NISTIR 8317

Reliable, High-Performance Wireless Systems for Factory Automation

Kang B. Lee
Rick Candell
Hans-Peter Bernhard
Dave Cavalcanti
Zhibo Pang
Iñaki Val

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8317

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8317

Reliable, High-Performance Wireless Systems for Factory Automation

Kang B. Lee
Rick Candell
Communications Technology Laboratory

Hans-Peter Bernhard
Silicon Austria Labs GmbH, Austria

Dave Cavalcanti
Intel Corporation, USA

Zhibo Pang
ABB Corporate Research, Sweden

Iñaki Val
IKERLAN Technology Research Centre, Spain

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8317

September 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8317
Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8317, 21 pages (September 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8317

Reliable, High-Performance Wireless Systems for Factory Automation

Kang B. Lee [1] (kang.lee@nist.gov), Rick Candell [1] (rick.candell@nist.gov),
Hans-Peter Bernhard [2], Dave Cavalcanti [3], Zhibo Pang [4], Iñaki Val [5]

[1] National Institute of Standards and Technology, USA
[2] Silicon Austria Labs GmbH, Austria
[3] Intel Corporation, USA
[4] ABB Corporate Research, Sweden
[5] IKERLAN Technology Research Centre, Spain

Abstract

Wireless has emerged as an enabling technology to improve operational flexibility and efficiency for factory automation. The latest wireless technology, standardization activities, and research issues were explored and discussed through the examination of different relevant wireless use cases in a workshop. Some key points, standardization challenges, and research needs of wireless in different areas of factory automation are presented in this article to be reviewed and considered by the industry and standardization development organizations.

Keywords

Factory automation, industrial wireless, precision motion control, cloud-fog automation, collaborative robotics, 5G, TSN.

Why Wireless For Factory Automation?

Life cycle costs for factory automation including structure design, thermal design, installation, commissioning, and maintenance could be improved significantly with the deployment of wireless technologies on the factory floor. Wireless enables new use cases and deployments by enhancing mobility and flexibility. As factory automation advances, wireless technologies can play significant roles in enabling the convergence of information technology (IT) and operational technology (OT) on the shop floor. Manufacturers applying wireless sensing and control technologies in new or existing factory automation systems for monitoring and controlling equipment and processes can realize significant operational and financial benefits.

Using wireless technologies can improve factory-floor operations. These realizations can be achieved through the elimination of costly cabling, which can facilitate mobility enablement, achieve configuration flexibility, improve operating conditions and efficiency, refine performance, and enhance the safety of workers.

Before applying wireless technologies, companies must determine which wireless technology is suitable and reliable for communicating measurement and control data in challenging industrial environments with many potential physical obstructions and sources of interference, in such areas as,

- **Supervisory Control**: Short messaging between machinery for monitoring and control of the manufacturing process
- **Mobility Enablement**: Robotics, Machinery, Discrete Sensors, and Edge Computers
- **Precision Motion Control**: Real-time synchronization and actuation of robot joints trajectories, and rotating machinery

A wireless workshop sponsored by the IEEE Industrial Electronics Society and organized jointly with the National Institute of Standards and Technology (NIST) was conducted at the 2019 IEEE 28th international Symposium on Industrial Electronics (ISIE), namely, “Reliable, High-performance Wireless Systems for Factory Automation”, to address these needs. The purpose of the workshop was to provide a forum for representatives from industry, academia, and government to work closely together and determine the best approach to develop reliable and high-performance wireless systems for factory automation by examining the needs, requirements, and solutions for wireless technologies via studies of use cases. The current effort at NIST is to work with industries to support the use of wireless technologies in factory automation (discrete manufacturing) to improve reliability, efficiency, and productivity of industrial wireless deployments based on previous and current work in discrete manufacturing such as collaborative robotics and precision sensing as well as continuous processes such as oil refinement and gas sensing in confined spaces [1].

Let Us Examine Some Wireless Use Cases

The Industry 4.0 paradigm envisions factories crowded with a huge number of heterogeneous wireless/wired interconnected devices, which can be automatically controlled, upgraded, and configured through ubiquitous networking. This network revolution will drastically cut the maintenance, installation, and operation costs of industrial facilities. Nonetheless, a major challenge arises when building such wireless industrial networks, since the wireless/wired technologies used to build the network must support the heterogeneous requirements: ultra-reliability, ultra-low-latency real-time operation, handling of tens to thousands of nodes, and highly-secured information exchange.

Industrial communications can be classified into three main applications [2]. Condition Monitoring covers the field of industrial applications in which the health status of different components is monitored (e.g., temperature, see Figure 1). Process automation applications are continuous production processes (e.g., chemicals), which are relatively slow. Whereas factory automation (FA) applications mainly comprise of discrete manufacturing processes. These processes are typically implemented as closed-loop, feedback-regulated systems which are automated by using sensors and actuators. These closed-loop systems have stringent real-time requirements, and their performance greatly depends on the properties of the determinism or predictability capabilities of the network protocol.

Last but not the least, if safety-related traffic, such as heartbeat messages and emergency shutdown commands, are also transmitted over the wireless networks, the requirements for latency and reliability will be much more critical to fulfilling the required Safety Integrity Level (SIL).

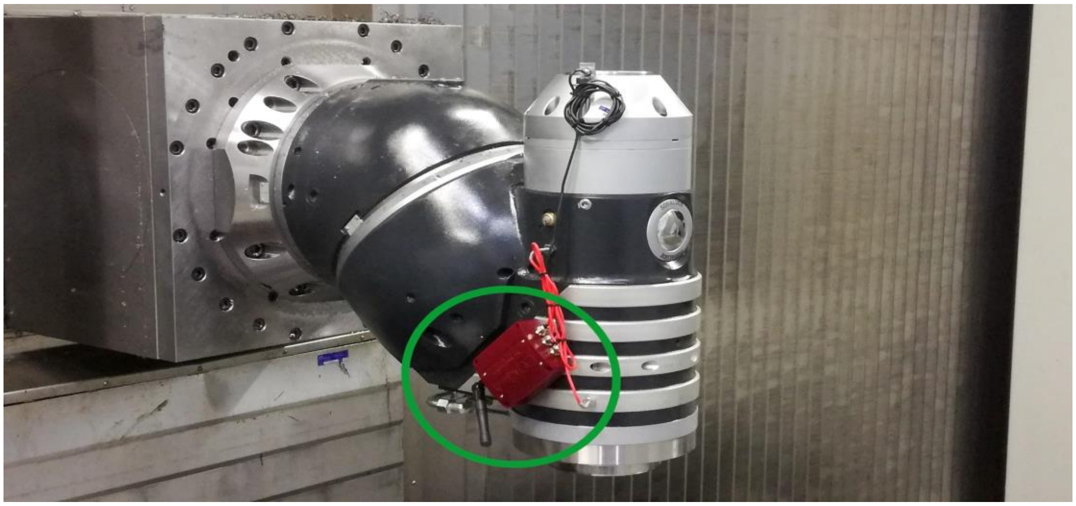

Figure 1. Milling machine monitored by a wireless sensor (Courtesy of SORALUCE-IDEKO **).

Factory Automation With Collaborative Robots Use Cases

The real-time wireless communications for FA are important issues for wireless sensor and actuator networks. For this purpose, a hybrid Time-Sensitive Networking (TSN) architecture was developed [3]. This architecture has been applied to a collaborative robotics use case, built upon a wired TSN architecture. Figure 2 shows how two robots collaborate through manipulating a common artifact; in this case, each robot is commanded from a different network, gaining flexibility, and opening the door to mobile robotics. This development has been based on a narrowband radio, which could be insufficient depending on the requirements. To tackle these restrictions, the SHARP (Synchronous and Hybrid Architecture for Real-time Performance) solution was developed [4], which is a hybrid architecture with TSN properties over both wired and wireless domains. The wireless part combines features from Long-Term Evolution (LTE) and Wi-Fi technologies to provide high-performance and deterministic communications for industrial automation use cases.

Figure 2. Wireless TSN applied to collaborative robotics

Integrating Real-Time Measurements Into Manufacturing Process Control Use Case

In the era of Industry 4.0, there is a great need to build smart manufacturing systems to produce precision parts efficiently by integrating real-time measurements into manufacturing process controls via wireless means, as shown in Figure 3. This is echoed in a project, namely, "Real-time Laser Guided Robot Manufacturing", sponsored by MxD (Manufacturing times Digital) USA, with the collaboration and supports of industry partners. In this use case, a robot used to perform precision manufacturing processes via precision motion controls is guided by a precision measurement system that provides feedback on its positions during its execution of the manufacturing processes to achieve an accuracy of +/-0.05 mm from the robot's original accuracy of +/-(2-3) mm. Wireless communications will greatly enhance the flexibility of robotic manufacturing operations during intricate manipulations. The communication requirements are described below and in Figure 3.

- Low latency is needed for real-time, closed-loop control;
- Reliability of communication is important;
- Wired communication is currently used, viable wireless solutions would reduce costs and facilitate ease of setup and operation.

However, current industrial wireless technologies are slow and unreliable. They garner unacceptably long latency and jitter. There is a lack of industry standards that could solve the aforementioned problems. A new, robust, and standardized high-speed industrial wireless technology is needed.

Courtesy of Automated Precision, Inc.

Figure 3. Integrating measurements into a real-time control system.

Prospects Of Wireless For Mission-Critical Use Cases: From Classic Pyramid Automation To Cloud-Fog Automation

Despite the efforts for more than two decades, there are still major challenges in reliability, latency, and security before wireless can be applied in mission-critical controls in factory automation, especially for machine control and transmission of safety integration and protection messages [5]. These challenges cannot be solved without new physical and Media Access Control (MAC) layers and chipsets specifically addressing the industrial requirements [6]. Unfortunately, the efforts from major chip vendors and communication companies in these industry-specific use cases do not sufficiently drive technology development due to the lower volume demands coupled with much higher technical challenges as compared to the consumer market. In recent years, some research efforts have led to the High-Performance Wireless (WirelessHP) which has achieved significant benchmarks, e.g., a packet transmission time of 6.72us with 100-bit level payload [7], a packet error rate of $10e^{-7}$ [8], and the possibility of security against Probing-Free-Attacks [9]. This progress has motivated positive changes in major wireless communities targeting critical control, e.g., the Avnu Alliance towards wireless-based TSN, the 3rd Generation Partnership Project (3GPP) towards TSN over 5G, and the IEEE towards IEEE 802.11be.

Moreover, the impacts of wireless critical control are not just in communication and networking architecture alone, but more in the overall design paradigm of factory automation. As illustrated in Figure 4, the design paradigm of industrial automation systems is evolving from the classic hierarchical pyramid architecture to the cloud automation architecture where the upper-layer applications in the Enterprise Resource Planning and Manufacturing Execution Systems are deployed over the cloud. If the wireless-based critical control comes into reality one day, the lower layer applications in the supervisory controllers, machine controllers, and input and output (I/O) modules can be deployed over local wireless networks, and the overall architecture becomes the so-called Cloud-Fog Automation.

In Cloud-Fog Automation, the costs of machines can be reduced significantly by off-loading the major portion of computation to fog or cloud. More advanced algorithms and machine intelligence can be implemented on a more powerful and cost-effective computation platform. More flexible load distribution and resilient redundancy can be expected through the wireless fog networks, adapting to tasks and environments dynamically. We hope this disruptive vision can motivate chip vendors and communications companies to make more efforts in this direction.

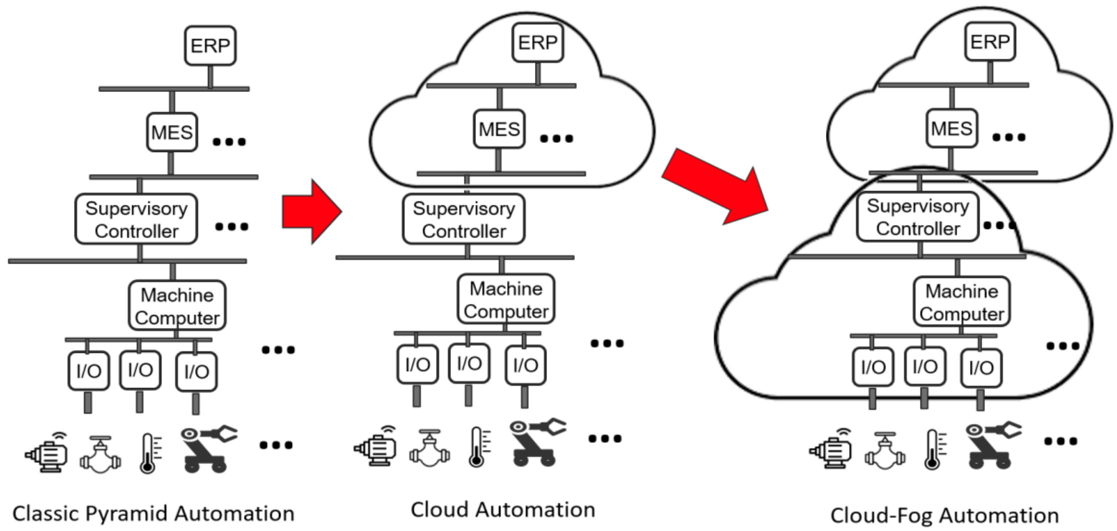

Figure 4. The evolution of industrial automation systems design paradigms.

As for the directions of future research, we first expect the communication communities to find out together a roadmap for future wireless factory automation where the TSN traffics can be transmitted seamlessly throughout hybrid wired and wireless media without upper-layer translation. Secondly, we appeal for more wireless channel measurements and modeling of actual industrial environments. Then based on that, enhancement of latency, reliability, and security should be explored [10]. Thirdly, we recommend the automation communities to prototype wireless-based critical controls by software-defined-radio (SDR) and showcase the benefits of the Cloud-Fog Automation before new generation chipsets are available [7].

Some Wireless User Requirements For Factory Workcells

After reviewing various wireless requirements considerations, such as latency, reliability, scalability, range, update rate, and security, and various perspectives on wireless user requirements from standards organizations, such as the International Society of Automation (ISA) and European Telecommunications Standards Institute (ETSI), NIST has developed some specific wireless user requirements for factory workcells. A report has been published as the NIST Advanced Manufacturing

Series 300-8 report [11]. As stated in the report, there are some basic assumptions for setting these user requirements, and they are: a) a typical workcell size is 10 m x 10 m, with no more than one system failure every 1,000 years, b) individual transmissions are independent, and c) one wireless link would be used involving multiple sensors/regulators.

Wireless TSN: Next Generation Wireless For Time-Critical Industrial Systems?

Factory communications for time-sensitive applications have historically relied on a variety of Ethernet-based, real-time protocols. More recently, the IEEE 802.1 TSN standards have emerged as a unifying opportunity to enable interoperable, time-sensitive communications. The standards defined by the IEEE 802.1 TSN working group enable time synchronization and bounded latency communications with very low packet loss in converged networks where time-sensitive and other traffic shares the same underlying medium. The 802.1 TSN standards can be seen as a toolkit to be selected, deployed, and configured based on the requirements of the applications. Some of the TSN standards include time synchronization (802.1AS), time-aware scheduling (802.1Qbv), redundancy (802.1CB), frame preemption (802.3br/802.Qbu), and resource reservation and management (802.1Qcc). More details on 802.1 TSN standards can be found in [12]. Although some of the 802.1 TSN standards and capabilities have been defined over 802.11/Wi-Fi (e.g., 802.1AS-based time synchronization), more TSN capabilities need to be extended over wireless networks, primarily related to providing bounded latency services with high reliability. Many challenges remain to be addressed to enable seamless TSN capabilities across wired and wireless domains as discussed in [13], including:

- Wireless channel characteristics and variations in industrial scenarios;
- Wireless channel access latency and jitter;
- Coexistence and interference management;
- Consideration of security and safety levels.

The opportunities to enable time-sensitive applications have motivated research and standardization efforts towards the next generation of wireless technologies. Related efforts are happening in the scope of the IEEE 802.11 Wireless LAN working group (802.11ax/Wi-Fi 6, and the next generation 802.11be) and 3GPP cellular standards, mainly in the context of 5G URLLC (Ultra-Reliable Low-Latency Communications).

Time synchronization between end devices and bridges is a fundamental capability for supporting many applications (e.g., controller to controller coordination, sensor fusion) and other TSN capabilities (e.g., time-aware scheduling). The 802.1AS protocol has been the standard used to distribute time across TSN-enabled networks. Support for 802.1AS has been extended to 802.11 links, as defined in the IEEE 802.11-2012 specification. Other TSN standards, such as time-aware scheduling (802.1Qbv) can leverage the wireless time synchronization to avoid congestion and enable bounded latency in 802.11 networks. The trigger-based access capabilities recently enabled in the 802.11ax (Wi-Fi 6) standard can be used to better control latency as the Access Point (AP) can schedule downlink (DL) and uplink (UL) communications, avoiding contention, and random-access delays. Further enhancements in latency reduction, reliability, and capacity are being defined in the next generation 802.11be standard, including an enhancement for the worst-case latency/jitter and integration with TSN.

The low-latency capabilities with high reliability that enabled by the 5G URLLC mode has motivated the integration of 5G systems with 802.1 TSN-enabled networks. In addition to enabling 802.1AS time synchronization across a 5G system introduced in the 3GPP Release 16 specifications. Further support for time-aware scheduling and other TSN capabilities are also being considered as potential topics for the 3GPP Release 17 specifications.

What Is Control-Communications Co-Design And How Does This Approach Can Work With Wireless In Factory Automation?

Control systems treat the "network" as an ultra-reliable deterministic (wired) data pipe with the expectation for "wire-equivalent" performance from wireless technologies. What if, rather than trying to meet “wire-equivalent” latency and reliability, we try meeting control or task-specific goals using a co-design approach. Co-design refers to resource-utilization optimization in a wireless network based on the state of the control system, and the control algorithm to proactively guarantee the control performance based on the awareness of the imperfect nature of wireless networks [20]. This enables the wireless network to support many more control loops compared to the traditional black-box approach. The development of wireless capabilities and standards in both IEEE 802.11 and 3GPP to support time-critical industrial communications has been driven by the goal to achieve “wire-equivalent” performance. This design goal has assumed that the underlying network needs to be an ultra-reliable (wired) data pipe with no knowledge about the applications running on top. Although such a design approach has worked well for wired (Ethernet) industrial communications, it imposes extreme requirements on wireless links that are intrinsically subjected to stochastic variations. The new co-design approach proposed in [14] focuses on meeting control/task-specific goals (e.g., the stability of a control system, minimal drift in a trajectory, …) rather than only focusing on achieving bounded latency and high reliability for all the packets. The proposed co-design approach increases the resource utilization in the wireless network by using state information of the control system. For instance, if a control system is in a stable condition, it may afford to not receive inputs for a certain period without impacting the overall task as the controller would still be able to maintain stability. From a communication perspective, it means that the controller may not necessarily need extremely high reliability for every input (or output) transmission. As the authors demonstrate in [14], by enabling the exchange of state information between the control system and the resource scheduler in a wireless network (e.g., Access Point), it is possible to meet the goals of many more control systems over the same wireless resources compared to a “black-box” approach that assumes extremely high reliability is needed in every transmission. This is an important design consideration that could enable and accelerate the deployment of wireless-based, time-critical industrial systems.

How To Make Wireless TSN Secure?

Security and reliability are the most prominent prerequisites for the trustworthiness of wireless technologies in factory automation. Their implementations must be in line with the given framework of industry standards like ISA/IEC 62443 in order to create a strong acceptance of wireless technologies in the industry. This is a cross-section matter and necessary to pave the way for a holistic approach to use wireless technologies for operational technology (OT) and information technology (IT) networks. Therefore, trustworthiness has to be guaranteed, which relies on three pillars: *communication performance*, *reliability*, and *security*.

A key concept of security standards is the application of security zones and conduits introduced in ISA/IEC 62443-1-1 [16]. It specifies technical control system requirements (SRs) associated with seven foundational requirements (FRs), which define the requirements for control system capability in terms of Security Levels (SLs). The seven FRs are:

1. identification and authentication control (IAC);
2. use control (UC);
3. system integrity (SI);
4. data confidentiality (DC);
5. restricted data flow (RDF);
6. timely response to events (TRE);
7. resource availability (RA).

However, if wireless networks are deployed in OT networks, these seven requirements are not sufficient. Hence, we propose an expansion by adding the following requirements:

8. synchronous deterministic response to events (SDRE);
9. resource sovereignty (RS);
10. verification and validation (VV).

Both wired and wireless communications typically use the same media access methods, such as Time Division Multiple Access (TDMA), which relies on full control of the communication media and on cooperative use by communication peers. In wired communication access can be easily controlled, which enables full RS. In wireless communications, the resource is the set of wireless channels within one but also between several adjacent zones. These channels must be protected to claim resource sovereignty similar to copper cables which need insulation and shielding. Therefore, it is necessary to guarantee access by reserving licensed channels like in 4G/5G cellular mobile radio. Nevertheless, accessibility must still be monitored. Therefore, we propose research work to protect the premises by an electromagnetic border (EMB) consisting of nodes listening to the communications over the reserved channels in the specific zone. The EMB is set up physically around a factory cell. Figure 6 shows the guard nodes monitoring the communications within the channel and analyzing the exchanged messages. Based on the guard nodes, an estimation of the direction of arrival by triangulation or fingerprinting can be performed to localize an interfering or jamming source [23]. As a countermeasure, beamforming [18] can be used to attenuate the jamming signals, and as in 5G, cooperative multipoint communication allows for alternative wireless routes such as the blue beam shown in Figure 6. Also, well-established approaches like channel hopping can be used to combat jamming, but at the cost of higher latency.

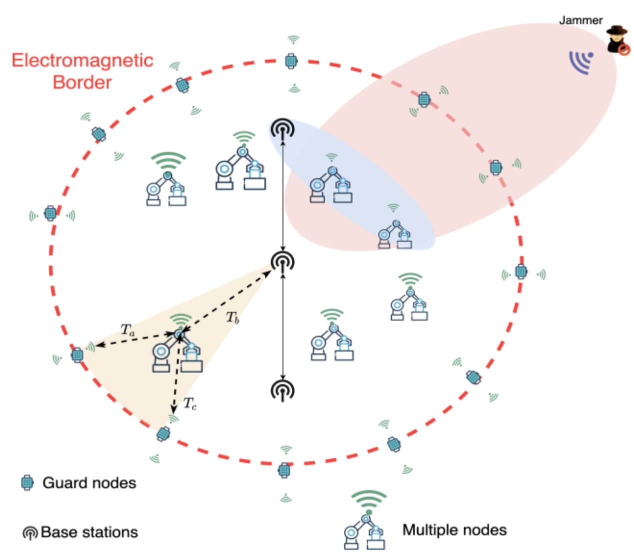

Figure 6. Protecting premises by an electromagnetic border.

Due to hard real-time requirements, clocks are synchronized to a master clock and synchronization issues are considered as severe and have to be avoided. Consequently, the timing of synchronized communication -- sporadic, event-driven, and streaming -- is used for time-of-flight measurements (TFM) by guard nodes [22], such as that shown in Figure 6, to provide distance bounding for security. Additionally, it fulfills the SDRE requirements. Another trustworthiness improvement of the system is achieved by channel impulse response (CIR) measurements [12]. A recent research project [17] is working on trustworthiness indicators using the addressed parameters. This indicator allows a continuous verification and validation process (VV) in order to decide upon the trustworthiness of the communication link and the transmitted data. As the measures described above still have major limitations, we call for more research in this direction with high priority.

Conclusions

Based on the discussions at the workshop and the examination of the various use cases applicable to factory automation, we believe this industry would benefit greatly from reliable, secure, and high-performance wireless communications, in particular in the areas of collaborative robotics with and without interaction with human and robotic automation in manufacturing. Some emerging standards or research activities, e.g., the WirelessHP [5], SHARP [4], and TSN-over-WiFi [12], and the 5G New Radio have achieved significant progress toward the long-term vision of Cloud-Fog Automation to enable TSN-grade wireless transmission of critical control traffics. However, major challenges are still open in not only the latency and reliability but also time synchronization and security including intentional jamming. We have discussed some active research topics with possible directions which could be promising for future solutions, e.g., control-communication co-design, hybrid wired-wireless network architecture with convergence towards TSN, integrating the wireless links into real manufacturing processes to validate the proposed new designs and physical layer security, especially against jamming attacks. Also, the NIST wireless project [21] will continue to assist the industry to adopt and use wireless standards and technologies to improve operational performance and efficiency in factory automation.

Acknowledgments

The authors would like to thank the participants of the wireless workshop on “Reliable, High-performance Wireless Systems for Factory Automation” for their contributions.

Disclaimer

** Commercial equipment and software, many of which are either registered or trademarked, are identified to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

References

1. R. Candell, et. al., “Guide to Industrial Wireless Systems Deployments”, Advanced Manufacturing Series (NIST AMS) 300-4. [Online] Available: https://doi.org/10.6028/NIST.AMS.300-4
2. Z. Fernández, Ó. Seijo, M. Mendicute and I. Val, "Analysis and Evaluation of a Wired/Wireless Hybrid Architecture for Distributed Control Systems With Mobility Requirements", IEEE Access, vol. 7, pp. 95915-95931, 2019.
3. C. Cruces, R. Torrego, A. Arriola and I. Val, "Deterministic Hybrid Architecture with Time Sensitive Network and Wireless Capabilities," 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Turin, Italy, pp. 1119-1122, 2018.
4. O. Seijo, Z. Fernández, I. Val, and J. A. López-Fernández, "SHARP: A novel hybrid architecture for industrial wireless sensor and actuator networks," 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), pp.1-10, 2018.
5. M. Luvisotto, Z. Pang and D. Dzung, "High-Performance Wireless Networks for Industrial Control Applications: New Targets and Feasibility," Proceedings of the IEEE, vol. 107, no. 6, pp. 1074-1093, June 2019.
6. Michele Luvisotto; Dacfey Dzung, “Wireless High-Performance Communications: The

Challenges and Opportunities of a New Target", IEEE Industrial Electronics Magazine, Volume: 11, Issue: 3, Pages: 20-25, 2017.

7. Henrik Hellström, Michele Luvisotto; Roger N. Jansson, Zhibo Pang; "Software-Defined Wireless Communication for Industrial Control: A Realistic Approach Time-Sensitive Networking", IEEE Industrial Electronics Magazine, December 2019.
8. Ming Zhan; Zhibo Pang; Dacfey Dzung; Michele Luvisotto; Kan Yu; Ming Xiao, "Towards High-performance Wireless Control: $10e^{-7}$ Packet Error Rate in Real Factory Environments", IEEE Transactions on Industrial Informatics, 2019.
9. Fei Pan, Zhibo Pang, Michele Luvisotto, Ming Xiao, Hong Wen, "Physical Layer Security for Wireless Industrial Control Systems: Basics and Future Directions", IEEE Industrial Electronics Magazine, Volume: 12, Issue: 4, Page(s): 18-27, December 2018.
10. Xiaolin Jiang, Zhibo Pang, Michele Luvisotto, Fei Pan, Richard Candell, Carlo Fischione, "Using Large Data Set to Improve Wireless Communications: Latency, Reliability, and Security", IEEE Industrial Electronics Magazine, Vol 13, Issue 1, pp6-12, 2019.
11. Karl Montgomery, Richard Candell, Yongkang Liu, and Mohamed Hany, "Wireless User Requirements for the Factory Workcell", NIST Advanced Manufacturing Series 300-8, September 2019. [Online] Available: https://doi.org/10.6028/NIST.AMS.300-8
12. L. Bello and W. Steiner, "A Perspective on IEEE Time-Sensitive Networking for Industrial Communication and Automation Systems," Proceedings of IEEE, Vol 107, No. 6, June 2019.
13. D. Cavalcanti et al, "Extending Accurate Time Distribution and Timeliness Capabilities over the Air to enable Future Wireless Industrial Automation Systems," Proceedings of the IEEE, Vol 107, No.6, June 2019.
14. G. Venkatesan, et al, "Performance Evaluation of IEEE 802.1AS-based Time Distribution over 802.11", Poster presented at the 2019 International IEEE Symposium on Precision Clock

Synchronization (ISPCS), Portland, OR, USA, September 2019.

15. M. Eisen, et al, “Control Aware Radio Resource Allocation in Low Latency Wireless Control Systems,” IEEE Internet of Things Journal, Vol. 6, No. 5, October 2019.
16. IEC 62443-1-1: Industrial communication networks- Network and system security-Part 1-1: Terminology, concepts and models (IEC/TR 62443-1-1:2009).
17. SCOTT Secure Connected Trustable Things (737422), Research Project, H2020 ECSEL-IA, 2017-05-01 to 2020-06-30, [Online] Available: https://scottproject.eu
18. M. Tarkowski, M. Rzymowski, L. Kulas and K. Nyka, "Improved jamming resistance using electronically steerable parasitic antenna radiator", IEEE EUROCON 2017 -17th International Conference on Smart Technologies, Ohrid, pp. 496-500, 2017. doi: 10.1109/EUROCON.2017.8011161
19. L. Liu, G. Han, S. Chan and M. Guizani, "An SNR-Assured Anti-Jamming Routing Protocol for Reliable Communication in Industrial Wireless Sensor Networks", IEEE Communications Magazine, vol. 56, no. 2, pp. 23-29, February 2018. doi: 10.1109/MCOM.2018.1700615
20. Guodong Zhao, Muhammad Ali Imran, Zhibo Pang, Zhi Chen, Liying Li, “Towards Real-Time Control in Future Wireless Networks: Communication-Control Co-Design”, IEEE Communications Magazine, Vol. 57, Iss. 2, 2019.
21. Reliable, High Performance Wireless Systems for Factory Automation, National Institute of Standards and Technology, 2018. [Online] Available: https://www.nist.gov/programs-projects/reliable-high-performance-wireless-systems-factory-automation
22. N. Ballber Torres, B. Etzlinger, E. Dehmollaian and A. Springer, "TDOA-enhanced Distance Bounding in the Presence of Noise", 16th IEEE International Conference on Factory Communication Systems (WFCS), Portugal, Porto, pp.1-6, 2020.

23. H-P. Bernhard, J. Karoliny, B. Etzlinger, A. Springer, Work-In-Progress paper, “RSSI-Based Presence Detection in Industrial Wireless Sensor Networks”, 16th IEEE International Conference on Factory Communication Systems (WFCS), Portugal, Porto, pp. 1-4, 2020.