications in OT	Possible applications in IT
IEEE 802.1 Higher Layer LAN Protocols	Protocols and definitions for ISO-OSI Layer 2 transmission systems (Bridges)	Industrial Ethernet Switch with Real-Time functions	IT infrastructure access switch with high port count and bandwidth
IEEE 802.3 Ethernet	Physical Media (ISO-OSI Layer 1) and Media Access Control (ISO-OSI Layer 2) specifications for wired transmission media	Two-wire Ethernet physical layer access for long-reach, cost-effective sensor attachments	Fiber-optical Ethernet physical access for ultra-high bandwidth applications
IEEE 802.11 Wireless LAN	Physical Media (ISO-OSI Layer 1) and Media Access Control (ISO-OSI Layer 2) specifications for wireless transmission media in local area networks	Connection of automated guided vehicles to a central control infrastructure	Connection of Laptops, PCs and smartphones to central data storage and data services
IEEE 802.15 Wireless Personal Area Network	Physical Media (ISO-OSI Layer 1) and Media Access Control (ISO-OSI Layer 2) specifications for wireless transmission media in personal area networks	Interconnection of distributed, low-cost sensors into a meshed sensor network	Interconnection of mobile devices, such as a smartphone to a hands-free device or car

From a technical viewpoint, IEEE is organized in divisions and, structurally below the divisions, societies that are grouped around specific areas of interest. One example is the IEEE Computer Society [11], which focuses on the technical aspect of computers and comparable machines.

Most relevant from a technology development viewpoint is the IEEE Standards Association (IEEE-SA), which is situated directly at the IEEE Board level. Through the IEEE-SA, either IEEE societies can engage in technical standards development work or IEEE standards' committees can be formed, which conduct the technical standardization processes without being firmly embedded within a single society that is driving the standardization effort.

Of particular importance for the topic of communication networks is the IEEE LAN/Metropolitan Area Network (MAN) Standards Committee (LMSC), also known by its project number, IEEE 802 [12].

Within the IEEE 802 LMSC, several WGs and study groups conduct research and engage in direct technical standards development, which focuses on technologies on ISO-OSI layers 1 and 2 for local and metropolitan area networks.

Since local and metropolitan area networks are among the primary application areas for IT and OT networks, such as networks for FA or the automation of public transportation systems; the technologies that are specified here are of great importance to automation and to IT networks. Since both IT and OT LAN and MAN area networks are based on the same technology, this creates a technological bridge between the two worlds that facilitate coexistence and convergence.

Many of the standards specified by IEEE 802 have been adopted in the IT, as well as in the OT world. The WGs that are listed in Table 1 are of particular importance.

Especially with standards development in recent years, the IEEE is providing technology offerings that are aimed at providing standardized solutions for ISO-OSI layers 1 and 2 both for the IT as well as for the OT space. Modern technology, such as TSN, was specifically developed to close existing gaps that, in the past, made the proliferation of IEEE 802 technology to mission-critical OT networks difficult.

Two technologies that are specified by IEEE 802 WGs are of special interest to the topic of IT and OT coexistence.

a) Focus technology—IEEE 802.1 time-sensitive networking: Ethernet has been in use in IT and datacenter environments for a long time—most of the advancements in Ethernet technology in the recent past concerned the constant increase in bandwidth demand. Standardization to reach higher bandwidths is an ongoing process, which is visible, for example, through recent study group working on 400-Gb/s Ethernet over multimode fiber [13].

Although the development of Ethernet as a high-bandwidth technology is ongoing, the IEEE 802.1 WG lately put a strong focus on the development of a set of standards aiming at dependability and bounded latency and jitter rather than bandwidth. This paper has been and is currently being performed by the IEEE 802.1 Time-Sensitive Task Group [14]. The scope of this new application to Ethernet technology is mission-critical control networks in cars, for example, for vehicular body control, and automation networks, for example, in FA or smart grids.

Bounded latency and dependability in Ethernet with TSN are realized by requiring all network participants to operate on distributed, synchronized clocks and by introducing new scheduling mechanisms in switches and end stations that base their operation on this common time frame. Time synchronization in the network is based on the IEEE 1588-2008 Precision Time Protocol [15] or one of the existing profiles. A key technology to achieve bounded latency is the IEEE 802.1Qbv-2015 Time-Aware Scheduler [16] by introducing a time-division multiple-access (TDMA) scheme into Ethernet. The assignment of frames to a particular time slice of the scheduler is based on the existing class-of-service prioritization in Ethernet. By using information that is already available in Ethernet frames before the introduction of TSN, backward compatibility is ensured.

The TSN technology extends the operational range of Ethernet from the factory backbone networks to the field, device, and machine levels of the factory, where bounded latency and jitter, as well as timing accuracy, are paramount.

TSN builds a strong bridge between the networks of the IT and of the OT world. With TSN, LAN, and MAN networks without boundaries or protocol gateways can be achieved. A standard Ethernet frame, in theory, can originate somewhere in the IT network, for example,

at a user, audit, or configuration PC workstation and can be transmitted seamlessly to the factory floor and—if necessary, reach as far as an individual sensor or controller on a production machine.

With TSN being an integral part of the basic Ethernet technology, IT and OT are based on the same transmission technology and can also immediately leverage new technological developments in IEEE 802 at the same time, for example, new physical layer transmission technology that is specified in IEEE 802.3.

Due to these significant benefits, many automation technologies are in the process of being converted from proprietary or partially proprietary ISO-OSI layers 1 and 2 transport technologies to TSN Ethernet. One example of this is Profinet@TSN by the Profibus Nutzerorganisation [17], and another example is Sercos International with Sercos over TSN [18].

b) Focus technology—Wireless LAN standard developments IEEE P802.11AX and P802.11AY: While wired communication is still dominating in IT as well as in OT networks, wireless technology is already an essential part of both worlds. Wireless, both in the IT and in the OT world, is based on the same IEEE 802.11 [19] set of standards. The differentiation between the two worlds is mainly on a design-level device. Wireless LAN access points and clients for industrial usage are often based on a ruggedized mechanical design and carry different approvals than IT access points, mainly for the use in rugged application scenarios as, for example, for the use on maritime vessels.

In the past, IEEE 802.11 standards were aimed at the IT, enterprise, and access technology space, whereas recent developments of the WG show a shift to also consider requirements from the OT world.

The standardization project P802.11ax [20] focuses on improving Wireless LAN performance and efficiency in high-density scenarios. This also includes interfering sources in the 2.4- and 5-GHz bands, a situation that is common both in the IT as well as OT world.

The project P802.11ay [21] focuses on the standardization of an enhanced throughput wireless technology on ISO-OSI layers 1 and 2, utilizing the license-free bands above 45 GHz. Again, this can be used in both the IT as well as in the OT world, covering use cases from low-range, ultrahigh bandwidth transmissions between mobile devices or mobile devices and infrastructure.

5) AVNU Alliance: The Avnu Alliance was founded in the wake of the IEEE 802.1 standardization on the audio and video bridging (AVB) specifications in 2009. The founding member companies [22] were mostly also active in the IEEE WGs and anticipated a need for an independent organization, outside the formal specification authorities, to bring the technology to market and to offer certification services for products. With the scope of AVB technology being on the markets of professional audio and video transport and home audio and video networks [23], these were also the focus markets of Avnu at its inception. With the further development of AVB into TSN by the IEEE 802.1 WG, the scope of the Avnu Alliance grew accordingly. At the time of writing of this paper, the Avnu Alliance specifies four target markets of interest [24], Automotive, Consumer, Pro Audio and Video, and Industrial Automation. Within these expanded fields of interest, Avnu WGs focus on the creation of product test and certification specifications that take into account the unique requirements of the different markets. While the Avnu Alliance started out as being the single source of AVB and TSN-related product conformity specifications for the industrial automation market, recent ongoing work within the joint IEEE/IEC 60802 WG now points to the IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE) [25] to provide these specifications and to disseminate them to testing and certifying laboratories. Subsequently, the work on test specifications is expected to shift from Avnu to IEC for the industrial automation market scope. Since the Avnu Alliance has not produced a final test specification for this market at the time of writing this paper, it is unclear whether existing draft specifications are transferred to IECEE or whether new specifications will be generated.

6) Industrial Internet Consortium: Membership in the Industrial Internet Consortium (IIC) is open to all interested parties. Its members represent large and small companies, entrepreneurs, academics, and government organizations interested in shaping and developing the industrial Internet. There are currently 19 WGs and teams, which are divided into 7 large areas. These groups are made up of representatives of the companies of the IIC. The member companies can assign an unlimited number of people to the WGs, who follow the rule "one vote, one company."

The IIC published the Industrial Internet Reference Architecture [26] first in 2015, known as the IIRA. This standards-based architectural template and methodology enables IIoT system architects to design their own systems based on a common framework and concepts.

The IIC activities have a strong focus on supporting brownfield use cases, thus allowing to retrofit existing automation equipment with the new technologies.

7) OPC Foundation: Initially, the acronym OPC was borne from object linking and embedding for process control. Technically limited to the Windows operating system, these OPC standard specifications, which are now known as OPC Classic, have enjoyed widespread adoption across multiple industries, including manufacturing, building automation, oil and gas, renewable energy and utilities, among others.

With the introduction of service-oriented architectures in manufacturing systems, new challenges in security and data modeling emerged. The OPC Foundation developed

the OPC UA (IEC 62541) [27] specifications to address these needs and, at the same time, provided a feature-rich technology open-platform architecture that is scalable and extensible. Today, the acronym "OPC" stands for Open Platform Communications.

The more than 600 OPC Foundation members vary greatly, from small system integrators to the world's largest automation and industrial suppliers.

Although OPC UA was, in the past, based on a client/server architecture, a more recent development focuses on the establishment of a publisher/subscriber scheme, called "OPC UA PubSub." This new specification was released as Part 14 of the OPC UA specification [28] in March 2018.

OPC UA "PubSub" focuses on device implementation that is very resource-efficient. The target is to expand the operational range of the OPC UA specification beyond its original aspect—process control on and above the controller level—into the field and device level. With the client/server architecture, the computational and memory resources that were needed to implement OPC UA would often overburden small sensors and controllers on the device or field level. With "PubSub," the OPC Foundation provides a specification that accommodates the requirements of devices below the controller level [29].

In parallel to the work of the PubSub group, an additional WG was started around the topic of using the newly available IEEE 802 TSN mechanisms with OPC UA and, in particular, OPC UA "PubSub." The focus of this new WG was on the PubSub specification because of two main reasons: the first was the feasibility for use in resource-constrained devices, which was also in the scope of TSN in industrial automation environments. The second reason was that the communication stream mechanisms that are specified by IEEE 802.1 on ISO-OSI layer 2 for AVB and TSN, called Multiple Stream Reservation Protocol, that are specified in IEEE 802.1Qat, and that are expanded upon in IEEE 802.1Qcc, are also based on a publisher–subscriber mechanism. In the TSN context, publishers are described as "Talkers" and subscribers are called "Listeners." Thus, it was concluded that a mapping of OPC UA on TSN-based automation networks is feasible and that a concise mapping between Layer 2 TSN streams and the higher layer OPC UA communication flows can be established with relative ease.

At the time of establishment of the OPC UA over TSN WG, the focus of the group was primarily on controller-to-controller communication, with no particular focus on extending to the field level of the automation network.

The scope of OPC UA over TSN was extended to the automation field level with an initiative by the OPC Foundation that was announced at the SPS trade show in 2018 and that was called OPC UA field-level communication (FLC). Vendor-neutral communication profiles are being defined based on OPC UA and TSN that specifically include field level topics, such as functional safety, motion control, and real-time (RT) communication [30].

For vertical integration from the sensor/actuator level in OT toward IT, a recent activity between the OPC foundation and the IO-Link consortium [31] has defined a companion specification to map IO-Link to OPC UA [32].

8) AutomationML e.V.: The Automation Markup Language (AutomationML) initiative was founded in 2006 by the automotive industry as an open industrial consortium and became a registered association in 2009. AutomationML e.V. welcomes all interested companies and research institutes to develop and maintain a freely available, open, and neutral XML-based industry data representation standard, which enables the exchange of engineering data across domain and vendor boundaries. Purpose of AutomationML e.V. is the promotion and further development of AutomationML to standardize data exchange in the engineering and operational processes of production systems.

a) Focus technology—Automation markup language: AutomationML is based on Computer Aided Engineering Exchange (CAEX) according to IEC 62424 [33] and basically is an interlinking format for established domain-specific modeling standards, such as for the representation of plant data in general and specific model perspectives such as structure, geometry, kinematics, and logic description. Additional representations for networks, mechatronic systems, and others are currently under development. The parts of AutomationML are internationally standardized within IEC 62714 [34]. It provides the framework to handle models of OT systems in IT-based applications as outlined in Fig. 3.

A recent initiative among AutomationML e.V., the IO-Link consortium, and the CC-Link Partner Association aims to define AutomationML as a fieldbus neutral language for device description files [35], [36] to overcome the limited modeling capabilities of the existing fieldbus device description formats, such as IODD, GSD, EDS, CSP+, and so on. For reasons such as backward compatibility and investment protection, the intention is not to necessarily replace these fieldbus formats but to

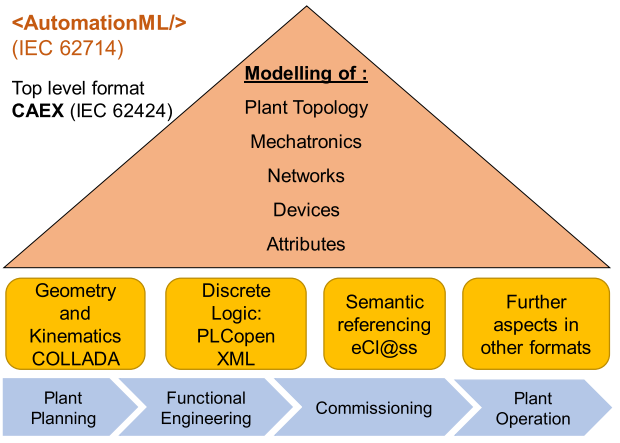

Fig. 3. ***Outline of AutomationML for the definition of plant data.***

Table 2 Examples of Norms and Standards Providing Properties for Submodels of the Administration Shell

Topic	Related standards
Administration Shell	IEC TR 62794 & IEC 62832 Digital Factory
Identification	ISO 29005 or URI Unique ID
Communication	IEC 61784-2 Real-Time-Ethernet (RTE)
Engineering	IEC 62714 AutomationML IEC 61360/ISO 13584 Standard data elements IEC 61987 Data structures and elements ecl@ss Database with product classes
Configuration	IEC 61804 EDDL, IEC 6253 FDT
Safety (SIL)	EN ISO 13849 EN/IEC 61508 Functional safety discrete EN/IEC 61511 Functional safety process EN/IEC Safety of machinery
Security (SL)	IEC 62443 Network and system security
Lifecycle Status	IEC 62890 Lifecycle
Energy Efficiency	ISO/IEC 20140-5
Condition Monitoring	VDMA 24582 Condition Monitoring

interlink them from an extendable AutomationML wrapper structure.

9) Standardization for "Industry 4.0" in Germany: For 160 years, the "Verein Deutscher Ingenieure" (VDI)—Association of German Engineers—has been providing important impulses for modern technologies and technical solutions. The VDI is the largest technical and scientific association in Germany and as the third-largest technical rule setter in Germany, an important partner for German industry and science.

The "Verband Deutscher Maschinen- und Anlagenbau" (VDMA) is the largest network organization for mechanical engineering in Europe. The association represents the common economic, technological, and scientific interests of this diverse industry. The VDMA is of particular interest to Industry 4.0 and the convergence of OT and IT due to the companion specifications that are provided to OPC UA. These specifications are intended to facilitate the integration of specific domain knowledge around VDMA key topics, such as robotics, into the OPC UA specifications.

The "Zentralverband Elektrotechnik- und Elektronikindustrie e.V." (ZVEI) is committed to advance the common interests of the electrical industry in Germany and on an international level. This commitment is supported by around 160 employees in the head office and over 5000 members of the member companies in an honorary capacity. Like the VDMA, the ZVEI plays an active role in the conceptual definition and promotion of the Industry 4.0 ecosystem [37], [38] and its underlying conceptual elements, such as the RAMI 4.0 model and the Asset Administration Shell (AAS). Their typical publications have the character of conceptual and promotional brochures and whitepapers rather than technical standards.

a) Focus technology—Administration shell: The AAS is a logical bridge between a physical OT asset and its representation in the IIoT world, sometimes also colloquially called a "digital twin." An own working subgroup "models and standards" has created the overview of relevant associated standards in Table 2. In November 2018, the consortium "Plattform Industrie 4.0" released a more detailed specification on the AAS [39]. Fig. 4 indicates the recommended main technologies for the AAS within the RAMI model.

III. CONVERGENCE OF OT AND IT

IT has a strong focus on agility and flexibility to build data processing systems, which are providing high-performance characteristics for specific tasks to be solved within the required response times. This is achieved by an open architecture: basically, anyone can communicate with anyone or anything through network connections. Being a major topic for the IT world, a clear strategy for cybersecurity is required and advanced cybersecurity technologies are utilized, for example, anomaly detection by continuous observation of the behavior of devices in a network, or a sophisticated patch management that monitors and handles the distribution of patches and software updates in regular intervals and in accordance to defined cybersecurity baseline definitions. The typical lifecycle of a system in IT is up to three years for hardware and up to five years for specific software.

OT has the goal to provide a useful function in a reliable and efficient way. The focus is on consistency of the information and continuity in the processing of automation. In the application field of PA, the typical investment in the technology is in the range of up to 30 years. In infrastructure OT such as building automation, energy distribution, or water treatment, we see OT installations that run for 30 years without any major change in the installed hardware and software. To allow this, OT systems are often isolated islands that are restricted for use by trusted communication partners and that are strictly separated from the open world. While more and more viruses and other malware are targeting OT networks specifically, sophisticated security mechanisms that take dynamic changes in the network into account are usually not utilized. This is done despite the fact that viruses such as StuxNet [72], [73] have demonstrated that the "air gap," the physical isolation of networks, is not a viable

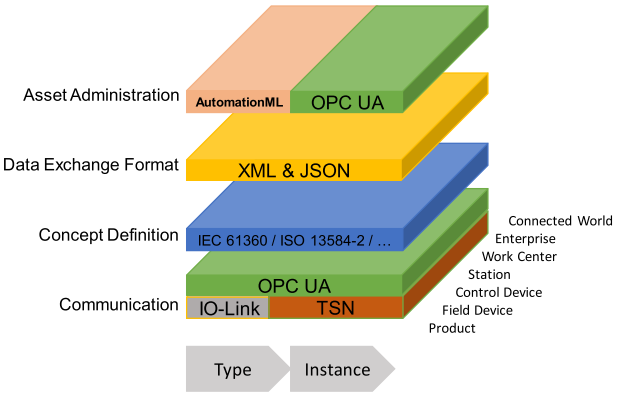

Fig. 4. ***Technologies for Industry 4.0 in the RAMI model.***

Table 3 Structure of IEC 62443 Industrial Communication Networks—Network and System Security and Potential Users

Product supplier	System integrator	Asset owner
develops IEC 62443-4-1	Integrates IEC 62443-2-4	operates IEC 62443-2-1 /-2-3 /-1-3
Product IEC 62443-4-2	Automation solution IEC 62443-3-3	Industrial automation and control system (IACS) IEC 62443-2-4
System, subsystem, or component such as applications, embedded systems, network components or host devices.	Includes a configured instance of the product and complementary hardware and software.	Operational and maintenance capabilities (policies and procedures)
Designed for intended environment(s)	Configured for intended environment	

security measure. The reasoning behind this is the stability of the systems: participating devices and users in the network are strictly limited and rarely change. The basic rule is: "never change a running system." However, there is a special focus on safety: the required functionality must be provided with a defined quality in a defined time under any circumstances.

A. Security

When connecting the worlds of IT and OT, the strong discrepancy between the cybersecurity postures of IT and OT raises some issues: OT is not prepared to be connected to the open world [40]–[44], [74], since security was previously not required in an isolated system. The first approaches to connect OT and IT networks gained a lot of attention due to frequently reported security-related incidents, such as industrial espionage or manipulations on production systems.

The OT must change its defensive posture: it needs to include basic security mechanisms that are part of the baseline security architectures of IT systems, such as access control, the authentication of user and devices, data encryption, and others. To enable this, a set of guidelines for product suppliers of automation devices, automation system integrators, and asset owners of an automation plant are collected in the IEC 62443 [45] set of standards as laid out in Table 3.

The challenge in practical applications is that security, in most cases, cannot be added to an existing network; it must be considered from the beginning and maintained through all stages of the system and network development. All aspects need to be taken into account, such as the security of the devices, into the system design and into the procedures of running and maintaining an automation plant. Just connecting the OT to the IT world and adding some additional security devices will not be successful in the long run.

An IT system is secured by separating different trust zones from the Internet with devices or mechanisms that implement different forms of access protection and filtering of communication flows. A common mechanism of performing the filtering function is a firewall. Firewalls allow and disallow traffic to and from one network zone into another zone, based on rules. Firewalls come in different levels of sophistication, spanning from pure stateless packet filters through stateful packet inspection firewalls to firewall functions that are application-aware and can enforce rulesets that are based on application protocol knowledge. Firewalls are also available in two different application characteristics: network firewalls and host firewalls. Network firewalls are devices that are placed inside the network at specific points to provide the filtering functions. Host firewalls are installed on a networked host device, such as a PC, and filter traffic at the host's network interface. While all of the sophistication levels and application characteristics are widely used in IT networks, firewalls are only slowly adopted in the OT world. Also, OT networks mostly utilize network firewalls due to the difficulty of implementing host firewalls on a closed embedded system, such as a programmable logic controller (PLC) or sensor.

IEC62443 introduces a concept called "Zones and Conduits": communication zones with similar security requirements are separated by conduits that implement checks and filter functions. By separating converged IT and OT networks into different security zones and implementing the appropriate security measure at the conduits, for example, firewalls, resilient network structures that follow the defense in depth approach can be built. Defense in depth is also a concept that is introduced through IT security and that is slowly being adopted in OT networks. Defense in depth is not a novel concept but was already used in the Middle Ages in the construction of castles: not a single wall is built for defensive purposes, but an overlying set of multiple defensive structures. By implementing defense in depth, the failure of one line of defense, for example, a firewall in a network, does not automatically compromise the entire network, but only one communication zone. Through stateful packet inspection firewalls, the OT network zones can receive additional protection by disallowing traffic, by default, from the IT to the OT part and allowing connections to be established from the OT to the IT zones.

In automation technology, most of the network protocols used for exchange of information to management level are based on the concepts and models of client–server communication (MMS/ISO 9506 [46]/OPC UA [28]/PROFINET [47], etc.). Under the assumption that the automation device is the holder of the information as a server, the client from outside cannot go through the firewall to access this information if the conduit disallows the connection from the client in one zone and the server in another zone.

IoT protocols are often using the publisher–subscriber model. Therefore, an automation device as publisher of information may simply access a subscriber, even if it is outside the trusted zone protected by a stateful

packet inspection firewall if it initiates the communication. New communication protocols must be adopted by the OT world to ensure they can be protected in a modern and secure network architecture.

B. Data Handling

To realize concepts like "Smart Factory," a connection between the production network with its devices and sensors (OT) to the Cloud with the data center (IT) is required. Automation devices in the OT typically communicate small amounts of information in short intervals. In applications for the PA, this can be in the range of a cycle of 100 ms down to a cycle of less than a millisecond in motion control applications for FA. The amount of available information can get easily into the range of gigabytes of data per second.

Edge computing is an optimization method for cloud computing systems to handle this data volume. Data processing, performing analytics, and knowledge generation take place near the source of the data, at the so-called "Edge." This reduces the communication bandwidth needed between sensors (OT) and the central datacenter (IT) and thus represents an important coexistence mechanism between OT and IT.

Depending on the application, the data collected on OT networks must be transferred to the cloud by suitable protocols. The cloud itself can reside in a remote server accessible via the public Internet or in a local server accessible via the local private network, sometimes called the "on-premise cloud." This interface between OT and IT is often realized by the so-called "Edge Gateways," which are usually the last physical instances before the cloud. They are part of the OT networks and are hardware and software components that monitor and control OT devices, processes, and events in RT.

C. Management Processes

IT/OT convergence, and thus the end-to-end management of IT and OT, requires that IT and OT strategies are harmonized, common governance and process models are installed, security and data are centrally managed, and human resources are skilled to understand and to know the requirements of both disciplines. Standards are required which can cover distinct levels of functionality as outlined in Table 4.

From a technical point of view, signals are transmitted with certain levels and temporal behavior. From these signals, data with a certain data type such as Integer16, Binary, or Float32 are formed by syntactic specifications. Only with the semantic meaning of these data does it become information such as "temperature of 20 °C." Only when this information is combined with each other, for example, where and when this temperature was measured, a complex application can be realized.

Table 4 Distinct Levels in Communication Specifications

	Level	Goal	Objects	Solutions
1	Technology	Data exchange	Signal	Data transmission protocol
2	Syntactic	Processing of transmitted data	Data	Standard formats of data (e.g. XML)
3	Semantic	Interpretation of transmitted data	Information	Common directories and keys
4	Functional	Interaction between different systems	Processes	Standard architecture, interfaces and models of processes

D. Real Time

In the OT, RT matters. An action provided by the automation system too late—or even too early—can lead to an erroneous state of the system. Therefore, a special class of communication networks dealing with RT was specified [48]. Today, these dedicated, low-cost fieldbuses are replaced more and more with RT Ethernet (RTE) solutions. IEC defined more than 20 of such RTE solutions [49], with distinct levels of performance and application fields, but with limited coexistence in one network. The market of these RTE systems has an annual growth of 22% and a market share of 52% of all industrial networks according to [50]. The previously mentioned OPC UA FLC initiative is expected to be a driver in consolidating the vendor-specific solutions into a single, unified automation network solution.

E. Ethernet-Based Networking and Protocols

RTE networks and protocols for communication in FA and process control systems provide the technical base for a coexistence and merger of protocols of the IT and OT world.

Table 5 provides an overview of protocols and technologies mapped to the distinct levels according to Table 4 and the mapping to the respective ISO/OSI-model layer.

The adoption of the IT protocols such as MQTT and AMQP allows for secure connections from the factory floor to automation cloud infrastructures. OPC UA is well-suited for machine-to-machine communication and defines the functional behavior of typical automation applications with the VDMA companion specifications.

Merging of OT and IT on an Ethernet network with TSN is a promising key technology for RT applications in the factory floor with cycle times at or below the range of milliseconds. Different OT solutions will give a competition to fill the semantic and functional gap of the actual IT solutions. While OPC UA FLC and TSN are expected to be a driver for further standardization toward one single OT networking technology that is used by multiple vendors, established OT ecosystems around RTE technologies such as EtherCAT or CC-Link IE will have to formulate long-term migration strategies for the communication portion of

Table 5 Overview of Different Protocols to Layers and Functional Levels

Layer	Level 1)	Information Technology IT	Operation Technology OT
Profile/User	Functional	e-mail etc.	Companion Standards like MTConnect, PLCOpen, AutomationML, Field Device Integration FDI, Analyzer Device Integration ADI
Application	Semantic	http	PROFINET, OPC UA, CIP (part of Ethernet/IP)
Presentation	Syntactic	XML, JSON	XML
Session	Communication	MQTT, AMQP, CoAP, HTTPS	HTTP
Transport		TCP/IP	TCP/IP, UDP,
Network			
Data Link		TSN	TSN, EtherCAT, Ethernet PowerLink, CC-Link IE
Physical		Ethernet	Ethernet, IO-Link

1) According to table IV

their solution. Thus, while the OT world has started consolidating on the wired network transport level, existing solutions will only slowly phase out due to the usual very long lifecycle of automation networks.

F. Wireless Networks

The coexistence of wireless communication systems in a factory floor is the basis for wireless RT networks to be able to meet the demanding hard-RT performance criteria required for field-level applications [51]–[53].

There is only a limited range of frequency bands available for free access, the so-called "Industrial Scientific Medical" (ISM) bands. These ranges have different properties and are used by different wireless network technologies. Most of the actual wireless technologies utilize the same 2.4-GHz band as listed in Table 6 [54].

1) WLAN: This is the acronym for "Wireless Local Area Network" and is the wireless radio specification that is based on the IEEE 802.11 standard documents series. WLAN is characterized by high data rates, supporting many network nodes and average ranges. Roaming of mobile nodes between infrastructure devices, called access points, is possible. Its disadvantages are nondeterministic communication, high bandwidth usage, and high-power consumption. For OT usage, it is especially suitable for soft- and non-RT critical tasks, such as human–machine interface (HMI) connectivity or bulk data transfer toward the backbone. However, in association with PROFINET, also deterministic communication between automation devices, even for safety-related applications, has been implemented with certain limitations.

Table 6 Wireless Standards and License-Free Frequency Bands

Frequency in MHz	Properties	Standards
433 .. 434	Good penetration, reduced data rate	
863 .. 870	Wide ranges	WIA-PA ?
2400 .. 2483,5	Available almost worldwide, broad bandwidth, already widely used	WLAN, Bluetooth, ZigBee, IO-Link Wireless, WirelessHART, ISA100.1, WIA-PA, WIA-FA
5150 .. 5350 5470 .. 5725	Low penetration of walls, quasi-optical propagation, high data rate. Required backoff-mechanism for radar prevents true real-time usage.	WLAN, WIA-FA

The frequencies used for WLAN within the license-free ISM bands are defined in the individual 802.11 standards documents. IEEE 802.11b and g use three nonoverlapping channels with a bandwidth of 22 MHz each in the 2.4-GHz band with gross data rates of 11 and 54 Mb/s, respectively.

IEEE 802.11h uses 19 nonoverlapping channels with a bandwidth of 22 MHz each in the 5-GHz band, also with a gross data rate of 54 Mb/s. WLAN provides data security during radio transmission by providing authentication and encryption features [WPA2, Advanced Encryption Standard (AES)]. The ongoing standardization project P802.11ax [20] focuses on improving WLAN performance in high-density scenarios and with radio interferers.

2) WIA-FA (IEC 62948): This is also based on 802.11 but defines dedicated mechanisms to improve RT capabilities for OT applications. It was initiated by the Chinese Industrial Wireless Alliance (CIWA). The Wireless Networks for Industrial Automation—Factory Automation (WIA-FA) protocol defines the physical layer (PHY), the data link layer (DLL), and the application layer. The PHY is based on the IEEE 802.11 physical layer, whereas DLL communication is based on TDMA, frequency-division multiple-access (FDMA), retransmission, and aggregation to guarantee RT, reliable, and secure communication between field and access devices.

3) Bluetooth: Bluetooth radio technology was initially standardized in accordance with IEEE 802.15.1 but later moved to the Bluetooth Special Interest Group (SIG). This technology uses an adaptive frequency-hopping spread spectrum (FHSS) technology with 1600 frequency hops per second to a maximum of 79 channels with a bandwidth of 1 MHz each, where many systems can be operated in parallel. This FHSS is a particularly rugged technology for industrial environments since it can cope well with effects such as multipath propagation in strongly reflecting environments. It, however, strongly interferes with other wireless systems in the same ISM band, especially WLAN. The Bluetooth SIG defined application profiles, for example, for voice transmission. In industrial applications, the serial port profile and personal area network application profiles for transparent Ethernet transmission are available for control and parameterization tasks. The technology features both authentication and encryption. The net data rate of approximately 700 kb/s is sufficient for these automation applications.

Newer versions of Bluetooth, such as Bluetooth Low Energy departed from utilizing the frequency band as defined in IEEE 802.15.1.

4) IO-Link Wireless: This is a novel standard for sensor/actuator communication in the range of a machine cell. It has taken special consideration regarding the fact that wireless communication systems like WLAN and Bluetooth used on the IT level may conflict with wireless systems used on the OT level. Neither WLAN nor Bluetooth provides sufficient coexistence mechanisms. IO-Link wireless (IOLW) provides dedicated mechanisms for the highest availability even in the context of such other wireless systems, interferers, and otherwise fading wireless channels.

IOLW was defined by the IO-Link consortium [55], [56] and works in the 2.4-GHz ISM band based on the frequency band utilization as defined in IEEE 802.15.1. A new RT capable concept for roaming of mobile devices between access points was defined in the context of IOLW [57].

A typical application scenario for these kinds of wireless systems in the OT world is the replacement of connector technology that is subject to wear and expensive maintenance, such as friction rings.

5) ZigBee: This was defined by the ZigBee Alliance based on the IEEE 802.15.4 standard for a gross data rate of 250 kb/s in the 2.4-GHz ISM band, with further channels with lower data transfer rates available in other bands. Zigbee has been optimized regarding energy consumption. Autonomous sensor nodes can achieve long operating times of up to several years without battery replacement, resulting in low data transfer rates. ZigBee supports the design of wide-coverage mesh and star topologies, supporting security and availability. Although the ZigBee Alliance addresses the complete automation sector, the standard is primarily established in the home and building automation sector.

The following 802.15.4-based standards are all targeting at the application area of process control field instrumentation and share many similarities but are incompatible to each other. They have been developed almost in parallel by different organizations. These 802.15.4-based wireless standards provide similar coexistence mechanisms, especially "listening before talk."

6) WirelessHART (IEC 62591): This was designed by the Highway Addressable Remote Transducer (HART) Foundation as the wireless expansion of the HART standard, for typical applications such as monitoring, diagnostics and slow control in PA [58]. To cover large plants with a small number of access points, the participants of a WirelessHART network provide a routing functionality, thus they are able to pass the data of other participants to the destination in the network. This results in alternative data paths so that no data losses occur, even with local radio interferences. The behavior of this network is controlled by a special software, termed "network manager." For example, the frequency occupation and the timings are controlled so that information can be transferred simultaneously between the participants on different paths.

7) ISA100.11a (IEC 62734): This was developed by the ISA. The official description is "wireless systems for industrial automation: process control and related applications." It shares many similarities with WirelessHART.

8) WIA-PA (IEC 62601): This was initiated by the CIWA and—although technically similar—claims performance advantages over WirelessHART and ISA 100.11a [59].

As for the main differences between these IEEE 802.15.4-based technologies, WirelessHART uses a fixed channel hopping table, whereas ISA100.11a and WIA-PA utilize multiple-channel hopping tables including the one used by WirelessHART. Medium access slot time is fixed at 10 ms for WirelessHART, whereas ISA100.11a and WIA-PA allow a variable slot time with a default of 10 ms. It must be noted that an identically configured slot timing is necessary for networks to interoperate. ISA100.11a uses the meshing protocol of IEEE 802.15.4e, whereas WirelessHART and WIA-PA use proprietary meshing protocols.

9) Automatic Identification and Data Capture: These systems are in a wider sense also OT wireless technologies, since they utilize technologies like radio frequency identification (RFID) or bar codes that are identified by optical readers to track tags attached to objects. ISO/IEC 20248 [60] specifies a method for data that are stored within a barcode and/or RFID tag, in order to be structured, encoded, and digitally signed. This information is then usually processed within IT systems. The purpose of the standard is to provide an open and interoperable method between services and data carriers to verify data originality and integrity in offline use cases.

10) Public Cellular Mobile Communication Systems: These systems with established technologies such as local thermal equilibrium (LTE) or WiMax (4G), Universal Mobile Telecommunications System (3G), and Global System for Mobile Communications (GSM) (2G) are used in both the IT and the OT domain. Use cases for cellular broadband modems in the OT world are well-established, that is, for remote monitoring and maintenance [61].

IV. PROBLEM-SOLVING APPROACHES

Convergence between the different systems and approaches is required and possible. We identify the possibility to get a common wired infrastructure based on Ethernet and TSN technology, a common handling of the available wireless bandwidth with a coexistence management, and a common modeling of data structures and device modules.

A. Ethernet Extended With TSN

Ethernet in its basic version is not RT capable. To overcome this, IEC defined different technologies from RTE [44] that also cover different profiles [2].

In the OT, we use two types of information. On the one hand, the transmission of process information is in RT so that the main task of controlling the physical process can be fulfilled. On the other hand, parameters, status messages, diagnostic information, and programs are increasingly also transmitted noncyclically on the same medium, only when required. This sporadic data exchange can be implemented also with typical IT protocols.

TSN is well suited for the separation of RT data and noncyclic data on an Ethernet network. Therefore, it is a key technology to allow a coexistence of IT and OT in the future. With the introduction of TSN, Ethernet technology as defined by IEEE becomes feasible for use in all aspects of OT. For the transmission of RT data, the existing OT protocols such as PROFINET [17] or SERCOS [18] will be adapted to utilize Ethernet with TSN as transport technology, with the outlook of further long-term convergence through OPC UA and TSN, including FLC, as announced at the SPS Trade Show in November 2018.

OPC has proven itself for the transmission of acyclic services in the OT. OPC UA has the potential to become the universal parameterization interface for noncyclic data.

B. Coexistence in Wireless Systems

If several wireless nodes want to use a common frequency band simultaneously, this can lead to medium access conflicts. In IT, the goal is to have these conflicts resolved by the nodes themselves, using appropriate protocols, that is, "Listen before Talk." This is, however, not feasible for hard RT communication in an automation environment, as unpredictable delays can occur.

The proposed solution for OT is the planning and supervision of the utilization of the individual frequency bands by the system integrator or operator. An approach to this has been summarized in IEC 62657 "Industrial communication networks—Wireless communication networks—Coexistence management." According to this standard, the coexistence management is mainly comprised of the following activities.

1) The registration of all radio applications in the company according to where is which radio system used and in which frequency range, who is responsible, what is the exact application, and how is the radio spectrum utilization in time.
2) The assessment of the coexistence situation prior to installation, and if necessary, minimization of radio influences.
3) Continuous checking during operation for compliance with the initial requirements of frequency management.

C. Outlook for Wireless Technology

Technology and standardization in communication networks is a highly dynamic topic with substantial potential for future developments from the commercial and IT side to influence the OT installations and networks. The fifth generation of mobile cellular networks, often abbreviated as "5G" networks, is such an example. 5G will succeed 4G (LTE/WiMax), 3G (UMTS), and 2G (GSM) systems. 5G targets improved performances such as higher data rate, reduced latency, energy saving, and connectivity for a large number of devices. 5G is currently in the specification phase within the Third Generation Partnership Project (3GPP) [61], with Release-15 completed by July 2018 for early commercial deployment [62]. Release-15 is centered around enhanced Mobile Broadband (eMBB), the successor technology to existing mobile broadband technologies. The second phase in Release-16 [63] is planned for March 2020, for submission to the ITU as a candidate for International Mobile Telecommunication system 2020 technology. With Release-16, the scope changes from Mobile Broadband to "massive IoT" and "Critical Communications." With this scope change, the 3GPP is expanding into new application areas and explicitly into the OT world, as shown in Fig. 5. As defined by ITU-R, the capability of 5G new radio (NR) is expected to enable new usage scenarios in both the IT and OT worlds, such as eMBB, ultrareliable low-latency communications, and massive machine-type communications. As one example, industrial control applications are in scope for the critical communications and mission-critical data requirements. This puts 5G as a potential technology contender to existing RT fieldbus and Ethernet systems [64]. To facilitate the migration of IT technology into OT space and to ensure that industrial automation requirements are understood and met, the ZVEI has initiated a WG, the 5G-Alliance for Connected Industries and Automation, to work with and contribute to the 3GPP standardization.

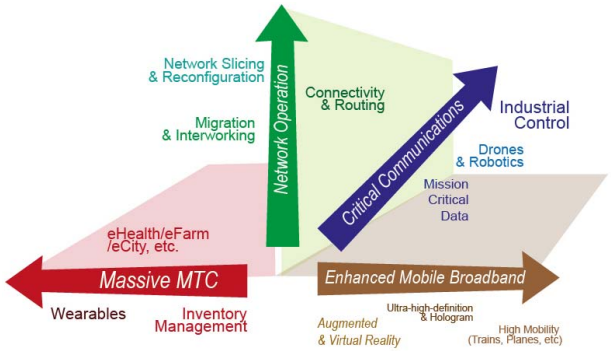

Fig. 5. *5G cellular networks scope [64].*

Depending on the technical feasibility to cover industrial applications, the impact potential of 5G Release-16 to existing OT technology is substantial [65]. The air interface defined for 5G is termed NR, supporting two frequency bands with different capabilities. The first frequency range FR1 lies below 6 GHz with a bandwidth of 100 MHz and a maximum modulation format of 256-QAM, thus similar to LTE-Advanced. The second frequency range FR2 between 24 and 86 GHz defines a

maximum channel bandwidth of 400 MHz, with possible aggregation of two channels. For Europe, the proposed frequencies range is 24.25–27.5 GHz. The maximum potential data rate supported is approximately 40 Gb/s. Multiple-input–multiple-output (MIMO) technology increases sector throughput and capacity density using large numbers of individually controlled antennas that may embed radio transceiver components, termed "massive MIMO."

D. EDGE Gateway

When the worlds of IT and OT are merged, it is not appropriate to simply interconnect both networks. Rather, it is recommended to use a so-called "Edge Gateway" as shown in Fig. 1.

The purpose of this edge gateway is to secure access from IT to the OT, that is, by firewall functionalities, to ensure the integrity of the OT in the automation network. On the other side, the IT network is protected from being flooded with cyclical process data from the OT network. OT data can be concentrated and condensed—thus preprocessed—by the Edge Gateway, so that basically only change notifications are transferred to the cloud. This reduces the demands for transmission and storage capacities, thus also the costs. These measures are often summarized with the term "Edge Computing." In 2019, a new industry consortium is organizing, the "Edge Computing Consortium Europe," with the primary goal to specify a reference architecture model for edge computing and the associated terminology [66].

E. Enterprise-Control System Integration

Abstract models are a helpful tool to comprehensively grasp the multidimensional complexity of horizontal, vertical, and lifecycle integration challenges within automation systems. Evolved from the well-known, but meanwhile outdated "Automation Pyramid" model, both the IIC and the Industry 4.0 initiatives have developed architectural reference models.

ANSI/ISA 95 [6] is an international standard for the integration of enterprise (IT) and control (OT) systems. Its models and terminology are structured and described using the unified modeling language. These models can serve as a base for the development of interfaces between IT and OT systems.

The ISA-95 standard addresses horizontal and vertical integration of activities in the value chain through the adoption of a level for each activity. Levels 3 and 4 IT are usually the domain of traditional IT functions on the office level, such as enterprise resource planning and manufacturing execution. The OT domain is usually placed in Levels 0 through 2, sometimes partially in Level 3.

The critical infrastructure protection (CIP) standards developed by the North American Electric Reliability Corporation (NERC) helps to bring IT and OT together by specifically addressing the security policy management and control-network visibility requirements of converged IT and OT infrastructure. The NERC CIP standards [67] are often applied in the form of IT and OT gateways that act as multilayer network security platforms.

V. CONCLUSION

One can recognize many standardization activities going on in the field of OT/IT convergence and coexistence. Major driving forces are both the German-based "Industry 4.0" initiative and the U.S.-based counterpart "IIC" [68]–[71]. Legal regulations that enable novel business models and ensure coexistence, as well as technical interoperability between the systems, are an important field of the activities. At this point of time, some challenges remain unsolved, which may not be of a technical nature and that are out of the scope of this paper. For example, there is yet clear legislature to be established on the topic of data ownership in a converged IT/OT network with different owners of the network and application infrastructure. Although there are still many challenges present, consolidation and a drive for coexistence can clearly be observed, especially on the communication level. Wired communication technologies are expected to converge from a multitude of existing approaches toward solutions that are based on IO-Link and TSN Ethernet with OPC UA. In particular, the convergence to standardized RTE is a strong supporting factor to converge IT and OT networks on a transport technology level and to interface with IT networks. Modern communication schemes that are introduced, for example, by OPC UA allow state-of-the-art security solutions to be established in OT networks. With wireless network solutions, the convergence is not as pronounced. This is partially due to the fact that some technical solutions are not fully defined yet. An example is an ongoing work in 5G networks and the still unclear position on the cellular network operators to enable OT operators to establish their own localized cellular infrastructure that operates in certain reserved frequency bands. The convergence path on wireless OT network technology in the future may be strongly influenced by the outcome to this ongoing discussion.

While IT/OT convergence paths are being established, the overall convergence will take some time due to the longevity of OT networks. With an operational cycle of 10 years or even longer in OT, convergence will not happen overnight but will be an ongoing process. While the technology is currently being established, the long-term convergence process is in line with another nontechnical development that has to happen for IT/OT convergence to be a success: engineers need to be educated and need to learn to converge IT and OT technologies in requirements, designs, opportunities, and constraints. The current convergence process allows for this change to happen and to make IT/OT convergence a lasting success. ■

REFERENCES

[1] M. Felser and T. Sauter, "The fieldbus war: History or short break between battles?" in *Proc. 4th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, Aug. 2002, pp. 73–80.

[2] M. Felser, "Real-time ethernet—Industry prospective," *Proc. IEEE*, vol. 93, no. 6, pp. 1118–1129, Jun. 2005.

[3] *IEC/IEEE 60802 TSN Profile for Industrial Automation*. [Online]. Available: https://1.ieee802.org/tsn/iec-ieee-60802-tsn-profile-for-industrial-automation/

[4] *IEC/IEEE 60802 TSN Profile for Industrial Automation*. [Online]. Available: http://www.iec.ch/dyn/www/f?p=103:38:15747970231351::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1376,23,100489

[5] L. Bello and W. Steiner, "A perspective on IEEE time sensitive networking (TSN)," *Proc. IEEE*, to be published.

[6] (2017). *ANSI/ISA 95, Enterprise-Control System Integration–Set of 25 Parts*. [Online]. Available: https://www.isa.org/isa95/

[7] B. Lydon. (Dec. 2016). IoT impact on manufacturing. ISA. Accessed: Jul. 6, 2018. [Online]. Available: https://www.isa.org/intech/20161201/

[8] Internet Engineering Task Force (IETF). *RFC Documents Series About the Internet*. Accessed: Jul. 16, 2018. [Online]. Available: https://www.ietf.org/standards/rfcs/

[9] *OASIS*. [Online]. Available: https://www.oasis-open.org/

[10] *Summary of the IEEE Organization*. Accessed: Feb. 2018. [Online]. Available: https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/organization_summary.pdf

[11] *The IEEE Computer Society Web Presence*. [Online]. Available: https://www.computer.org/

[12] *IEEE 802 LAN/MAN Standards Committee*. [Online]. Available: http://www.ieee802.org/

[13] IEEE P802.3cm 400 Gbit/s over Multimode Fiber Task Force, available at. [Online]. Available: http://www.ieee802.org/3/cm/index.html

[14] *Time-Sensitive Networking Task Group*, IEEE Standard 802.1. [Online]. Available: https://1.ieee802.org/tsn/

[15] *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*. IEEE Standard 1588-2008. [Online]. Available: https://standards.ieee.org/findstds/standard/1588-2008.html

[16] *IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks—Amendment 25: Enhancements for Scheduled Traffic*, Standard 802.1Qbv-2015, Amendment to 802.1Q-2014 as amended by 802.1Qca-2015, 802.1Qcd-2015, and 802.1Q-2014/Cor 1-2015. [Online]. Available: http://standards.ieee.org/findstds/standard/802.1Qbv-2015.html

[17] Profinet and TSN. Karlsruhe, Germany. *Profibus and Profinet International (PI)*. [Online]. Available: https://www.profibus.com/technology/industrie-40/#tab2-218039

[18] Sercos International. Süßen, Germany. *Ethernet TSN Heralds a New Era of Industrial Communication*. [Online]. Available: https://www.sercos.org/fileadmin/user_upload/Ethernet_TSN_heralds_a_new_era2.pdf

[19] *IEEE 802.11 Wireless Local Area Networks—The Working Group for WLAN Standards*. [Online]. Available: http://www.ieee802.org/11/

[20] *IEEE P802.11 Task Group AX–High Efficiency (HE) Wireless LAN Task Group*. [Online]. Available: http://grouper.ieee.org/groups/802/11/Reports/tgax_update.htm

[21] *IEEE P802.11 Task Group AY–Enhanced Throughput for Operation in License-Exempt Bands Above 45 GHz*. [Online]. Available: http://www.ieee802.org/11/Reports/tgay_update.htm

[22] *Avnu Alliance Member Overview*. Accessed: Dec. 13, 2018. [Online]. Available: https://avnu.org/our-members/

[23] *Avnu Alliance Frequently Asked Questions (FAQ)*. Accessed: Dec. 13, 2018. [Online]. Available: https://avnu.org/faqs/

[24] *Avnu Alliance Markets Overview*. Accessed: Dec. 13, 2018. [Online]. Available: https://avnu.org/markets/

[25] *IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)*. Accessed: Dec. 2018. [Online]. Available: https://www.iecee.org/index.htm

[26] Industrial Internet Consortium. (Jan. 31, 2017). *Industrial Internet Reference Architecture Technical Report, Version 1.8*. Accessed: Jul. 10, 2018. [Online]. Available: http://www.iiconsortium.org/IIRA

[27] *OPC Unified Architecture, Part 1 to 13*, document IEC 62541, Int. Electrotechnical Commission, Geneva, Switzerland, 2016.

[28] OPC Foundation. *OPC Unified Architecture–Specifications Overview*. [Online]. Available: https://opcfoundation.org/developer-tools/specifications-unified-architecture

[29] OPC Foundation. *OPC Unified Architecture—Part 14: PubSub*. Accessed: Dec. 14, 2018. [Online]. Available: https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-14-pubsub/

[30] D. Bruckner *et al.*, "An introduction to OPC UA TSN for industrial communication systems," *Proc. IEEE*, to be published.

[31] IO-Link Community. Karlsruhe, Germany. *IO-Link System Description–Technology and Application*. Accessed: Mar. 2018. [Online]. Available: http://io-link.com/share/Downloads/At-a-glance/IO-Link_System_Description_eng_2018.pdf

[32] IO-Link Community. *OPC UA for IO-Link Companion Specification Draft Version 0.3.5*. Accessed: Jul. 2018. [Online]. Available: http://io-link.com/share/Downloads/OPC_UA/OPC-UA_for_IO-Link_10212_d035_Jul18.pdf

[33] *Representation of Process Control Engineering–Requests in P&I Diagrams and Data Exchange Between P&ID Tools and PCE-CAE Tools*, document IEC 62424, International Electrotechnical Commission, Geneva, Switzerland, 2016.

[34] *Engineering Data Exchange Format for Use in Industrial Automation Systems Engineering—Automation Markup Language–Three Parts*, document IEC 62714, Int. Electrotechnical Commission, Geneva, Switzerland, 2018.

[35] R. Drath and M. Rentschler, "Modeling and exchange of IO-link configurations with automationML," in *Proc. CASE*, Munich, Germany, Aug. 2018.

[36] M. Rentschler and R. Drath, "Vendor-independent modeling and exchange of fieldbus topologies with automationML," in *Proc. ETFA*, Torino, Italy, Sep. 2018.

[37] R. Drath and A. Horch, "Industrie 4.0: Hit or hype? [industry forum]," *IEEE Ind. Electron. Mag.*, vol. 8, no. 2, pp. 56–58, Jun. 2014.

[38] R. Rosendahl, N. Schmidt, A. Lüder, and D. Ryashentseva, "Industry 4.0 value networks in legacy systems," in *Proc. IEEE 20th Conf. Emerg. Technol. Factory Autom. (ETFA)*, Luxembourg, Sep. 2015, pp. 1–4.

[39] Details of the Asset Administration Shell. Berlin, Germany. *Federal Ministry for Economic Affairs Energy (BMWi)*. Accessed: Nov. 2018. [Online]. Available: https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/2018-verwaltungsschale-im-detail.pdf

[40] S. Higginbotham. (Jun. 20, 2018). 6 reasons why IoT security is terrible. IEEE Spectrum. Accessed: Jul. 2, 2018. [Online]. Available: https://spectrum.ieee.org/telecom/security/6-reasons-why-iot-security-is-terrible

[41] M. Waidner and M. Kasper, "Security in industrie 4.0-challenges and solutions for the fourth industrial revolution," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Dresden, Germany, Mar. 2016, pp. 1303–1308.

[42] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, San Francisco, CA, USA, Jun. 2015, pp. 1–6.

[43] T. Meany, "Functional safety and industrie 4.0," in *Proc. 28th Irish Signals Syst. Conf. (ISSC)*, Killarney, Ireland, Jun. 2017, pp. 1–7.

[44] M. Ehrlich, L. Wisniewski, H. Trsek, and J. Jasperneite, "Modelling and automatic mapping of cyber security requirements for industrial applications: Survey, problem exposition, and research focus," in *Proc. 14th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, Imperia, Italy, Jun. 2018, pp. 1–9.

[45] *Industrial Communication Networks-Network and System Security—Part 1-1: Terminology, Concepts and Modelss*, document IEC 62443-1-1, Int. Electrotechnical Commission, Geneva, Switzerland, 2009.

[46] *Industrial Automation Systems–Manufacturing Message Specification (Withdrawn)*, Standard ISO 9506, 2003.

[47] *Industrial Communication Networks-Fieldbus Specifications—Part 5-10: Application Layer Service Definition-Type 10 Elements*, document IEC 61158-5-10, Int. Electrotechnical Commission, Geneva, Switzerland, 2014.

[48] *Industrial Communication Networks–Profiles—Part 1: Fieldbus Profiles*, document IEC 61784-1, Int. Electrotechnical Commission, Geneva, Switzerland, 2014.

[49] *Industrial Communication Networks-Profiles—Part 2: Additional Fieldbus Profiles for Real-Time Networks Based on ISO/IEC 8802-3*, document IEC 61784-2, Int. Electrotechnical Commission, Geneva, Switzerland, 2014.

[50] HMS Industrial Networks. (Feb. 16, 2018). *Industrial Ethernet is Now Bigger Than Fieldbuses*. Accessed: Jul. 3, 2018. [Online]. Available: https://www.anybus.com/about-us/news/2018/02/16/industrial-ethernet-is-now-bigger-than-fieldbuses

[51] A. Frotzscher *et al.*, "Requirements and current solutions of wireless communication in industrial automation," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2014, pp. 67–72.

[52] H. Hayashi, "Standardization of coexistence management for industrial wireless," in *Proc. SICE Annu. Conf. (SICE)*, Akita, Japan, Aug. 2012, pp. 693–696.

[53] D. Schulze, L. Rauchhaupt, and U. Jumar, "Coexistence for industrial wireless communication systems in the context of industrie 4.0," in *Proc. Austral. New Zealand Control Conf. (ANZCC)*, Gold Coast, QLD, Australia, Dec. 2017, pp. 95–100, doi: 10.1109/ANZCC.2017.8298492.

[54] ZVEI-German Electrical and Electronic Manufacturers Association. (Apr. 2009). *Coexistence of Wireless Systems in Automation Technology*. Accessed: Jul. 4, 2018. [Online]. Available: https://www.i40solutions.com/app/download/626079/zvei+coexistence+of+wireless+systems+in+automation+technology.pdf

[55] IO-Link community. *IO-Link Wireless System Extensions V1.1*. Accessed: Mar. 2018. [Online]. Available: http://io-link.com/share/Downloads/System-Extensions/IO-Link_Wireless_System_10112_V11_Mar18.pdf

[56] R. Heynicke *et al.*, "IO-Link Wireless enhanced factory automation communication for Industry 4.0 applications," *J. Sensors Sensor Syst.*, vol. 7, no. 1, pp. 131–142, 2018. doi: 10.5194/jsss-7-131-2018.

[57] M. Rentschler, "Roaming in wireless factory automation networks," in *Proc. IEEE 22nd Int. Conf. Emerg. Technol. Factory Automat. (ETFA)*, Sep. 2017, pp. 1–4. doi: 10.1109/ETFA.2017.8247723.

[58] S. Petersen and S. Carlsen, "Performance evaluation of WirelessHART for factory automation," in *Proc. IEEE Conf. Emerg. Technol. Factory Autom.*, Mallorca, Spain, Sep. 2009, pp. 1–9, doi: 10.1109/ETFA.2009.5346996.

[59] M. Zheng, W. Liang, H. Yu, and Y. Xiao, "Performance analysis of the industrial wireless networks standard: WIA-PA," in *Mobile Networks and Applications*. New York, NY, USA: Springer, 2015, doi: 10.1007/s11036-015-0647-7.
[60] *Information Technology–Automatic Identification and Data Capture Techniques–Data Structures–Digital Signature Meta Structure*, International Electrotechnical Commission, Geneva, Switzerland, Standard ISO/IEC 20248, 2018.
[61] *3RD Generation Partnership Project*. [Online]. Available: http://www.3gpp.org/
[62] *3GPP Release 15*. [Online]. Available: http://www.3gpp.org/release-15
[63] *3GPP Release 16*. [Online]. Available: http://www.3gpp.org/release-16
[64] *5G Requirements Study From the 3GPP*. [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1786-5g_reqs_sa1
[65] *ZVEI Working Group 5G-Alliance for Connected Industries and Automation (5G-ACIA)*. [Online]. Available: https://www.5g-acia.org/
[66] *Edge Computing Consortium Europe (ECCE)*. [Online]. Available: https://ecconsortium.eu/
[67] *NERC CIP Standards*. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[68] P. Madhusudan. (2017). *Interoperability Between IIC Architecture & Industry 4.0 Reference Architecture for Industrial Assets*. Accessed: Jul. 2, 2018. [Online]. Available: https://www.infosys.com/engineering-services/white-papers/Documents/industrial-internet-consortium-architecture.pdf
[69] S. Mellor and S.-W. Lin. (Dec. 5, 2017). *Architecture Alignment and Interoperability*. Accessed: Jul. 2, 2018. [Online]. Available: https://www.iiconsortium.org/pdf/JTG2_Whitepaper_final_20171205.pdf
[70] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the Internet of Things and industry 4.0," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 17–27, Mar. 2017.
[71] A. Torkaman and M. Seyyedi, "Analyzing IoT reference architecture models," *Int. J. Comput. Sci. Softw. Eng.*, vol. 5, no. 8, p. 154, Aug. 2016.
[72] *Common Vulnerabilities and Exposure (CVE) Entry on StuxNet*. [Online]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568
[73] Langner. *Ralph–Technical Analysis of StuxNet*. [Online]. Available: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
[74] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 277–293, Feb. 2013.

ABOUT THE AUTHORS

Max Felser (Senior Member, IEEE) received the B.Sc. degree from the Ecole Ingénieur de Fribourg, Friborg, Switzerland, and the M.Sc. degree in electrical engineering from ETH Zürich, Zürich, Switzerland.

He was with the Telecom Industry, Ascom AG, Bern, Switzerland, as a Group Leader for system design. He was with the Automation Industry, SAIA Burgess AG, Murten, Switzerland, as the Head of the PLC development division. Since 1991, he has been a Professor with the Berne University of Applied Sciences, Burgdorf, Switzerland, where he teaches system design, automation technology, and industrial networks. He runs the fieldbus laboratory recognized as Profibus and Profinet competence and training center by Profibus International, Karlsruhe, Germany. He is currently the Head of the Division of Electrical Engineering and Information Technology, Bern University of Applied Sciences BFH. His current research interests include industrial networks, real-time communication, and fieldbuses.

Mr. Felser has been a member of the National Committee TC65 of IEC since 1989 (as the Chairman from 2007 to 2012), responsible for the standardization of automation technology. He was the Chairman of Profibus Switzerland from 1992 to 2015 and the Coordinator of all Profibus and Profinet Competence Centers in Profibus International from 2003 to 2013. He was a recipient of the Fellow Membership of Electrosuisse.

Markus Rentschler (Senior Member, IEEE) was born in Freudenstadt, Germany, in 1965. He received the Dipl.-Ing. degree (Hons.) in communications technology from the University of Applied Sciences, Constance, Germany, in 1992, and the M.Sc. degree in digital systems engineering from Heriot-Watt University, Edinburgh, U.K., in 1993.

From 1994 to 1998, he was a Software Engineer with Alcatel-SEL, Stuttgart, Germany, where he was involved in developing protocol stacks for GSM communication systems. From 1999 to 2013, he was a Software Engineer for Ethernet- and TCP/IP-based protocols and the Head of the Research and Development System Testing Department, Hirschmann Automation and Control GmbH, Neckartenzlingen, Germany. Since 2010, he has been a Part-Time Lecturer of software engineering with Cooperative State University, Stuttgart. In 2013, he joined Balluff GmbH, Neuhausen, Germany, as the Head of development for networking products. His current research interests include industrial communication networks and protocols, especially wireless and redundancy. He is regularly publishing on these subjects and is also involved in a range of industry consortia and standardization activities, recently with the OPC Foundation, AutomationML, and IO-Link.

Oliver Kleineberg (Member, IEEE) was born in Esslingen, Germany, in 1978. He graduated from the Esslingen University of Applied Sciences in computer engineering, Esslingen, and received the Ph.D. degree in computer engineering from the University of Limerick, Limerick, Ireland.

In 2007, he joined Hirschmann Automation and Control GmbH, Belden's Industrial Networking Business Unit, Neckartenzlingen, Germany, where he was involved in project management, supply chain management, and advance development and is currently the Industrial Networking CTO. He has been involved in numerous standardization bodies, including the IEC and IEEE 802 groups, and fault-tolerant and real-time industrial communication specifications, including the ongoing TSN standardization efforts in IEEE 802.1 and IEEE 802.3.