Computer Communication Within Industrial Distributed Environment—a Survey

Piotr Gaj, *Member, IEEE*, Jürgen Jasperneite, *Senior Member, IEEE*, and Max Felser, *Member, IEEE*

***Abstract*—Nowadays, computer systems are presented in almost all types of human activity and they support any kind of industry as well. Most of these systems are distributed where the communication between nodes is based on computer networks of any kind. Connectivity between system components is the key issue when designing distributed systems, especially systems of industrial informatics. The industrial area requires a wide range of computer communication means, particularly time-constrained and safety-enhancing ones. From fieldbus and industrial Ethernet technologies through wireless and internet-working solutions to standardization issues, there are many aspects of computer networks uses and many interesting research domains. Lots of them are quite sophisticated or even unique. The main goal of this paper is to present the survey of the latest trends in the communication domain of industrial distributed systems and to emphasize important questions as dependability, and standardization. Finally, the general assessment and estimation of the future development is provided. The presentation is based on the abstract description of dataflow within a system.**

***Index Terms*—Cellular, communication, dataflow, dependability, industrial distributed systems, industrial networks, models, requirements, rte, standardization, wireless.**

I. Introduction

SINCE automation systems become indispensable means to obtain more sophisticated products with a better quality and lower costs than the manually-controlled ones, the computers' involvement in being their part is constantly growing, in not necessary a linear way. Computer bonds with industrial systems exist on the process level as well as on any higher level of data exchange model described in [1], [2]. Although most considered issues refer to control systems with real-time (RT) abilities, there are also described techniques dedicated to any other levels of the mentioned model. In RT systems, every single physical signal either used to control actuators or to collect data from sensors must be processed by some kind of natural or artificial intelligence. Currently, a human acts as an automation system designer, builder, and finally user. But the role of the main controller is assigned to a computer. From a historical point of view, computers were used in automation but in the early stage they only acted as rather powerful ones used as centralized processing stations, and mutually as the nodes of decentralized systems, commonly named DCS (Distributed Computer Systems). The main role in this case was continuous control of an industrial process. Circuits dedicated to discrete control were designed based on relays, and following the progress, they were transformed into PLC (Programmable Logic Controller) devices constructed as relatively simple computers [3]. At this time, the differences between computers used in DCS and as PLC faded out. Sometimes, exactly the same hardware base is used in both cases. Another group of computers as PC (Personal Computer), IPC (Industrial Personal Computer), HMI (Human Machine Inferface), and other, equipped with human interfaces, is mostly considered as points of information exchange between the digital system and a human [4]. However, using such devices on the factory floor provides problems with proper timelining [5].

Currently, industrial distributed systems are characterized mostly by the distribution of hardware, software, and physical components for the implementation of control and automation systems [6], [7]. In the paper, the usage of this kind of computer systems is considered. In such a case, the human knowledge referring to the given industrial process is embedded in the form of system and data structure and in processing algorithms applied among physical resources of distributed computers, where the control function may be freely distributed to different computers. As processing resources are territorially dispatched, there is a great necessity to assure the connectivity in order to exchange events and data between them. Currently, there are no other ways to do this than using (industrial) data networks. Thereby, they became a crucial part of distributed systems due to providing unnecessary resources allowing running the whole system. Networked control systems are used in application areas including factory automation, process automation, building automation, automotive systems, energy distribution system, etc. The usage of industrial data networks in such domains should always be done with consideration of time. On the mentioned control level, there is a set of information represented as part of system data, which interacts directly with the physical automation objects, i.e., with the physical process. It causes that all system components, including the network and its computer nodes with their hardware and software infrastructure, should work in real-time mode. Therefore, the main discriminant of industrial networks is the ability for temporal deterministic behavior. It means that all network activities are subjected to time limitations in the range from minimum achievable to maximum allowable duration time. However,

Manuscript received January, 2012; revised June, 2012; accepted June 09, 2012. Date of publication July 20, 2012; date of current version December 19, 2012. Paper no. TII-12-0061.

P. Gaj is with the Institute of Informatics, Silesian University of Technology, Gliwice 44-100, Poland (e-mail: piotr.gaj@polsl.pl).

J. Jasperneite is with the inIT-Institute Industrial IT, Ostwestfalen-Lippe University of Applied Sciences, and Fraunhofer IOSB-INA, 32657 Lemgo, Germany (e-mail: juergen.jasperneite@hs-owl.de).

M. Felser is with the Berne University of Applied Sciences, CH-3400 Burgdorf, Switzerland (e-mail: max.felser@bfh.ch).

Digital Object Identifier 10.1109/TII.2012.2209668

there are also various areas in industry where a particular attitude to time constraints depends on requirements from the application. It is especially noticeable when one takes into consideration the inter-system integration process and the remote access ability within a heterogeneous environment. Therefore, within the current networked control systems (NCS) the soft RT communication solutions are also desirable, including even the ones which operate within the public zone.

II. Application Properties

The industrial environment is invariant, contrary to the desktop and business ones. There are at least a few important features which determine the way the systems are constructed and operated. The following section discusses what is happening under the hood based on a few of such features.

The characteristics of information representation (coding), its mapping (storage and transfer), and processing (algorithms) in a given technological process are constant. The expectations of the NCS result from these characteristics and from operations which can be done for the technological process and in favor of a user. The set of typical NCS functionalities is fixed to data acquisition, control, supervision, monitoring, diagnostics, etc. In the domain of industrial communications, there is also a **limited number of abstract activities**. The typical kind of data exchange is a cyclic one based on a predefined scheme. It is used to treating the cyclic exchanges as the main industrial network activity due to the simple assurance of the time and spatial data consistency yielded by indigenous retransmission ability. The need for acyclic exchanges on demand also exists, but this kind of data transmission is always subordinated to the schema of the cyclic ones. Thus, the cyclic and acyclic updates in the local or remote scope can be simply distinguished as the main industrial network activities. It produces a situation where despite the variety of existing communication solutions, the main idea of its functioning is the same (Fig. 1). It is based on the cyclical network activity which is built on a schema working under one of a few existing and well-known network models (Master-Slave, Token Passing, Producer-Distributor-Consumer, Time Slicing, TDMA) in pure or combined versions. All network activities are executed within a network cycle which is in the form of one repeated time-window or repeated series of time-windows. Time-arrangement of activities within a cycle depends on the given schema of predefined cyclical actions and unpredictable acyclical events.

In most cases a distributed computer system working on the automation level does not need to be very fast from any point of view and in any meaning, but it needs to process data with hard or soft RT constraints as well as be run with an appropriate safety class. The system handles data which represents a state of the technological process and its own internal state as well. All data which is connected with the application can be called useful. From such a useful dataflow point of view, a system consists of a virtual application which is dispersed physically among system nodes and which real parts communicate with each other via the network. The useful data transmitted over the network is serviced by tasks related to the used protocol stack and is commonly called payload.

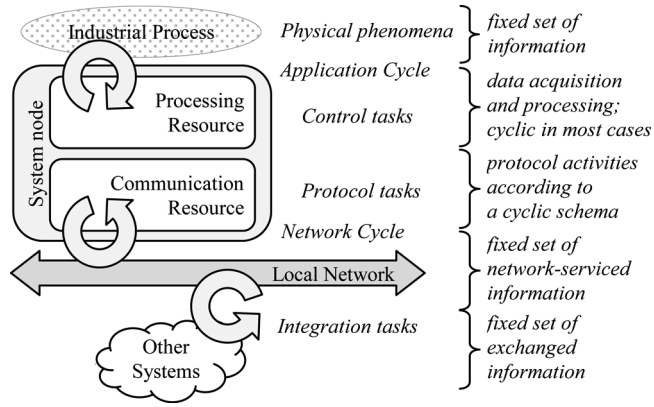

Fig. 1. Schema of a general dataflow and node activities within the NCS.

A. Asynchronous Tasks

The constituent application tasks are executed by the processing resources within system nodes, together with protocols tasks executed either in their independent network coprocessors or by appropriate processes within nodes. In any case, to ensure the temporal deterministic behavior, the task execution is controlled by time constrained software, e.g., RT operating systems. It leads to the characteristic dual-cycle dataflow in each system node (Fig. 1). The first cycle depends on a control task execution and the second one depends on the network activity. Both cycles are time-constrained, i.e., the cycle period is limited by the maximum value. The synchronization between the cycles is performed in the given moment in the time specified by the node operating system. It could be for example a special section of a PLC cycle or an interruption service.

B. Interconnection of Heterogeneous Subsystems

Another significant application requirement is the ability to integrate various systems on the horizontal level as well as vertically between other levels. The integration issue provides a bunch of questions described in [8]–[10]. The most important ones are connected with the heterogeneous nature of interconnected systems. A significant trend of integration is to connect remote systems via public networks in order to gain the maintenance accessibility or increase the interoperability of factory-wide and inter-branch systems. In such a case physical and functional distribution has a local and remote character. Note that available services differ, depending on the system scope of operation. Locally, the main task is to exchange useful data in a vertical and horizontal manner in order to extend the interoperability. It can be done with or without time constraints, according to process application requirements. During the integration the most important impact on the local run is to assure the proper dataflow, without interrupting a network cycle of a time-deterministic exchange scenario and without passing unwelcome or malicious traffic. Remotely, the main task is to collect data from the system in order to get the ability to present the system state, or to assure the input to the system. As mentioned previously, the time constraints are not reliable in this case and some activities should be deeply considered and secured. Security is the key aspect [11], [12]. Due to the non-deterministic character of the public channel and the fact that it is outside the

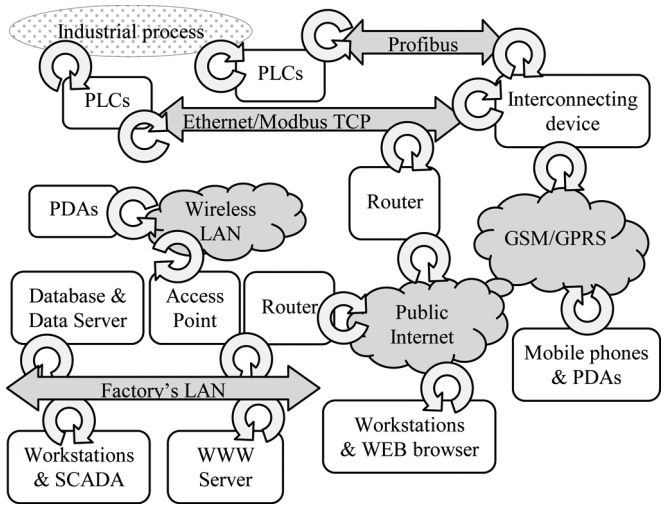

Fig. 2. General schema of the data passing in the example of NCS.

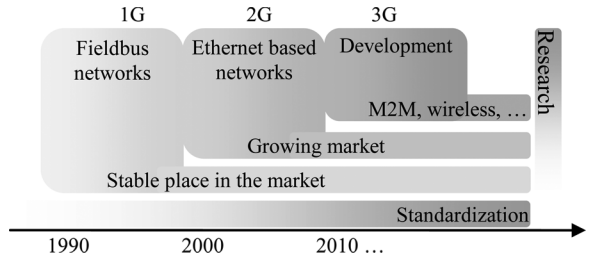

Fig. 3. Generations of industrial networks.

factory administrative area, only non-critical services should be executed. The typical ones are monitoring, database access, visualization, backup of alarm notification, remote support of data processing, parameterization, etc. [13], [14] Nonetheless, there are attempts to use the public network to execute control tasks [15]–[17]. Unfortunately, sometimes the available services and user requested ones do not match together at all. In any case, a redundant or multi-network approach can be useful: some examples are presented in [18]–[21].

As a sample of integration complexity and significance of this subject, a simple example of the real system is presented in Fig. 2. There are several remote visualizations and monitoring services connected via the GPRS/Internet network as well as local control executed on a PLC and on two independent industrial networks. In practice, there is often a need to create more complex systems.

Furthermore, in a contemporary industry there is also a strong obligation to be flexible for clients. It means that the likelihood that a given technology line or communication services (e.g., Fig. 2) are new or modified is quite high. Thus, despite the fixed character of the industrial process, the designers of IT systems are very keen to use network solutions with a high flexibility to rearrange the topology and dataflow. A good but not brand new one in this matter is the object-orientation approach [22], [23]. It allows reducing the reconfiguration effort during software and hardware parts change [24], [25] as well as simplifies the other aspects of system rearrangement: distribution range, general scalability, self-adaptive property, fault tolerance, availability of safety, and simplicity of maintenance [26].

III. Industrial Communications

In the following section, the current trends and problems in communication technologies in the context of industrial distributed environment are discussed.

A. Data Communication Models

Data between distributed automation systems is always exchanged based on different communication models. The classic message exchange between two distributed computers is flexible but hard to maintain in the long term. Therefore, in automation technology a memory mapping communication paradigm was developed and is widely used for centralized control with remote inputs and outputs (e.g., Profibus [27]). For vertical access, a Client-Server model following the Virtual Field Device approach was developed in ISO 9506 as the Manufacturing Message Specification (MMS) and copied and modified for most fieldbus and industrial Ethernet solutions. For horizontal communication between controllers inside a distributed automation system, additional paradigms had to be defined, mostly ones like publisher-subscriber or producer-consumer.

B. Industrial Networks

The broad range of environmental requirements mentioned above leads to many different industrial applications, which must be fulfilled by real-time communication systems. The most typical and common among them are fieldbus systems which are considered as the 1st generation of industrial networks. Currently, such solutions are no longer developed in a significant way but the existing ones are well described and documented as well as analyzed [2], [28], [29]. The main reason for stopping the development of the fieldbus technology seems to be reaching the maturity as well as the appearance of the 2nd generation of industrial networks known as Real-Time Ethernet. Additional reason can be also considered from development point of view. The uncommonness of existed protocol stack, especially including MAC and physical media leads to high costs of the infrastructure elements and difficulties with integration. Moreover, even if one takes into consideration the commonly used and standardized physical layers of fieldbuses, they are no longer attractive as they do not assure the required bandwidth and throughput. To clarify the situation it is important to emphasize that the 2nd generation is not introduced instead of 1st one. The fieldbus technology with low bandwidth will always have a place in NCS. But the new challenges require new generation of communication solutions.

The division of communication solutions into generations is quite a common procedure. In Fig. 3 the informal generations of industrial networks are shown.

Nowadays, as a response to mentioned issues, industrial automation vendors adopted the Ethernet technology to enable a real-time communication. Ethernet can assure the low cost and high data transfer speed by itself. Since the existing Ethernet (IEEE 802.3) cannot meet stringent timing requirements, many extensions have been introduced during the last decade

to improve the temporal deterministic behavior. These extensions try to cover key requirements that include implementation costs, IEEE 802.3 compatibility, configuration effort, and real-time performance [30]. Furthermore, these extensions are documented under IEC-61158 [29] as a reference for Real-Time Ethernet (RTE) based industrial communication technologies. A comprehensive survey of RTE variants and relevant standards and performance optimization in this field can be found in e.g., [28], [31]–[33].

The spontaneous development of fieldbus solutions in the 90s has led to the existence of a big variety of incompatible communication technologies. For a short period of time the RTE appeared as a chance to be a common platform for industrial communication. Unfortunately, due to the global market competition the result of RTE development is almost the same as in case of fieldbuses. There are dozens incompatible protocols available. Of course, from the research and general progress point of view, the diversity and competition are welcome. However, considering the dataflow in the current heterogeneous environment, the lack of common platform is onerous in practice for integrating engineers. Thus, the development of a universal solution is still in progress. For instance, projects as Virtual Automation Network [21] or quite small attempts as [20] can be emphasized.

The further development trend concerns the growing importance of multimedia applications and intersecting their requirements with the requirements of industrial applications. The Ethernet Audio Video Bridging (AVB) TG [34] is working to develop the existing Ethernet into a real-time capable Ethernet [35]. With AVB 1.0 it is possible to offer worst-case delays for all real-time message classes. This is a new quality in comparison to standard Ethernet, where only for the highest priority an upper bound can be denoted. Even if the worst-case latencies can be determined, the absolute values for the highest priority class are not smaller than those of standard Ethernet [36].

For a couple of years wireless technologies have been identified as a very attractive option for industrial distributed systems because of their flexibility and the reduction of cabling. The key challenges include: achieving a timely and reliable transmission despite channel errors, the creation of deterministic hybrid systems in which wireless stations are included in existing wired systems [10], [37] and addressing the variation of available bandwidth/latency for data traffic due to moving mobile devices [38]–[41]. Over the years, wireless communication technologies (e.g., the IEEE 802.11 Wireless LAN, the IEEE 802.15.x Wireless PAN) along with a considerable improvement of their performance [42], [43], have become a viable solution even for industrial environments. Solutions specifically designed for industrial application include wireless HART, Zigbee, and ISA100.11a that are mesh networks, which rely on the IEEE 802.15.4 WPAN (Wireless Personal Area Networks). Another protocol WISA is developed to provide a wireless connection of sensors and actuators in factory automation systems based on IEEE 802.15.1 Bluetooth. Moreover, due to strong need for connection of various and many wireless devices from automation, healthcare, office, and home there are some universal communication solutions established with the great aim of applying the Internet Protocol Version 6 (IPv6) into even very simple and small devices from our surroundings, including industrial environment. One of the well know concept is “Internet of Things”, and a representative technology is 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) which is based on IEEE 802.15.4 and defined in RFC4919 and RFC4944 [44]. All mentioned WPAN technologies are suitable for distributed systems constructed as a low power sensor networks e.g., applications for smart grid measurements. A comprehensive survey of wireless industrial technologies and related standards can be found in [45], [46]. In addition, [47] it presents a detailed overview of various states of art technologies and practices in industrial communication systems. Due to the dynamic growth of the wireless segment, and especially the low power personal area networks, it might be expected to be an interesting influence on the industrial computer systems. Unfortunately, technologies based on a radio transmission are prone to logical and physical disturbances. It is hard or even impossible to adapt such solutions into RT systems with time critical limitations. Hence, the precise impact is hard to estimate so far.

Another emerging branch of Industrial Communications is the use of public IP-based networks for interconnecting remote subsystems [21]. In the absence of other transmission media, such as dedicated lines, and/or wherever it would be too expensive to set up a dedicated radio network, data transmission via the mobile network could be an alternative solution [48].

GSM is developed by the European Telecommunications Standards Institute (ETSI) to describe technologies for the second generation (2G) digital cellular networks (developed as a replacement for first generation analog cellular networks). The standard was expanded over time to accommodate higher data transfer speeds via EDGE and succeeded by the third generation (3G) UMTS standard. In the road map, the fourth generation (4G) LTE advanced standard is now being rolled out. The future envisioned fifth generation (5G) wireless mobile systems are expected to provide global roaming across different types of wireless and mobile networks, for instance, from satellite to mobile networks and to WLANs [49].

Fig. 4 shows the round-trip time of a typical M2M (Machine-to-Machine) application, consisting of a remote programmable logic controller with a cellular modem as a data end point (DEP) and a plant control system as the Data Integration Point (DIP).

The measurements were performed over a period of five days for different cellular technologies offered by a German telecommunication provider. The round trip times indicate a relatively high jitter. The similar jitter problems were observed in [20]. The communication gap in connection between DEP and DIP was observed in range from several milliseconds up to several seconds in GPRS case. With respect to mission-critical M2M applications, the occurred service interruptions with a recovery time of up to several seconds must be evaluated as critical. It is the same problem as one mentioned previously in the case of public and radio networks, and the reason lies out of technical issues but is related to administrative scope and to susceptibility to disturbances. However, the acceptable jitter depends on application; hence, usage of cellular technologies strongly depends on application requirements.

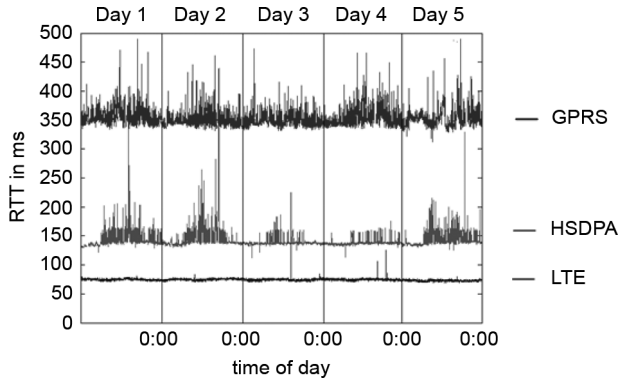

Fig. 4. Measurement results of the roundtrip times over a period of five days using 2G (GPRS), 3G (HSDPA) and 4G (LTE) cellular networks [48].

In the past few years, new wireless devices combined with the Internet have enabled plants to wirelessly collect data and make it available via the Web [50]. The growth of wireless networks and the ubiquity of cellular networks have made it far easier for Machine-to-Machine (M2M) communication to take place and has lessened the amount of power and time necessary for information to be communicated between machines [51]. These days M2M communication is already used for remote monitoring, control and automation of distributed networks [15], [52], [53].

As mentioned in the environmental description, the communication methods which operate in the public zone and provide really attractive services should not be used without a critical assessment. It is important to remember that such solutions are vulnerable to security threats as well as are not suited for hard-real time systems, even if used protocols potentially allow to keep time constraints. The engineers are not familiarized with such a danger because they have not faced it too often yet. Such communication ways are quite new. For the time being, due to the dependability requirements, the public zone should not be trusted.

C. System Dependability

According to current maintenance requirements the issue of communication should be considered wider then only tasks of data transfer. There is the term of dependability which is composed of safety, security, and availability of a distributed system [54]. Safety, according to the definition that it is "Freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment" [55], is an important feature for a DCS. Functional safety is a part of the overall safety that depends on the correct operation of DCS in response to its inputs.

The basic standard for functional safety related to DCS is the IEC 61508 [55] series of standards. In this series the DCS is defined as a programmable electronic system. The possible structure for hardware and software is defined, including the design process for safety related to DCS. The principle of safety is based on a risk assessment evaluating the risk of a failure of the distributed system [56]. In the sense of adding controlled redundancy in hardware and software, the system is made more error-tolerant, i.e., in case of errors in the system the system does not fail to provide the required function.

For the distributed control, also safe network protocols conforming to the requirements of functional safety are required. All the proposed solutions for safety-related networks are collected in the IEC 61784–3 [57] part standard. All these safety-related networks list possible errors as the source of failures, and show how the defined technical solutions ensure the integrity of the system. Typical methods are adding data numbers and additional redundancy, e.g., in the form of checksums. These measures can typically be implemented as software on top of a non-safe communication channel (black channel principle).

Functional safety of a DCS depends on the integrity of the DCS. This is also a security issue. With the adoption of more and more IT-based technology for DCS, like Ethernet and PC based controller, we see that virus, worms and other forms of malware are also getting into the range of automation systems [58]–[60]. Security—"the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional" is not only a problem of networking and the separation of networks with firewalls; it includes all types of measures to prevent the access of not permitted persons or software into a critical system.

With the usage of DCS in mission-critical systems, the availability—"ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided" gets more importance. In a DCS, not only the availability of the computers, but also the availability of the communication network is a key issue. One method of increasing the availability is to add redundancy to the transmission media of the network. In case of a failure of one resource, the system switches to the redundant resource. The grace time of the application defines how long the switchover time can be.

The application-independent media redundancy methods are collected in the IEC 62439 standards. It is not an efficient approach to simply double the complete network. A more efficient approach is the adoption of ring architecture which allows building a one error fault tolerant system with a simple, bumpless switchover mechanism [61]–[63]. A mesh network is more efficient, but the management and switchover procedures are almost impossible to handle in hard real-time in case of a resource failure. A survey of Real-time Ethernet Redundancy Methods can be found in [64].

D. The Necessity for Standardization

From the practical point of view the main task faced to engineers is to design and run the system which is able to service the industrial process properly. Accomplishing such a task is definitely easier when components are well defined. Standards and patents reflect the "state of the art" of a technology also from the legal point of view. If a technology is part of a standard, this does not mean that there is no patent involved. According to the Guidelines for Implementation of the Common Patent Policy it is possible to have international standards covering patents, as long as the patent holder is willing to negotiate licenses with other parties on a non-discriminatory basis on reasonable terms and conditions.

TABLE I
LIST OF IEC WORKING GROUPS AND STANDARDS RELATED TO DCS.

TC/SC-WG	Topic	Standard
TC65	Industrial-process measurement, control and automation	
TC65-WG 10	Security for industrial process measurement and control - Network and system security	IEC 62443
SC65A	System aspects	
SC65A-WG 14	Functional Safety Guide	IEC 61508
SC65B	Measurement and control devices	
SC65B-WG 7	Programmable control systems	IEC 61131
SC65B-WG 15	Function block	IEC 61499
SC65C	Industrial networks	
SC65C-WG 12	Functional Safety for Fieldbus	IEC 61784-3
SC65C-WG 13	Cyber Security	See TC65 WG10
SC65C-WG 15	High Availability Networks	IEC 62439
SC65C- WG 16	Wireless	IEC 62591 / 62601
SC65C- WG 17	Wireless Coexistence	IEC 62657
SC65C- MT 9	Maintenance Team for Fieldbus	IEC 61158, IEC 61784-1/2
SC65C- JWG10	Industrial Cabling	IEC 61784-5
SC65E	Devices and integration in enterprise systems	
SC65E- WG 4	Field device tool (FDT) interface specification	IEC 62453
SC65E- WG 7	Function blocks for process control and EDDL	IEC 61804
SC65E- WG 8	OPC unified architecture	IEC 62541

The International Electrotechnical Commission (IEC) is in charge of the definition of international standards in the domain of general automation technology. The Technical Committee TC65 is in charge of preparing "International standards for systems and elements used for industrial process measurement and control concerning continuous and batch processes" with 26 countries participating in and 15 observing this standardization process. The TC is split into several subcommittees (SC) and working groups (WG) as listed in Table I.

The definition of the protocols for Fieldbus and Real-Time Ethernet are located at the SC65C-MT9 maintenance team. Almost every year additional protocols are added to these standards. These protocols are listed as 'types' in the IEC 61158 and the IEC 61784–1/2 defines how to build compatible systems out of these types.

All aspects of System Dependability as described in the previous section are covered by the different Working Groups (WGs). In addition we find also WGs for programming (IEC 61131 & IEC 61499), engineering (IEC 62453 & IEC 61804) as well as for vertical integration (IEC 62541). Also the new wireless transmission systems and frequency allocation is included. Most of these standards are split into several parts and subparts and may be downloaded from the website of IEC (www.iec.ch).

IV. VIEWS OF THE FUTURE

Taking into consideration the variety and multiplicity of existing IT, even only the ones dedicated to strictly industrial computer systems, it is no problem to design and create a distributed system. However, to create a system in a proper way, which on the one hand is in accordance with process requirements and on the other hand with structural flexibility, together with a reasonable economic background, is a task not for a team consisting of one profession. Together with a standard automation team, industrial IT specialists are necessary, including people strongly involved in computer system architecture, networks and programming.

A general conclusion is that the time of monogenic and isolated systems is over as well as the dream about one universal and best technology for constructing computer systems in industrial environment.

On the one hand, the future vision of computer distributed systems in industry seems to be based on the utilization of various standardized technologies integrated together in order to dynamically choose the requested one in a given moment of time of system activity. Due to a big variety of industrial communication solutions as well as assuring high dependability, the further research for both emerging and well-known technologies should be focused on ways of the mutual usage of available protocols. The other way of evolution is to keep standardizing and to keep open all new and prospective solutions.

On the other hand, due to extending the NCS functionalities, the technologies of wireless and public network access seem to gain more importance in industry. The main impact is undoubtedly related to the remote and mobile access to the whole system and individual devices as well. It is hoped that system designers will do their best to assure a proper security level in this case.

REFERENCES

[1] G. Pratl, D. Dietrich, G. P. Hancke, and W. T. Penzhorn, "A new model for autonomous, networked control systems," *IEEE Trans. Ind. Inf.*, vol. 3, no. 1, pp. 21–32, Feb. 2007.

[2] T. Sauter, "The three generations of field-level networks—Evolution and compatibility issues," *IEEE Trans. Ind. Electron.*, vol. 57, no. 11, pp. 3585–3595, Nov. 2010.

[3] W. Bolton, *Programmable Logic Controllers*. New York: Newnes, 2009.

[4] J.-Y Fiset, *Human-Machine Interface Design for Process Control Applications*. New York: ISA, 2009.

[5] M. Cheminod, I. Bertolotti, L. Durante, P. Maggi, D. Pozza, R. Sisto, and A. Valenzano, "Detecting chains of vulnerabilities in industrial networks," *IEEE Trans. Ind. Inf.*, vol. 5, no. 2, pp. 181–193, May 2009.

[6] M. Shahraeini, M. Javidi, and M. Ghazizadeh, "Comparison between communication infrastructures of centralized and decentralized wide area measurement systems," *IEEE Trans. Smart Grid*, vol. 2, no. 1, pp. 206–211, Mar. 2011.

[7] A. Sendjaja and V. Kariwala, "Decentralized control of solid oxide fuel cells," *IEEE Trans. Ind. Inf.*, vol. 7, no. 2, pp. 163–170, May 2011.

[8] G. Cena, A. Valenzano, and S. Vitturi, "Hybrid wired/wireless networks for real-time communications," *IEEE Ind. Electron. Mag.*, vol. 2, no. 1, pp. 8–20, Mar. 2008.

[9] J. Ploennigs, M. Neugebauer, and K. Kabitzsch, "Diagnosis and consulting for control network performance engineering of csma-based networks," *IEEE Trans. Ind. Inf.*, vol. 4, no. 2, pp. 71–79, May 2008.

[10] T. Sauter, J. Jasperneite, and L. Lo Bello, "Towards new hybrid networks for industrial automation," in *Proc. ETFA IEEE*, Sep. 2009, pp. 1–8.

[11] Y. Xu, R. Song, L. Korba, L. Wang, W. Shen, and S. Lang, "Distributed device networks with security constraints," *IEEE Trans. Ind. Inf.*, vol. 1, no. 4, pp. 217–225, Nov. 2005.

[12] M. Cheminod, A. Pironti, and R. Sisto, "Formal vulnerability analysis of a security system for remote fieldbus access," *IEEE Trans. Ind. Inf.*, vol. 7, no. 1, pp. 30–40, Feb. 2011.

[13] N. Torrisi, "Monitoring services for industrial," *IEEE Ind. Electron. Mag.*, vol. 5, no. 1, pp. 49–60, Mar. 2011.

[14] A. Mercurio, A. Di Giorgio, and P. Cioci, "Open-source implementation of monitoring and controlling services for ems/scada systems by means of web services—Iec 61850 and iec 61970 standards," *IEEE Trans. Power Del.*, vol. 24, no. 3, pp. 1148–1153, Jul. 2009.

[15] A. Yazidi, H. Henao, G. Capolino, F. Betin, and F. Filippetti, "A web-based remote laboratory for monitoring and diagnosis of ac electrical machines," *IEEE Trans. Ind. Electron.*, vol. PP, no. 99, p. 1, 2011.

[16] J. Korniak, "The gmpls controlled optical networks as industry communication platform," *IEEE Trans. Ind. Inf.*, vol. 7, no. 4, pp. 671–678, Nov. 2011.

[17] A. Jestratjew, "Improving availability of industrial monitoring systems through direct database access," in *Computer Networks, Ser. Communications in Computer and Information Science*, A. Kwiecien, P. Gaj, and P. Stera, Eds. Berlin, Heidelberg: Springer, 2009, vol. 39, pp. 344–351.

[18] A. Willig, "Redundancy concepts to increase transmission reliability in wireless industrial lans," *IEEE Trans. Ind. Inf.*, vol. 1, no. 3, pp. 173–182, Aug. 2005.

[19] M. Short and M. Pont, "Fault-tolerant time-triggered communication using can," *IEEE Trans. Ind. Inf.*, vol. 3, no. 2, pp. 131–142, May 2007.

[20] P. Gaj, "The concept of a multi-network approach for a dynamic distribution of application relationships," in *Computer Networks, Ser. Communications in Computer and Information Science*, A. Kwiecien, P. Gaj, and P. Stera, Eds. Berlin, Heidelberg: Springer, 2011, vol. 160, pp. 328–337.

[21] J. Beran, P. Fiedler, and F. Zezulka, "Virtual automation networks," *IEEE Ind. Electron. Mag.*, vol. 4, no. 3, pp. 20–27, Sep. 2010.

[22] T. Cucinotta, A. Mancina, G. Anastasi, G. Lipari, L. Mangeruca, R. Checcozzo, and F. Rusina, "A real-time service-oriented architecture for industrial automation," *IEEE Trans. Ind. Inf.*, vol. 5, no. 3, pp. 267–277, Aug. 2009.

[23] R. Cupek, M. Fojcik, and O. Sande, "Object oriented vertical communication in distributed industrial systems," in *Computer Networks, Ser. Communications in Computer and Information Science*, A. Kwiecien, P. Gaj, and P. Stera, Eds. Berlin, Heidelberg: Springer, 2009, vol. 39, pp. 72–78.

[24] K. Thramboulidis, "Model-integrated mechatronics—Toward a new paradigm in the development of manufacturing systems," *IEEE Trans. Ind. Inf.*, vol. 1, no. 1, pp. 54–61, Feb. 2005.

[25] M. Schumacher, J. Jasperneite, and K. Weber, "A new approach for increasing the performance of the industrial ethernet system profinet," in *Proc. WFCS 2008*, May 2008, pp. 159–167.

[26] M. H. Kim, S. Lee, and K. C. Lee, "Kalman predictive redundancy system for fault tolerance of safety-critical systems," *IEEE Trans. Ind. Inf.*, vol. 6, no. 1, pp. 46–53, Feb. 2010.

[27] J. Kjellsson, A. Vallestad, R. Steigmann, and D. Dzung, "Integration of a wireless i/o interface for profibus and profinet for factory automation," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4279–4287, Oct. 2009.

[28] B. M. Wilamowski and J. D. Irwin, *Technologies, in the Industrial Electronics Handbook: Industrial Communication Systems*, 2nd ed. Boca Raton, FL: CRC Press, 2011.

[29] *IEC, Industrial communication networks—Fieldbus specifications, in International IEC 3rd*, Standard IEC 61158-x, Aug. 2010.

[30] J. Jasperneite, J. Imtiaz, M. Schumacher, and K. Weber, "A proposal for a generic real-time ethernet system," *IEEE Trans. Ind. Inf.*, vol. 5, no. 2, pp. 75–85, May 2009.

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

[32] J.-D. Decotignie, "The many faces of industrial ethernet (past and present)," *IEEE Ind. Electron. Mag.*, vol. 3, no. 1, pp. 8–19, Mar. 2009.

[33] P. Gaj, "Pessimistic useful efficiency of epl network cycle," in *Computer Networks, Ser. Communications in Computer and Information Science*, A. Kwiecien, P. Gaj, and P. Stera, Eds. Berlin, Heidelberg: Springer, 2010, vol. 79, pp. 297–305.

[34] G. Garner and H. Ryu, "Synchronization of audio/video bridging networks using ieee 802.1as," *IEEE Commun. Mag.*, vol. 49, no. 2, pp. 140–147, Feb. 2011.

[35] J. Imtiaz, J. Jasperneite, and S. Schriegel, "A proposal to integrate process data communication to Ieee802.1 audio video bridging (AVB)," in *Proc. 16th IEEE Int. Conf. ETFA*, Toulouse, France, Sep. 2011, pp. 1–8.

[36] J. Imtiaz, J. Jasperneite, and L. Han, "A performance study of ethernet audio video bridging (avb) for industrial real-time communication," in *Proc. ETFA*, Sep. 2009, pp. 1–8.

[37] H. Trsek, L. Wisniewski, E. Toscano, and L. Bello, "A flexible approach for real-time wireless communications in adaptable industrial automation systems," in *Proc. ETFA*, Sep. 2011, pp. 1–4.

[38] U. Hentschel, A. Schmidt, and A. Polze, "Predictable communication for mobile systems," in *Proc. ISORC*, Mar. 2011, pp. 24–28.

[39] S. eun Yoo, P. K. Chong, D. Kim, Y. Doh, M.-L. Pham, E. Choi, and J. Huh, "Guaranteeing real-time services for industrial wireless sensor networks with ieee 802.15.4," *IEEE Trans. Ind. Electron.*, vol. 57, no. 11, pp. 3868–3876, Nov. 2010.

[40] K. Kunert, E. Uhlemann, and M. Jonsson, "Predictable real-time communications with improved reliability for ieee 802.15.4 based industrial networks," in *Proc. WFCS*, May 2010, pp. 13–22.

[41] M. Jonsson and K. Kunert, "Towards reliable wireless industrial communication with real-time guarantees," *IEEE Trans. Ind. Inf.*, vol. 5, no. 4, pp. 429–442, Nov. 2009.

[42] Y. Zheng, A. Xu, Y. Song, W. Zhao, and M. Liu, "Industrial wireless deterministic communication based on WLAN: Design, implementation and analysis," in *Proc. ICCTA*, Oct. 2009, pp. 274–278.

[43] *Industrial Wireless LAN. Industrial Features and Current Standards*, SIMATIC NET White Paper V.1.1, SIEMENS AG.

[44] J. Ko, A. Terzis, S. Dawson-Haggerty, D. Culler, J. Hui, and P. Levis, "Connecting low-power and lossy networks to the internet," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 96–101, Apr. 2011.

[45] S. Petersen and S. Carlsen, "Wirelesshart versus isa100.11a: The format war hits the factory floor," *IEEE Ind. Electron. Mag.*, vol. 5, no. 4, pp. 23–34, Dec. 2011.

[46] A. Willig, "Recent and emerging topics in wireless industrial communications: A selection," *IEEE Trans. Ind. Inf.*, vol. 4, no. 2, pp. 102–124, May 2008.

[47] B. M. Wilamowski and J. D. Irwin, *Wireless communication standards, The Industrial Electronics Handbook: Industrial Communication Systems*, 2nd ed. Boca Raton, FL: CRC Press, 2011.

[48] J. Jasperneite and M. Schäfermann, "Investigation of Cellular Networks for m2m Applications," Institut Industrial IT, 2011.

[49] S. Akhtar, "Evolution of technologies, standards, and deployment of 2G-5G networks," *Encyclopedia of Multimedia Technology and Networking. IGI Global*, pp. 522–532, 2009.

[50] N. Baxter and H. D. Jesus, "Remote machinery monitoring—A developing industry," *Machinery Reliab. Sound Vibration Mag.*, pp. 20–24, May 2008.

[51] W. Amer, U. Ansari, and A. Ghafoor, "Industrial automation using embedded systems and machine-to-machine, man-to-machine (m2m) connectivity for improved overall equipment effectiveness (oee)," in *Proc. SMC*, Oct. 2009, pp. 4450–4454.

[52] S. K. Tan, M. Sooriyabandara, and Z. Fan, "M2m Communications in the Smart Grid: Applications, Standards, Enabling Technologies and Research Challenges," Toshiba Res. Europe Ltd. Telecommun. Res. Lab., Bristol, U.K., 2011.

[53] Y. Kwon and T.-L. Tseng, "Remote monitoring and control of smart grid power network system," in *Proc. CIE*, Jul. 2010, pp. 1–6.

[54] H. Kirrmann, "Fault Tolerant Computing in Industrial Automation," 2nd Ed., ABB Research Center, 2005.

[55] *IEC, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems—Part 1 to 7, International IEC 2nd*, Standard IEC 61508-x, Jun. 2010.

[56] Y. Sato, "Throwing a bridge between risk assessment and functional safety," in *Proc. SICE*, Sep. 2007, pp. 2484–2488.

[57] *IEC, Industrial Communication Networks—Profiles—Part 3: Functional Safety Fieldbuses, Several Subparts, International IEC 2nd*, Standard IEC 61784–3-x, Jun. 2010.

[58] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May-Jun. 2011.

[59] T. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *IEEE Computer*, vol. 44, no. 4, pp. 91–93, Apr. 2011.

[60] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Fovino, and A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in scada systems," *IEEE Trans. Ind. Inf.*, vol. 7, no. 2, pp. 179–186, May 2011.

[61] H. Kirrmann, K. Weber, O. Kleineberg, and H. Weibel, "Hsr: Zero recovery time and low-cost redundancy for industrial ethernet (high availability seamless redundancy, iec-3)," in *Proc. ETFA*, Sep. 2009, pp. 1–4.

[62] H. Kirrmann, M. Hansson, and P. Muri, "Iec 62439 prp: Bumpless recovery for highly available, hard real-time industrial networks," in *Proc. ETFA*, Sep. 2007, pp. 1396–1399.

[63] C. De Dominicis, P. Ferrari, A. Flammini, S. Rinaldi, and M. Quarantelli, "On the use of ieee 1588 in existing iec 61850-based sass: Current behavior and future challenges," *IEEE Trans. Instrum. Meas.*, vol. 60, no. 9, pp. 3070–3081, Sep. 2011.

[64] L. Wisniewski, M. Hameed, S. Schriegel, and J. Jasperneite, H. S. H. Juanole Guy, Ed., "A survey of ethernet redundancy methods for real-time ethernet networks and its possible improvements," in *Proc. Fieldbuses and Networks in Industrial and Embedded Systems, Ser. in: 8th Int. Conf. Fieldbuses Networks Industrial; Embedded Systems (FET'2009)*, May 2009, vol. 8, pp. 163–170.

Piotr Gaj (M'10) received degrees from the Silesian University of Technology, Gliwice, Poland.

He was at a few professional, teaching, and research positions. He authored or coauthored a several dozen papers in the area of industrial systems. He served as a member and reviewer for a few of scientific conferences and journals. His research interests include the area of industrial informatics, including industrial computer networks and systems. He is currently a lecturer in the Department of Automatic Control, Electronic and Computer Science, Silesian University of Technology, Gliwice, Poland.

Dr. Gaj is currently the Organizing Chair of the Computer Networks International Science Conference.

Jürgen Jasperneite (M'98–SM'06) studied electrical engineering and received the Dr.-Ing. Degree in electrical engineering and information technology from the Otto-von-Guericke University of Magdeburg, Germany, in 2002.

Since 2005, he has been a Full Professor of Computer Networks at the Ostwestfalen-Lippe University of Applied Sciences, Lemgo, Germany. He authored or coauthored more than 100 papers in the area of industrial communications. Since the beginning of 2007, he has been the founding Director of the University Institute for Industrial Information Technologies (inIT-Institut Industrial IT). He served as a member or reviewer for a lot of scientific conferences and journals. His current research interests are modeling, testing, and evaluating of real-time communication systems, especially in the field of industrial automation. Since 2009 he has been also the director of the Fraunhofer Application Center Industrial Automation in Lemgo, Germany.

Prof. Jasperneite is vice-chair of the IEEE IES Technical Committee "Factory Automation."

Max Felser (M'84) received degrees from the Ecole d'ingénieurs et d'architectes de Fribourg and the Swiss Federal Institute of Technology Zurich (ETHZ), Switzerland.

He was responsible for the developed methodology for data communication systems at Ascom AG and he was the head of the Programmable Logic Controller (PLC) development at SAIA-Burgess AG. He joined the Berne University of Applied Sciences in the faculty of Engineering and Information Technology as a professor in 1991 and runs the fieldbus laboratory at the Institute of Mobile Communications in Burgdorf (Switzerland). His research interest includes industrial wired and wireless real-time networks.

Prof. Felser is a Fellow of Electrosuisse, a Chairman of the national TC65 mirror committee of IEC, and a Chairman of the Regional PROFIBUS Association (RPA) in Switzerland.