Guest Editorial
Special Section on Industrial Communication Technologies and Systems

Claudio Zunino, *Member, IEEE,*, Roman Obermaisser and Stig Petersen, *Senior, IEEE*

Industrial Communication Systems (ICS) have become an increasingly essential part of many automation applications and are deployed in diverse fields such as factory automation, motion control, process automation, networked control systems, and building automation.

Major requirements of ICS are real-time support and dependability under all considered load and fault assumptions. ICS may need to meet stringent deadlines as a basis for stability in control lops and alarm monitoring. At the same time, high reliability and availability is demanded to avoid down times. In particular, reliability with respect to critical failure modes is of utmost importance for safety-critical applications where failures may result in significant financial losses or risk to humans and the environment.

From the point of view of the information and communication technology (ICT), current ICS solutions are based on wired systems to support distributed industrial controls (e.g., specialized fieldbuses and Industrial Ethernet communications [1]). To this regard, a family of Ethernet-based protocols were defined and developed for shopfloor communications, that typically adopts Ethernet techniques and mechanisms at the physical and data link communication levels, but able to provide extensions for real-time support and fault tolerance. Real-time Ethernet solutions such as PROFINET, Ethernet Powerlink, EtherCAT and Time-Sensitive Network (TSN) belong to these classes of industry-oriented protocols: these technologies introduce the separation of normal and real-time traffic, for instance by changing the medium access control (MAC) layer to support prioritization or time-division multiple-access (TDMA) schemes. In addition, fault tolerance mechanisms were introduced such as techniques for frame replication and elimination for reliability [2].

Time-Triggered (TT) extensions to Ethernet [3] such as TSN and TTEthernet are promising solutions to achieve both the real-time and reliability requirements. These protocols support stringent real-time requirements and fault isolation. In TT networks, communication activities are controlled by the progression of a global time base. Each node sends messages with predefined periods and phases regardless of events occurring within the node and/or in the environment.

Nowadays industrial application requirements have forced ICS from insulation to openness, from the use of proprietary technologies to increased adoption of off-the-shelf (even consumer) solutions. ICS are constantly including more and more open hardware and software components for massive interconnection to achieve unprecedented flexibility and adaptability of manufacturing and production systems.

The main goal is progressively moving from traditional approaches to intelligent systems, which are dynamically adaptable to changing production environments and highly flexible, so as to satisfy different process requirements. Factories are evolving into intelligent environments and the main Industry 4.0 [4] concepts are shifting from theory to reality: “plug-and-produce” and “smart infrastructures” are going to become reference keywords in the next years for automation, manufacturing plants and automated production systems.

Therefore, dynamic configuration mechanisms were introduced in ICS. For example, TSN supports the dynamic updating of schedules with time-triggered gate control lists based on IEEE 802.1Qcc [5].

However, rewiring and reconfiguring are neither flexible nor inexpensive activities, so that cable-based approaches might reveal not very effective for future manufacturing environments, where a large number of complex and heterogeneous tasks and processes will need frequent adjustments, likely in real-time. As a result, wireless communications are being considered as one of the most appealing technologies for future industrial applications. Early adoption of wireless technologies in factory and process automation where based on the high capacity wireless LAN offered by the IEEE 802.11 family of standards. While IEEE 802.11 solutions where able to serve some applications, the relatively high power consumption makes them unsuitable for battery-powered operations [6]. Another key issue is the management of real-time needs in an efficient and reliable way [7]. Initially, some of these shortcomings where addressed by the Bluetooth specification, but the practical limitation of maximum seven nodes in a piconet makes it unsuitable for the larger networks often encountered in automation disciplines. The industry-driven WirelessHART and ISA100.11a specifications have satisfactorily addressed the need for large, scalable, low-power, reliable wireless networks for applications with moderate real-time requirements, with their offering of self-configuring, self-healing multi-hop mesh networks [8]. However, for low latency applications like process control, issues with power consumption and latency prevents a successful adaptation [9]. Therefore, new dependable and real-time solutions must be developed, able to address the timing and reliability requirements of Industry 4.0 for local and geographical networks (LANs and WANs) [10].

At the same time, another trend is catching on: moving communication management functions from hardware to software. This is the approach introduced by both the paradigms

Software Defined Networking (SDN) [11] and Network Function Virtualization (NFV) [12] to enhance flexibility and to decouple traffic control from message filtering and forwarding. The main idea behind this approach is separating the data and control planes. While the former is kept inside forwarding devices, the latter is assigned to a central controller where the behavior of the whole network is managed in software.

Because one of the main ideas behind Industry 4.0 is to create smart factories composed by smart machines interconnected by smart networks and to the Internet, cybersecurity becomes fundamental [13] [14]. However the security of industrial systems concerns aspects as different as the protection of physical infrastructures and processes, communications and software and hardware lifecycle management, which cannot be addressed in the same way as done in conventional ICT world. Instead, the peculiarities of industrial networks discourage the adoption of classical approaches to their security and, in particular, of those popular solutions that are mainly based on a detect and patch philosophy. Only recently some specific devices (namely, industrial firewalls) have become available: they are able to recognize and analyze typical application protocols used in industrial environments. Surely, it remains fundamental to introduce security at the very beginning of any industrial system design.

This Special Section on "Industrial Communication Technologies and Systems" presents eleven papers that deal with relevant aspects pertaining to the topics highlighted above: from wired industrial communication systems to wireless solutions and cyber-security: they are briefly described in the following.

The paper *"Incremental Flow Scheduling and Routing in Time-Sensitive Software-Defined Networks"* by Nayak *et al.* presents algorithms to manage a network architecture based on the union of two paradigms: Time Sensitive Networks and Software-Defined Networking. The target is to add incrementally time-triggered flows using a dynamic scheduling approach combined with the SDN features. Time-Sensitive Software-Defined Networks (TSSDN) combines the centralized control system of SDN to time-triggered traffic to provide real-time guarantees. The proposed algorithms formulate the scheduling problem using Integer Linear Programming (ILP) to find solutions for static and dynamic scenarios. It is worth mentioning how TSSDN can achieve sub-second configuration times to schedule time-triggered flows and can be profitably used for on-the-fly schedules.

The paper *"Accurate Timing Networks for Dependable Smart Grid Applications"* by Ramos *et al.* addresses the achievement of deterministic timing reference for smart grid applications. In particular, the authors examine, as an use case, the Substation Automation System (SAS), a fundamental element of a smart grid, typically synchronized with a timing signal provided by a satellite clock. In this case, the solution proposed is based on the novel Ethernet-based protocol White Rabbit, a new high-accuracy profile for the IEEE 16588 standard. The implementation has been carried out on a real SAS system taking in consideration, for the evaluation, time distribution, reliability, scalability and security of the network. Results show how the used technology can improve the performance of all the parameters under analysis.

The paper *"Characterization of Substation Process Bus Network Delays"* by dos Santos *et al.* addresses an analytical delays evaluation methodology in an IEC 61850 process bus substation area network using both a theoretical approach and simulations. Considering how the IEC 61850 standard will be used in substation automation systems and because process bus communication network will support critical data exchanges, a performance evaluation has to be carried out. In particular, the authors present a characterization based on an analytical estimation of the delays introduced in the communication , e.g. processing delay or the queuing delay. Then numerical simulations have been used showing a good agreement with the results obtained with the theoretical approach.

The paper *"Improving Effectiveness of Seamless Redundancy in Real Industrial Wi-Fi Networks"* by Cena *et al.* identifies most relevant design aspects that have to be considered in a redundant wireless communication system, based on the IEEE 802.11 standard, to mitigate joint and mutual interference among channels. Besides considering all the benefits a redundant link can provide, it is equally fundamental to analyze all the aspects that can worsen the seamless redundancy effectiveness. Several phenomena which may cause a general degradation of the performance, such as the Delivery Traffic Indication Map (DTIM) mechanism, interferences within devices or between adjacent channels, were investigated, analyzed in a real testbed, and counteracted through a set of guidelines proposed by authors. After the mitigation of these effects, benefits a redundant link can provide are as good as expected theoretically.

The paper *"A PSSS Approach for Wireless Industrial Communication Applying Iterative Symbol Detection"* by Underberg *et al.* investigates a Parallel Sequence Spread Spectrum (PSSS) approach for wireless industrial communications. More in details, the authors evaluate the proposed solution considering the Bit Error Rate (BER) performance index to reach an exact synchronization and a small temporal misalignment.

The paper is based on both theoretical and simulated evaluations, with also a comparison of a Direct Sequence Spread spectrum (DSSS) system with Walsh codes. Results show how this transmission scheme can enable shortest latencies and flexible resource assignment for star topology based networks.

The paper *"Co-Optimal Placement of PMUs and Their Communication Infrastructure for Minimization of Propagation Delay in the WAMS"* by Appasani *et al.* describes a possible solution to the problem of co-optimal positioning of Phasor Measurement Units (PMUs) and their communication infrastructure to minimize propagation delay in a wide-area measurement system. Because wireless technology has discernible advantages over the fiber optics in this specific context, a microwave communication can be considered a viable solution for fast data transfer. The problem of the placement of PMUs and of theirs towers with radio terminals is described and a solution using Integer Linear Programming (ILP) is proposed. Moreover, the paper presents a comparison with exiting plants based on fiber optics in terms of cost, reliability and speed. Finally, some considerations on security aspects are discussed.

The paper *"Probabilistic Per-Packet Real-Time Guarantees for Wireless Networked Sensing and Control"* by Chen *et al.* proposes a probabilistic framework for per-packet real-time delivery guarantees in a wireless networked sensing and control system. In particular, the proposed solution, defines a real-time notion based on ensuring every packet to be successfully delivered within its deadline with a probability greater than a user-specified threshold. Then, starting from the requirements and the links reliability, it specifies the optimal number of re-transmissions reserved for each packet. In second phase, an EDF (Ealiest Deadline First) real time scheduling with an admission test and traffic load optimization algorithm are applied to maximize the system performances. Both theoretical and simulation approaches have been used to validate the proposed methodology.

The paper *"Novel Power Management Scheme and Effects of Constrained On-Node Storage on Performance of MAC Layer for Industrial IoT Networks"* by Kiran *et al.* introduces a novel IEEE 802.15.4 medium access control (MAC) scheme able to reach user specified reliability levels using with minimal power consumption. The authors developed an analytical model based on a three dimensional Markov chain and a M/G/1/K queue to evaluate the effects of size constrained packet queues. They have also modeled the distributions for service times. Some simulations sessions have been carried out to assess the correctness of the proposed analytical model.

The paper *"Performance evaluation and modeling of an industrial application-layer firewall"* by Cheminod *et al.* presents the characterization and a performance evaluation of a commercial industrial firewall. The device can act both as a normal firewall and as an application-layer filter able to make deep inspection of packets compliant with the Modbus/TCP industrial protocol. The authors have first developed a performance model for the device under analysis. Then they validated the model using an experimental testbed based on COTS hardware and carrying out a set of performance evaluations on the IP filtering capabilities as well as on the application-layer deep packet module. Moreover, results show how a measurement testbed can be used to analyze commercial devices before their deployment in industrial communication systems.

The paper *"A Method for Anomalies Detection in Real-Time Ethernet Data Traffic Applied to PROFINET"* by Sestito *et al.* proposes a generic methodology to detect anomalous events in real time networks using an optimized data extraction and classifying a subset of the traffic features. More specifically, this approach uses am Artificial Neural Network as a classifier, trained using specific relevant traffic features. The method is base on a multiple step strategy: data collection, optimal sliding windows size determination, relevant features selection and classification. Authors have applied the algorithm to the PROFINET protocol with satisfactory results. The proposed solution, however, can be used on any other protocol based on Real-Time Ethernet protocol.

The paper *"An Efficient and Secure Automotive Wireless Software Update Framework"* by Steger *et al.* proposes a framework to enable software updates and diagnostics of Electronic Control Units (ECUs) installed on modern vehicles, using a wireless communication system based on the IEEE 802.11s standard. The framework allows efficient and secure software updates for the entire vehicle lifetime: from the development phase in the assembly line, to the normal maintenance in service centers. It is worth noting how, for the proposed framework, security aspects are carefully considered: from analysis and definition to a evaluation based also on formal methods. The system has been tested on existing ECUs of real vehicles, for example running diagnostic applications. Results show how wireless software updates can increase the efficiency, without impacting on the security aspect.

ACKNOWLEDGMENT

The Guest Editors would like to express their deep gratitude to all the authors, for their contributions and cooperation in replying promptly to the numerous and highly qualified reviewers' comments; to the reviewers, for their careful reviews, which contributed in a significant way to the quality level of the papers that were published; and, finally, to Prof. Ren C. Luo, Editor-in-Chief of the IEEE Transactions in Industrial Informatics, for giving us the opportunity to organize this Special Section and to the TII Editorial team, for the professional support and assistance during the whole preparation of this Special Section.

REFERENCES

[1] P. Gaj, J. Jasperneite, and M. Felser, "Computer Communication Within Industrial Distributed Environment – a Survey," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 182–189, Feb 2013.

[2] *IEEE Draft Standard for Local and metropolitan area networks – Frame Replication and Elimination for Reliability - IEEE P802.1CB/D2.8*, IEEE Computer Society Std., 2017.

[3] R. Obermaisser, R. I. Sadat, and F. Weber, "Active Diagnosis in Distributed Embedded Systems Based on the Time-Triggered Execution of Semantic Web Queries," in *2014 IEEE 17th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing*, June 2014, pp. 222–229.

[4] 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 Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17–27, March 2017.

[5] *IEEE Draft Standard for Local and metropolitan area networks–Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks Amendment: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements*, IEEE Computer Society Std., Jan 2018.

[6] W. Ikram, S. Petersen, P. Orten, and N. F. Thornhill, "Adaptive Multi-Channel Transmission Power Control for Industrial Wireless Instrumentation," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 978–990, May 2014.

[7] G. Cena, S. Scanzio, and A. Valenzano, "Experimental Evaluation of Seamless Redundancy Applied to Industrial Wi-Fi Networks," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 856–865, April 2017.

[8] S. Petersen and S. Carlsen, "WirelessHART Versus ISA100.11a: The Format War Hits the Factory Floor," *IEEE Industrial Electronics Magazine*, vol. 5, no. 4, pp. 23–34, Dec 2011.

[9] W. Ikram, N. Jansson, T. Harvei, N. Aakvaag, I. Halvorsen, S. Petersen, S. Carlsen, and N. F. Thornhill, "Wireless communication in process control loop: Requirements analysis, industry practices and experimental evaluation," in *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*, Sept 2014, pp. 1–8.

[10] L. Seno, G. Cena, S. Scanzio, A. Valenzano, and C. Zunino, "Enhancing Communication Determinism in Wi-Fi Networks for Soft Real-Time Industrial Applications," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 866–876, April 2017.

[11] D. Kreutz, F. M. V. Ramos, P. E. Verssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Jan 2015.

[12] R. Mijumbi, J. Serrat, J. L. Gorricho, N. Bouten, F. D. Turck, and R. Boutaba, "Network Function Virtualization: State-of-the-Art and Research Challenges," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 236–262, Firstquarter 2016.
[13] M. Cheminod, L. Durante, and A. Valenzano, "Review of Security Issues in Industrial Networks," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 277–293, Feb 2013.
[14] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security - A Survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, Dec 2017.

Claudio Zunino Claudio Zunino received the degree in computer engineering and the Ph.D. degree in software engineering from the Politecnico di Torino, Turin, Italy, in 2000 and 2005, respectively. Since 2006, he has been a Researcher with the National Research Council of Italy (CNR). He is currently with the Institute of Electronics, Computer and Telecommunications Engineering (IEIIT). He has authored and coauthored several papers in international journals and conferences in the area of wireless communication, Industrial Ethernet protocols, computer graphics, parallel and distributed computing, and scientific visualization. He serves as reviewer for several international conferences and journals. He has also taken part in the program and organizing committees of many international conferences in the areas of industrial informatics and automation.

Roman Obermaisser Prof. Dr. Roman Obermaisser is full professor at the Division for Embedded Systems of University of Siegen. He has studied computer sciences at Vienna University of Technology, and received the Master's degree in 2001. In February 2004, Roman Obermaisser has finished his doctoral studies in Computer Science with Prof. Hermann Kopetz at Vienna University of Technology as research advisor. In July 2009, Roman Obermaisser has received the habilitation ("Venia docendi") certificate for Technical Computer Science. His research work focuses on system architectures for distributed embedded real-time systems. He wrote a book on an integrated time-triggered architecture published by Springer-Verlag, USA. He is the author of several journal papers and conference publications. He has also participated in numerous EU research projects (e.g., SAFEPOWER, universAAL, DECOS, NextTTA) and was the coordinator of the European research projects DREAMS, GENESYS and ACROSS.

Stig Petersen Stig Petersen (stig.petersen@sintef.no) received his M.Sc. degree in electrical engineering from Norwegian University of Science and Technology (NTNU), Trondheim, Norway, in 2000, and his Doctor of Science (Ph.D) in Computer Science from the University of Antwerp, Belgium in 2013. He is currently a senior research scientist at SINTEF Digital, Trondheim, Norway.

Dr. Petersen's research interest includes industrial communication, wireless communication and functional safety and safety analysis. He is the author and co-author of more than 30 book chapters, journal articles and conference papers on industrial communication, and he has been an invited speaker at both academic and industrial international conferences on this topic. He is a reviewer of manuscripts for various IEEE Industrial Electronics Society journals and conferences. He was the Track Chair of ETFA 2015 and 2016, the General Chair of WFCS 2017 and the Program Chair for SIES 2018.