Scanning the Issue

Special Issue on Industrial Communication Systems

I. INTRODUCTION

The advances in design of embedded systems, tools availability, and falling fabrication costs of semiconductor devices and systems allowed for infusion of intelligence in to field devices such as sensors and actuators. The controllers used with these devices provide typically on-chip signal conversion, data and signal processing, and communication functions. The increased functionality, processing, and communication capabilities of controllers have been largely instrumental in the emergence of a widespread trend for networking of field devices around specialized networks, frequently referred to as field area networks.

One of the main reasons for the emergence of field area networks in the first place was an evolutionary need to replace point-to-point wiring connections by a single bus, thus paving the road to the emergence of distributed systems and, in future, networked embedded systems with the infusion of intelligence in to the field devices. The details of the fieldbus technology evolution are presented in this issue in the paper "Fieldbus Technology in Industrial Automation" by Thomesse. The field area networks, or fieldbuses [1] (fieldbus is, in general, a digital, two-way, multidrop communication link) as they are commonly referred to, are, in general, networks connecting field devices such as sensors and actuators with field controllers (for instance, programmable logic controllers (PLCs) in industrial automation, or electronic control units (ECUs) in automotive applications), as well as man–machine interfaces. The field area networks are used in a variety of application domains: industrial and process automation, building automation, automotive and railway applications, aircraft control, control of electrical substations, etc. The benefits are numerous, including increased flexibility, improved system performance, and ease of system installation, upgrade, and maintenance. Unlike LANs, due to the nature of communication requirements imposed by applications, field area networks, by contrast, have low data rates and a small size of data packets, and typically require real-time capabilities which mandate determinism of data transfer. However, data rates above 10 Mb/s, typical of LANs, have become a commonplace in field area networks. The field area networks employ, either directly or in combination, three basic communication paradigms: client–server, producer–consumer, and publisher–subscriber models. The use of these models reflects intimately the requirements and constraints of an application domain or a specific application.

Although for the origins of field area networks, one can look back as far as the end of the 1960s in the nuclear instrumentation domain (the CAMAC network [2]) and the beginning of the 1970s in avionics and aerospace applications (MIL-STD-1553 bus [3]), it was the industrial automation area which brought the main thrust of developments. The need for integration of heterogeneous systems, difficult at the time due to the lack of standards, resulted in two major initiatives which have had a lasting impact on the integration concepts, and architecture of the protocol stack of field area networks. These initiatives were Technical and Office Protocol (TOP) [4] and Manufacturing Automation Protocol (MAP) [5] projects. The two projects exposed some pitfalls of the full seven-layer stack implementations (ISO/OSI model [6]) in the context of applications in industrial automation. As a result, typically, only layers 1 (the physical layer), 2 (the data link layer, including implicitly the medium access control layer), and 7 (the application layer, which covers also the user layer) are used in field area networks [7]; also prescribed in the international fieldbus standard, IEC 61 158 [8]. In IEC 61158, functions of layers 3 and 4 are recommended to be placed either in layer 2 or layer 7; functions of layers 5 and 6 are covered in layer 7.

The evolution of fieldbus technology which began well over two decades ago has resulted in a multitude of solutions reflecting the competing commercial interests of their developers and standardization bodies, both national and international: IEC [9], ISO [10], ISA [11], CENELEC [12], and CEN [13]. This is also reflected in IEC 61 158 (adopted in 2000), which accommodates all national standards and user organization championed fieldbus systems. Subsequently, implementation guidelines were compiled into Communication Profiles, IEC 61 784-1, [14]. Those Communication Profiles identify seven main systems (or Communication Profile Families) known by brand names as Foundation Fieldbus (H1, HSE, H2), used in process and factory automation; ControlNet and EtherNet/IP, both used in factory automation; PROFIBUS (DP, PA), used in

---

Digital Object Identifier 10.1109/JPROC.2005.849727

factory and process automation, respectively; PROFInet, used in factory automation; P-Net (RS 485, RS 232), used in factory automation and shipbuilding; WorldFIP, used in factory automation; INTERBUS, INTERBUS TCP/IP, and INTERBUS Subset, used in factory automation; and Swiftnet transport and Swiftnet full stack, used by aircraft manufacturers. The listed application areas are the dominant ones.

Ethernet, the backbone technology of the office networks, is increasingly being adopted for communication in factories and plants at the fieldbus level. The random and native Carrier Sense Multiple Access With Collision Detection (CSMA/CD) arbitration mechanism is being replaced by other solutions allowing for deterministic behavior required in real-time communication to support soft and hard real-time deadlines, time synchronization of activities required to control drives, for instance, and for exchange of small data records characteristic of monitoring and control actions. A variety of solutions have been proposed to achieve this goal. Some can coexist with regular Ethernet nodes; some reuse the same hardware but are incompatible; some are compatible but cannot offer guarantees in presence of nodes that do not implement the same modifications—as classified in the paper "Ethernet Based Real-Time and Industrial Communications," by Decotignie, included in this issue.

The emerging Real-Time Ethernet (RTE), Ethernet augmented with real-time extensions, under standardization by the IEC/SC65C committee, is a fieldbus technology which incorporates Ethernet for the lower two layers in the OSI model. There are already a number of implementations, which use one of the three different approaches to meet real-time requirements. The use of standard components such as protocol stacks, Ethernet controllers, bridges, etc., allows for mitigating the ownership and maintenance cost. The direct support for the Internet technologies allows for vertical integration of various levels of industrial enterprise hierarchy to include seamless integration between automation and business logistic levels to exchange jobs and production (process) data; transparent data interfaces for all stages of the plant life cycle; the Internet- and Web-enabled remote diagnostics and maintenance, as well as electronic orders and transactions.

The use of wireless links with field devices, such as sensors and actuators, allows for flexible installation and maintenance, mobile operation required in case of mobile robots, and alleviates problems with cabling. A wireless communication systems to operate effectively in the industrial/factory floor environment has to guarantee high reliability, low and predictable delay of data transfer (typically, less than 10 ms for real-time applications), support for a high number of sensor/actuators, and low power consumption, to mention some. In the industrial environments, the wireless channel characteristic degradation artifacts can be compounded by the presence of electric motors or a variety of equipment causing the electric discharge, which contribute to even greater levels of bit error and packet losses. Improving channel quality and designing robust and loss-tolerant applications, both subjects of extensive research and development, seem to have a potential to alleviate the problems to some extent. Some of these solutions are discussed in this issue in the paper "Wireless Technology in Industrial Networks" by Willig *et al.* In addition to peer-to-peer interaction, the sensor/actuator stations communicate with the base station(s), which may have its transceiver attached to the cable of a fieldbus, thus resulting in a hybrid wireless–wireline fieldbus system. To leverage low cost, small size, and low power consumptions, Bluetooth 2.4-GHz radio transceivers may be used as the sensor/actuators communication hardware. To meet the requirements for high reliability, low and predictable delay of data transfer, and support for high number of sensor/actuators, custom optimized communication protocols may be required for the operation of the base station as the commercially available solutions such as IEEE 802.15.1/Bluetooth [15], [16], IEEE 802.15.4/ZigBee [17], and IEEE 802.11 [18]–[20] variants may not fulfill all the requirements.

The growing trend for horizontal and vertical integration of industrial automated enterprises, largely achieved through internetworking of the plant communication infrastructure, coupled with a growing demand for remote access to process data at the factory floor level, exposes automation systems to potential electronic security attacks, which may compromise the integrity of these systems and endanger plant safety. Safety, or the absence of catastrophic consequences for humans and environment, is, most likely, the most important operational requirement for automation and process control systems. Another important requirement is the system/plant availability; the automation system and plant have to be safe operational over extended periods, even if they continue operation in a degraded mode in the presence of a fault. With this requirement, security software updates in the running field devices may be difficult or too risky. The limited computing, memory, and communication bandwidth resources of controllers embedded in the field devices pose a considerable challenge for the implementation of effective security policies which, in general, are resource demanding. This limits the applicability of the mainstream cryptographic protocols, even vendor-tailored versions. The operating systems running on small footprint controllers tend to implement essential services only and do not provide authentication or access control to protect mission and safety critical field devices. As pointed out in the paper on security in this issue, "Security for Industrial Communication Systems," by Dzung *et al.*, "security is a process, not a product." This motto embeds practical wisdom that solutions depend on specific application areas, systems, and devices to be protected.

Another fast-growing application area for the field area networks is building automation [21]. Building automation systems aim at the control of the internal environment, as well as the immediate external environment of a building or building complex. At present, the focus of research and technology development is on commercial types of buildings such as office buildings, exhibition centers, shopping complexes, etc. However, the interest in (family type) home automation is on the rise. Some of the main services to be offered by the building automation systems typically include climate control to include heating, ventilation, and air conditioning; visual comfort to cover artificial lighting and control of daylight; safety services such as fire alarm and emergency sound system; security protection; control of utilities such as power, gas, water supply, etc.; and internal transportation systems, including lifts, escalators, etc. The communication architecture supporting automation systems embedded in the buildings has typically three levels: field level, control level, and management level. The field level involves operation of elements such as switches, motors, lighting cells, dry cells, etc. The automation level is typically used to evaluate new control strategies for the lower level in response to the changes in the environment; reduction in the daylight intensity, external temperature change, etc. LonWorks [22], BACnet [23], and EIB/KNX [24]–[27], open system networks for building automation, are suitable for use at more then one level of the communication architecture. In terms of the quality of the service requirements imposed on the field area networks, building automation systems differ considerably from their counterparts in industrial automation. There is seldom a need for hard real-time communication; the timing requirements are much more relaxed. Traffic volume in normal operation is low. Typical traffic is event driven and mostly uses peer-to-peer communication paradigm at the field level; toggling a switch activates lighting cell(s), for instance. Fault tolerance and network management are important aspects. In building automation networks, unlike in industrial automation, the routing functionality and end-to-end control is typically needed arising from the hierarchical network structure. LonTalk [22], for instance, implements all seven layers of the OSI model.

Trends for networking also appear in the automotive electronic systems where the electronic control units (ECUs) are networked by means of one of automotive communication protocols for the purpose of controlling one of the vehicle functions; for instance electronic engine control, antilocking brake system, active suspension, and telematics, to mention a few. There are a number of reasons for the interest of the automotive industry in adopting field area networks and mechatronic solutions, known by their generic name as x-by-wire, aiming to replace mechanical or hydraulic systems by electrical/electronic systems. The main factors seem to be economic in nature, improved reliability of components, and increased functionality to be achieved with a combination of embedded hardware and software. Steer-by-wire, brake-by-wire, and throttle-by-wire systems are representative examples of x-by-wire systems. The dependability of x-by-wire systems is one of the main requirements, as well as constraints on the adoption of this kind of systems. But, it seems that certain safety critical systems such as steer-by-wire and brake-by-wire will be complemented with traditional mechanical/hydraulic backups, for safety reasons. Another equally important requirement for the x-by-wire systems is to observe hard real-time constraints imposed by the system dynamics; the end-to-end response times must be bounded for safety critical systems. A violation of this requirement may lead to performance degradation of the control system, and other consequences as a result. Not all automotive electronic systems are safety critical, or require hard real-time response. For instance, system(s) to control seats, door locks, internal lights, etc., are not. Different performance, safety, and QoS requirements dictated by various in-car application domains necessitate adoption of different solutions, which, in turn, gave rise to a significant number of communication protocols for automotive applications. Some of those protocols are overviewed in this issue in the paper "Trends in Automotive Communication Systems" by Navet *et al.* For instance, time-triggered protocols, based on the time-division multiple access (TDMA) medium access control technology, are particularly well suited for the safety critical solutions, as they provide deterministic access to the medium. In this category, the Time-Triggered Protocol (TTP/C) [28] protocol has been experimented with and considered for deployment for quite some time. However, to date, there have been no actual implementations of that protocol involving safety-critical systems in commercial automobiles or trucks. In 1995, a "proof of concept," organized jointly by the Vienna University of Technology, Vienna, Austria, and DaimlerChrysler, demonstrated a car equipped with a "brake-by-wire" system based on the time-triggered protocol. The FlexRay [29] protocol (FlexRay supports a combination of both time-triggered and event-triggered transmissions) appears to be the front-runner for potential safety-critical applications in future. FlexRay is a joint effort of a consortium involving some of the leading car makers and technology providers—BMW, Bosch, DaimlerChrysler, General Motors, Motorola, Philips, and Volkswagen, as well as Hyundai Kia Motors as a premium associate member with voting rights. Both TTP/C and FlexRay provide additional dependability mechanisms and services which make them particularly suited for safety-critical systems, to mention replicated channels and redundant transmission mechanisms, bus guardians, fault-tolerant clock synchronization, membership service, etc. The cooperative development process of networked automotive applications brings with itself heterogeneity of software and hardware components. Even with the inevitable standardization of those components, interfaces, and even complete system architectures, the support for reuse of hardware and software components is limited, thus potentially making the design of networked automotive applications labor-intensive, error-prone, and expensive. This situation necessitates the development of component-based design integration methodologies and automotive-specific middleware. One of the main bottlenecks in the development of safety-critical systems is the software development process. The automotive industry clearly needs a software development process model and supporting tools suitable for the development of safety-critical software. At present, there are two potential candidates. The first is the Motor Industry Software Reliability Association (MISRA) [30] published recommended practices for safe automotive software. The recommended practices, although automotive specific, do not support x-by-wire. The second is IEC 61 508 [31], an international standard for electrical, electronic, and programmable electronic safety-related systems. IEC 61 508 is not automotive specific, but is broadly accepted in other industries.

The objective of this issue is to give a broad overview of the area of industrial communication networks, with a focus on industrial automation in manufacturing and process industries. To give a better appreciation of other application areas, the use of specialized field area networks in building automation control and in automotive applications is presented as well. The material presents relevant technologies, together with their evolution and standardization activities, and current standards. It also describes ongoing research and industry implementations, and recommended practices adopted by industry, and gives a perspective on current research and development activities driven largely by industrial groups and consortia.

II. PAPER DESCRIPTIONS

This issue includes seven contributions written by some of the leading experts from the area of industrial communication networks, from industry and academia. Some of the contributing authors have been actively involved in the creation of the fieldbus technology from the very beginning. The contributions present a comprehensive overview of the area of industrial networks and their evolution together with standards, the state of the art of the technology, and emerging trends. The material has been arranged in a way to cover most representative aspects of the fieldbus technology and applications in industrial automation, including an overview of technical aspects of fieldbuses, real-time extensions for Ethernet, wireless technology, and security issues. In addition, the issue also gives an overview of network technologies used in building automation control, and automotive applications.

A comprehensive overview of the fieldbus concept and its evolution, the standardization process, and technical aspects are presented in the paper "Fieldbus Technology in Industrial Automation," by Thomesse, who was directly involved in the development of the WorldFIP fieldbus and its standardization. This paper gives a captivating account of the origins of the fieldbus technology by outlining evolution phases driven by a combination of requirements imposed by specific industries and application domains, and standardization activities. This part of the paper is essential reading for anyone wishing to understand the reason for the large number of fieldbuses in existence today. It also presents a roundup of the current standardization activities, and an overview of some of the main standards. A technical analysis of fieldbuses is presented in the second part of the paper. It discusses, layer by layer, a (typical of fieldbuses) three-layer protocol stack architecture in the context of the seven-layer OSI model. It methodically shows some possible distributions of the services offered by the layers of the OSI model among the three layers of the fieldbus stack. The remaining part of the section provides a comprehensive overview of the concepts essential to understand the fieldbus technology. This paper is one of the most exhaustive treatments of fieldbuses, written with clarity and erudition of the technology insider.

An excellent introduction to Ethernet and ways to extend its operation to incorporate real-time requirements is presented in the paper "Ethernet Based Real-Time and Industrial Communications," by Decotignie. The paper gives an overview of selected characteristics of an industrial communication system. This discussion includes application model, network model, data model, error model, and soft versus hard real-time constraints. Subsequently, the paper introduces the conventional Ethernet together with its pros and cons, followed by a brief account of the technology evolution. The different approaches to improve the real-time behavior, surveyed and evaluated in the paper, are based on the reuse of existing Ethernet hardware. Specifically, the approaches presented deal with modifications that either alter or keep compatibility with existing Ethernet hardware. The paper also discusses and analyzes some of the major requirements of industrial communication systems, namely, action synchronization and temporal consistency. It demonstrates that the two cannot be achieved without adding a new layer of protocols dealing with time synchronization.

The focus of the paper "Real-Time Ethernet—Industry Perspective," by Felser, is on RTE, its standardization, and proposals for and actual implementations. The paper explains in detail the structure of the IEC/SC65C standardization committee and gives a roundup of activities to date. In the context of the standardization process, the paper overviews requirements for RTE. The second part of the paper gives a comprehensive overview of the proposals for standardization together with their key technical features. These proposals are, in general, based on the three different approaches to meet real-time requirements. The first approach is based on retaining the TCP/UDP/IP protocols suite unchanged (subject to nondeterministic delays). In this case, all real-time modifications are enforced in the top layer. In the second approach, the TCP/UDP/IP protocols suite is bypassed, the Ethernet functionality is accessed directly—in this case, RTE protocols use their own protocol stack in addition to the standard IP protocol stack. Finally, in the third approach, the Ethernet mechanism and infrastructure are modified. Each of the proposed solutions is described, as far as the details are available, in terms of the protocol implementation, topology and performance, and application protocol model.

A comprehensive overview of wireless communications in the industrial environment and relevant technologies is presented in the paper "Wireless Technology in Industrial Networks," by Willig *et al.* To better appreciate the requirements imposed on wireless communications in the industrial environment, the paper gives an overview of the adverse effects of the transmission errors and certain wireless channel properties on the packet transmission timing and reliability. Subsequently, the paper presents a comprehensive overview of the commercial off-the-shelf wireless technologies to include IEEE 802.15.1/Bluetooth, IEEE 802.15.4/ZigBee, and IEEE 802.11 variants. The suitability of these technologies for industrial deployment is evaluated to include aspects such as application scenarios and environments, coexistence of wireless technologies, and implementation of wireless fieldbus services. The last segment of the paper deals with the integration issues and techniques involved in hybrid wireless–wireline fieldbus systems. This material is illustrated by using a PROFIBUS-based case study.

The paper "Security for Industrial Communication Systems," by Dzung *et al.*, gives an overview of the IT security technologies and best practices for industrial communication system security and introduces some standardization activities in the area. It discusses security objectives, types of attacks, and the available countermeasures for general IT systems. The emphasis is on the TCP/IP protocol suite and the available cryptography-based secure communication protocols. Subsequently, the paper discusses security-relevant characteristics of industrial communication systems, and main types of industrial and utility communication network topologies and protocols, which have an influence on the implementation of security architectures. This is followed by a comprehensive discussion of security issues and solutions for industrial automation protocols on LAN/WAN level, security on the fieldbus and device level, and security in the networked embedded systems. The presented concepts and elements of IT security for industrial and utility communication systems are illustrated by two case studies describing security issues and recommendations for network configuration in electric-energy substation automation and plant automation.

A general overview of the building automation area and the supporting communication infrastructure is presented in the paper "Communication Systems for Building Automation and Control," by Kastner *et al.* The paper provides an extensive description of building service domains and the concepts of building automation and control, and introduces building automation hierarchy together with the communication infrastructure. The discussion of control networks for building automation covers aspects such as selected quality of service requirements and related mechanisms, horizontal and vertical communication, network architecture, and internetworking. As with industrial fieldbus systems, there are a number of bodies involved in the standardization of technologies for building automation. The paper overviews some of the standardization activities, standards, as well as networking and integration technologies. Open systems BACnet, LonWorks, and EIB/KNX are introduced at the end of the paper. The focus is on standardization and certification, physical characteristics, communication patterns, application data models, services, and standard hardware components as well as commissioning tools.

The paper "Trends in Automotive Communication Systems," by Navet *et al.* provides a broad overview of the field of automotive communication systems. Based on functional, performance, and safety requirements, the paper identifies a number of application domains for automotive networks: the powertrain domain, the chassis domain, the body domain, the telematics domain, and the multimedia and human–machine interface domains. Subsequently, the Society for Automotive Engineers (SAE) classification of automotive communication protocols is introduced. The overview of selected automotive networks and protocols is centered on priority buses, which incorporate priority mechanisms, to include Controller Area Network (CAN), Vehicle Area Network (VAN), and J1850; time-triggered networks: TTP/C, FlexRay, and Time-Triggered CAN (TTCAN); low-cost automotive networks such as Local Interconnect Network (LIN) and TTP/A; and multimedia oriented solutions: MOST and IDB-1394. The last major part of the paper has a focus on the software middleware layer for automotive applications. It presents a rationale for this layer and discusses specific requirements. The overview of the state of the art of the automotive middleware includes the OSEK/VDX communication environment (OSEK/VDX COM), the OSEK/VDX fault-tolerant communication layer (OSEK/VDX FTCom), and the Volcano development process and supporting tools.

The guest editor wishes to express his gratitude to the reviewers who volunteered a great deal of their time to provide feedback to the authors. He would also like to thank authors for their important contributions to this special issue.

RICHARD ZURAWSKI, *Guest Editor*
ISA Group
San Francisco, CA 94111 USA

REFERENCES

[1] *The Industrial Communication Technology Handbook*, R. Zurawski, Ed., CRC, Boca Raton, FL, 2005.
[2] R. Costrell, "CAMAC instrumentation system—Introduction and general description," *IEEE Trans. Nucl. Sci.*, vol. NS-18, no. 2, pp. 3–8, Apr. 1971.
[3] C.-A. Gifford, "A military standard for multiplex data bus," in *Proc. IEEE 1974 National Aerospace and Electronics Conf.*, pp. 85–88.
[4] S. R. Dillon, "Manufacturing automation protocol and technical and office protocols—Success through the OSI model," in *Proc. Compcon Spring '87*, pp. 80–81.
[5] H. A. Schutz, "The role of MAP in factory integration," *IEEE Trans. Ind. Electron.*, vol. 35, no. 1, pp. 6–12, Feb. 1988.
[6] H. Zimmermann, "OSI reference model: the ISO model of architecture for open system interconnection," *IEEE Trans. Commun.*, vol. COM-28, no. 4, pp. 425–432, Apr. 1980.
[7] P. Pleinevaux and J.-D. Decotignie, "Time critical communication networks: field buses," *IEEE Network*, vol. 2, no. 3, pp. 55–63, May 1988.
[8] "Digital data communications for measurement and control—Fieldbus for use in industrial control systems, part 1: Introduction," Int. Electrotech. Comm., IEC 61 158-1, 2003.
[9] International Electrotechnical Commission [Online]. Available: http://www.iec.ch
[10] International Organization for Standardization [Online]. Available: http://www.iso.org
[11] Instrumentation Society of America [Online]. Available: http://www.isa.org
[12] Comité Européen de Normalization Electrotechnique [Online]. Available: http://www.cenelec.org
[13] European Committee for Standardization [Online]. Available: http://www.cenorm.be
[14] "Digital data communications for measurement and control—Part 1: Profile sets for continuous and discrete manufacturing relative to fieldbus use in industrial control systems," Int. Electrotech. Comm., IEC 61 784-1, 2003.
[15] Specification of the Bluetooth system (1999). [Online]. Available: http://www.bluetooth.org
[16] "Specification of the Bluetooth system, version 1.1," Bluetooth Special Interest Group, http://www.bluetooth.com, 1999.

[17] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPAN's)*, Oct. 2003.

[18] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 Ghz Band*, 1999.

[19] *Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 1999.

[20] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band*, aNSI/IEEE Std 802.11, June 2003.

[21] D. Snoonian, "Smart buildings," *IEEE Spectr.*, vol. 40, no. 8, pp. 18–23, Aug. 2003.

[22] D. Loy, D. Dietrich, and H. Schweinzer, *Open Control Networks*. Norwell, MA: Kluwer, 2004.

[23] S. T. Bushby, "BACnet: A standard communication infrastructure for intelligent buildings," *Automat. Constr.*, vol. 6, no. 5–6, pp. 529–540, 1997.

[24] *Data communication for HVAC applications—Field Net—Part 2: Protocols*, ENV 13154-2, 1998.

[25] *CEBus-EIB router communications protocol—The EIB communications protocol*, EIA/CEA 776.5-1999.

[26] *Home and Building Electronic Systems (HBES)*, EN 50090-X, 1994-2004.

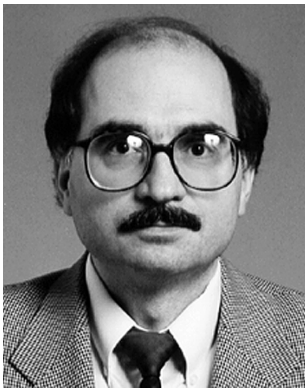
[27] *KNX specifications, V. 1.1*, 2004.

[28] Time-Triggered Protocol TTP/C, High-Level Specification Document, Protocol Version 1.1 (2003, Nov.). [Online]. Available: http://www.tttech.com

[29] FlexRay Communication System, Protocol Specification, Version 2.0 (2004, June). [Online]. Available: http://www.flexray.com

[30] Motor Industry Software Reliability Assoc. [Online]. Available: http://www.misra.org.uk

[31] *IEC 61508:2000, Parts 1–7, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, 2000.



Richard Zurawski received the M.S. degree in informatics and automation from the University of Mining and Metallurgy, Krakow, Poland, in 1977, and the Ph.D. degree in computer science from LaTrobe University, Melbourne, Australia, in 1990.

He held various executive positions with San Francisco Bay area based companies. He was also a full-time R&D advisor with Kawasaki Electric, Tokyo, Japan, and held a regular professorial appointment at the Institute of Industrial Sciences, University of Tokyo. During the 1990s, he participated in a number of Japanese Intelligent Manufacturing Systems programs. He is currently President of ISA Group, San Francisco and Santa Clara, CA, involved in providing solutions to Fortune 1000 companies. He is the Editor for the Industrial Information Technology book series (Boca Raton, FL: CRC). He was Editor of two major handbooks: *The Industrial Information Technology Handbook* (Boca Raton, FL: CRC, 2004) and *The Industrial Communication Technology Handbook* (Boca Raton, FL: CRC, 2004). Books on industrial information technology and networked embedded systems are in progress. He also served as Associate Editor for *Real-Time Systems; The International Journal of Time-Critical Computing Systems* and *The International Journal of Intelligent Control and Systems*. His research interests include formal methods, embedded systems, MEMS, hybrid systems and control, real-time systems, and control of large-scale systems. His involvement in R&D and consulting projects in the past few years include microelectromechical systems (MEMS), network-based solutions for factory floor control, network-based demand side management, Java technology, SEMI implementations, wireless applications, and business intelligence solutions.

Dr. Zurawski received the Anthony J. Hornfeck Service Award from the IEEE Industrial Electronics Society in 1996. He was General Cochairman of the 9th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2003) and the 5th IEEE International Workshop on Factory Communication Systems (WFCS 2004). He has served as Editor at Large for IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and Associate Editor for IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS. In 1998, he was invited by *IEEE Spectrum* to contribute material on Java technology to "Technology 1999: Analysis and Forecast Issue."