Industrial Wireless: Problem Space, Success Considerations, Technologies, and Future Direction

Richard Candell, *Senior Member, IEEE* and Mohamed Kashef, *Member, IEEE*

***Abstract*—The use of wireless technologies within factories demands a comprehensive understanding of the problems and potential solutions associated with the rigors of the manufacturing environment. A clearly defined problem space would significantly ease the selection and deployment of appropriate wireless solutions to connected factory systems. A mapping of potential technologies to classes of use cases within the problem space will be useful to factory operators, system integrators, and wireless systems manufacturers. Identification of use cases, not addressed by existing technologies, may be used to spur targeted innovation where reliability, resilience, latency, and scalability are joint concerns. Motivated by the industry need for independent practical guidelines and solutions to difficult wireless control problems, this paper provides a classification of the problem categories where networking technologies may be deployed. It then maps specific technologies that may serve as interim or terminal solutions for those use cases identified within the problem space taxonomy.**

***Index Terms*—industrial wireless, industrial communication, industrial control, networked control, manufacturing, cyber-physical systems, taxonomy**

I. Introduction

A. Purpose

Industrial wireless is a key enabling technology for the Industrial Internet of Things (IIoT). The IIoT promises lower costs of deployment, increased mobility of factory assets, massive interconnectivity, improved situational awareness, increased efficiency of the operation, and improved operations analytics. IIoT and advanced manufacturing technology seek to improve competitiveness, productivity, and responsiveness to customer needs. However, it is often stated that where wireless is deployed, factory enhancements fail to meet expectations typically in areas of reliability, resilience, and scalability. Moreover, transmission security is often cited as an area of concern. Risk averse organizations will establish policies that preclude wireless to be deployed for specific types of applications such as feedback control or safety. Yet, factory operators are increasingly demanding that wireless be deployed for critical and sometimes perceivably dangerous applications. For this reason, the National Institute of Standards and Technology (NIST) is developing best practice guidelines to help factory operators select appropriate wireless systems for their particular use case and then deploy that solution effectively. Such a mission requires participation by factory operators, system integrators, and device manufacturers. A comprehensive taxonomy of the existing problem space within industry and a survey of existing and missing technologies are necessary to the success of such a mission. This paper provides our classification of industrial wireless cases and links current technologies to those use cases if applicable.

R. Candell is with Intelligent Systems Division, Engineering Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, USA 20899 (e-mail: richard.candell@nist.gov).

M. Kashef is an associate researcher with Advanced Networking Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, USA 20899 (e-mail: mohamed.hany@nist.gov).

B. Related Work

The use of industrial wireless networks has been studied in many works in the literature. However, no comprehensive survey of the whole problem space of industrial communications has been performed.

In [1], the authors have introduced a comparison between the commercial and industrial communications networks where an industrial network has been divided to five different levels. These levels include field equipment, controller level, application, supervisory, and external networks. The differences in requirements between different levels are discussed. Moreover, three types of information are considered which are control, diagnostic, and safety information as described in [2]. However all these levels of industrial networks are mentioned in [1], the article focuses only on the manufacturing and instrumentation communications and does not consider other types of communications networks that exist in industrial environments. Also, in [3], three levels of communications are considered which are device, control, and information levels. Moreover, the current wired industrial technologies for these levels are discussed briefly.

More works focused on the communications at the field devices level where sensing and control information is transfered. In [4], the communication between field devices has

been studied where the requirements for a large number of nodes may not be achieved. The use of fieldbus solutions limit the scalability and resilience and hence industrial Ethernet capabilities are introduced in this article. Moreover, in [5], the communication for monitoring and control operations is discussed. A comparison between fieldbus technologies, industrial Ethernet, and wireless solutions is performed. The author has discussed the use of Wi-Fi, Bluetooth, ZigBee, and WirelessHART technologies in industrial applications. Similarly, the authors of [6] considered the industrial communications networks requirements in process automation specifically at field devices level. Finally, in [7], many case-studies are discussed for communication networks in industrial scenarios. Moreover, the design steps for these solutions are briefly discussed.

C. Paper Organization

The rest of the paper is organized as follows. The problem space for employing wireless networks is presented in Section II. Then, the technical considerations while designing industrial wireless networks are discussed briefly in Section III. In Section IV, a mapping between the problem space and the current technology space is provided. Finally in Section V, future directions and conclusions are presented.

II. Problem Space

A. Introduction and Success Considerations

Implementing a factory enhancement program requires economic and technical planning, and justification. Wireless technologies by themselves are interesting and can provide value; however, it is incumbent upon plant leadership to fully assess the potential risks and benefits of the enhancement before proceeding with deployment. Wireless technologies are often deployed as a means to monitor or control factory process. They have the potential to unlock improved observability and control. By understanding the problem space and the risks and benefits of potential wireless solutions, factory operators can assess if the rewards outweigh the risks. In navigating the risk/reward question, we assert that any wireless program must address one or more of the following success criteria before embarking on an enhancement involving wireless communications.

a) Reliability: Wireless systems can be deployed to add redundancy or replace faulty wired solutions with a more reliable wireless solution for particularly harsh industrial environments where temperature, pressure, vibration, radiation, and chemistry may make wired communication unreliable.

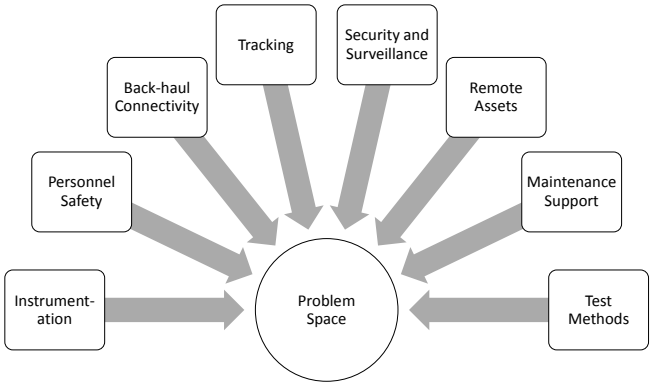

Fig. 1. Industrial wireless technologies are applicable across most aspects of an industrial operation.

b) Safety: Wireless systems may be used to detect or prevent injury to humans. They may be used as backup to wired systems or serve as the primary communication system.

c) Production Cost: Wireless systems can increase observability and the resulting data may be used for precise optimization of the factory operations, machine scheduling, and maintenance.

d) Quality: Various measurements are possible to improve quality of the factory output. Using wireless solutions may make deployment of sensors and inspection equipment more practical.

e) Environment: Wireless sensors and control mechanisms may be used to detect toxic conditions and prevent environmental accidents from occurring. Wireless actuation devices may serve to improve reliability and address environmental mitigation control.

f) Regulations: In some scenarios, government regulations may require specific sensor instrumentation to be deployed for certain scenarios. Wireless solutions could make regulatory compliance practical or cost effective in some cases.

B. Use Cases

Once a plant upgrade enhancement program is initiated, and some type of wireless technology is anticipated, the first step in realizing the program is defining and understanding the problem space where wireless technologies will be used. To support this assessment, we provide a taxonomy of industrial use cases to which wireless communication may be employed. The industrial wireless landscape is diverse, and a classification of those technologies can be helpful in mapping particular technologies to an application. Our classification is shown in Fig. 1 and includes instrumentation, safety, and backhaul connectivity, among others. Each class of the problem space is explained in the following subsections.

1) Manufacturing Instrumentation: Manufacturing instrumentation includes devices commonly known as sensors and actuators. Sensors transmit measured variables from the physical process. Actuators receive manipulation variables from a controller and apply changes to the physical process. This class of application demands typically a very low latency and high reliability communication channel.

2) Personnel Safety: Industrial settings can be hazardous to both humans and machines. For humans, conditions may arise that pose a substantial risk for injury or death. For machines, conditions may develop that cause substantial damage requiring extensive repair or replacement. Prevention of industrial accidents is therefore of paramount importance within factories [8]. Slips, trips, and falls on the same level are commonly cited as lead causes of injury [9]. Falls from higher levels are of great concern to the aerospace industry [10] as inspection teams must work on elevated levels where falls prove fatal. Within the oil and gas industry, safety concerns include air toxicity and combustibility in both open and confined spaces where reliable monitoring and reporting save lives. Wireless gas leak detection and leak localization provide important and effective safety enhancements to such systems [11]. Within smart manufacturing systems where humans and robots work closely and even within traditional robot environments, safety systems provide an added layer of protection to prevent human injury [12], [13]. Within these human-robot environments, it is clear that reliable, low-latency communication is an important aspect of safety implementation, and, as mobility of robots within the factory increases, reliable low-latency wireless networks will become increasingly important to safety implementation.

3) Back-haul Connectivity: The back-haul is generally defined as the network that connects a lower level network to a higher level network [14]. Back-haul connectivity is usually characterized by large amounts of transfered data. In industrial environments, various types of back-haul scenarios are needed to be deployed for the operation of industrial communication networks. We can divide the back-haul problem space into three partitions which are i) nearby or indoor back-hauls, ii) distant back-hauls, and iii) geographically remote back-hauls. This categorization is based on the distance over which data is transfered.

First, the indoor back-haul networks are used in factory floors or process plants for data transfer between the control level networks to data centers, and higher level application layer networks. Second, the distant back-hauls are used for information transfer between various buildings in a plant where the two ends may have a line of sight (LOS) or need a non-LOS (NLOS) technology [15]. Finally, the geographically remote back-hauls are used for information transfer between sites in different cities or even countries such as data transfer to headquarters. Various technologies which are currently used for back-haul networks are discussed in [15].

4) Tracking: Tracking in industrial environments is employed to follow the states of inventory, personnel, and tools which help in process control and factory management [16]. The focus of this class of the problem space is the set of transmissions related to the tracking process itself and not the recovered data transmissions back to higher levels. We categorize the tracking wireless systems to the following divisions based on various requirements: i) materials tracking, ii) personnel tracking, iii) tools tracking, iv) inventory management, v) localization, and vi) identification.

Materials, personnel, and tools tracking is focused on following the state and the location of the tracked item. The selection of the used technology will depend on the tracked item characteristics including its speed, required accuracy level, and scalability [17]. Inventory management includes the decisions related to the change of inventory status over time. Identification and localization are required for the determination of the position and identity of a person or an item at a specific situation or time. It can be important in safety and security related applications.

The characteristics and applications of various tracking, localization, and identification technologies are discussed in [16]. These technologies include the use of specific wireless communications technologies like the global positioning system (GPS), and the radio-frequency identification (RFID) or deploying the general-purpose technologies like Wi-Fi, Bluetooth, and the cellular-based technologies. Moreover, examples of the existing products for assets tracking and their performance are compared in [17].

5) Security and Surveillance: Industrial installations require protection of the physical grounds, the operation, and the data produced from the installation. This protection requires surveillance of the property and implementation of network security controls. Guidance on selecting which controls are applicable to a specific risk level may be found in [18]. Assessment of the security robustness of specific wireless technologies is outside the scope of this paper; however, the implementation of physical security controls such as personnel authorization and grounds protection requires transmission of varying amounts of data. Transmission of such data includes voice traffic, video, and status information. In some installations, security and surveillance transmissions will coexist with factory instrumentation. This is sometimes the case with IEEE 802.11 mesh networks carrying voice, video, and

instrumentation traffic.

6) Remote Assets: Remote monitoring and control extend the range of the management to remote sites, especially in the process industry. Industrial remote communications provide access to widely distributed assets such as well head and pipeline monitoring [19]. The main goals of employing remote monitoring and control are minimizing labor cost, improved operations of remote sites, and prevention of unplanned failures [20].

The use of wireless networks in remote monitoring and control reduces the installation and maintenance cost significantly. However, the main challenge for industrial wireless remote monitoring and control is security and hence encryption and authentication protocols are deployed. Examples of remote assets communications are discussed in [19].

7) Maintenance Support: Factories require maintenance teams to keep machinery operating efficiently. Machines may be instrumented with sensors that measure machine health data such as vibration levels or current calibration values. Using this information, machines can be scheduled for maintenance prior to failure thereby allowing the factory to operate without unexpected interruption. Maintenance of the factory may also include automation of the building and infrastructure for climate control. Heating, ventilation, and air conditioning (HVAC) systems can be automated such that the ambient conditions are controlled. Augmented reality is an emerging technology that promises to bring knowledge to the factory floor allowing maintenance personnel to gain access to information during uncertain situations [21]. Augmented reality is a high-bandwidth application that requires high-reliability, high-throughput wireless connectivity within the factory.

8) Test Methods: Industrial control systems are often intolerant of communication faults and network latency, and often require very high transmission reliability [22]. Depending on the purpose of the wireless network (monitoring, supervisory control, feedback control, or safety monitoring), understanding the system performance of the network may be critical. For feedback control and safety monitoring systems, understanding the performance of the network from the perspective of the industrial controller or safety alarm system is essential. Factory operators, system integrators, and control systems designers are rarely experts in wireless communications systems. Considerations such as electromagnetic propagation, antenna efficiency, path loss exponents, packet error rates, and medium access are often foreign concepts to factory engineers. If factory engineers are expert in wireless theory and design practice, the information that they need to make educated decisions are usually unavailable. When available, link quality metrics such as packet loss ratios are informative but can be difficult to understand with complex mesh architectures and routing algorithms.

Moreover, it is generally difficult to measure these quantities for operational networks. The control system designer will only need to know the statistical distribution of latency and reliability of information through the network to design a controller that is robust. Therefore, practical methods for characterizing the performance of the wireless network that do not require an in-depth understanding of wireless communications or electromagnetic wave propagation are needed.

III. Technical Considerations

A. Radio Frequency (RF) Environment

Using wireless communications in industrial environments requires the knowledge of the RF environment characteristics and their behavior under the added wireless networks. The first step is obtaining and modeling field data in industrial environments. In [23], the RF environments of multiple examples of industrial scenarios were studied where models and characterization parameters have been derived. Moreover, theoretical models are proposed to model the RF channel such as the IEEE802.15.4a model including its channel impulse response [24]. In characterizing the RF environments, various parameters should be included, such as the multi-path, the interference sources, the mobility, and shadowing effects. Moreover, the operating frequency band can play an important role based on the required performance and the nature of RF activity in a certain environment.

B. Device Characteristics

Another important aspect while deploying wireless networks in industrial environments is the used devices characteristics. Typically, the harsh industrial environments in many applications require higher ratings of the used devices. The considered device characteristics include size, weight, power, cost, safety, and ingress protection (IP) ratings. Based on the application requirements and the physical environments, these device requirements are determined.

C. Network Characteristics

Table I lists requirements typically expected of a network based on its intended purpose and problem domain. Industrial networks will have three basic characteristics: reliability, latency, and scale. These characteristics are described in the following subsections. The numbers listed in the table are based on existing applications. It is difficult to provide a standard metric for all use cases as each will impose different requirements on the network. In some cases, the control algorithm can be designed to adapt to information loss and

delay, thereby improving the performance of the physical system.

1) Latency: is a measure of the delay that information takes to arrive at its destination. We define latency, l, as the measured delay from the time of an event to the time in which knowledge of that event is made available to an application. Using the Open Systems Interconnection (OSI) model as a guide, latency would be measured at the application layer. In a packaging system, an example of measured latency would be the time between a proximity event and the time knowledge of that event is received by a programmable logic controller.

2) Reliability: is a measure of the likelihood of data loss within the industrial network. We define reliability, r, as the probability that a block of transmitted data is delayed long enough to become obsolete or lost due to noise. Similar to latency, we measure reliability at the application layer thereby ignoring technology-specific issues such as data segmentation and retries similar to the approach taken in the developing 5G cellular networks for machine-to-machine communications [25].

3) Scale: is a measure of the number of devices that may be deployed within a network without sacrificing reliability or latency. The network size will often dictate the maximum bandwidth allotted to any one node. The larger the network, the less bandwidth is alloted for transmissions between nodes. The complexity of a fully interconnect mesh will theoretically exhibit factorial growth in network interconnections. In practice, signal-to-noise ratios between nodes, programming within the governing network controller, and provisioned constraints will limit the number of interconnections. Most wireless sensor network specifications such as WirelessHART, ISA100.11a, and Zigbee provide support for large scale deployments; however, in such deployments, the network infrastructure must support the throughput load of the network and the scan rate requirements of the factory application [26]. The ISA100.11a standard provides support for distributed access points, prescribed routing, and a partitioned architecture to allow for large-scale deployments.

4) Interoperability: In a factory application, easy integration of devices is essential to the flow of data through a network. While many wireless standards exist, making physical layer integration of devices within the wireless domain easier, most industrial networks fail to address the application layer well. WirelessHART describes an application layer interface, while ISA100.11a provides the constructs for such an interface. ZigBee and Wi-Fi provide neither the interface nor the constructs for an application layer protocol. On the back-haul side of wireless networks which usually begins at a wireless gateway and ends at an automation server, many protocols such as Open Platform Communications (OPC) and Modbus make integration easier; however, again, they fail to specify the interface but instead provide the constructs. The authors assert that a standardization of the automation interface (gateway to automation server) is needed to provide such interoperability.

TABLE I
INDUSTRIAL CONTROL LATENCY, ERROR RATE, AND SCALABILITY CONSIDERATIONS FOR WIRELESS DEPLOYMENTS.

	Latency, l ms	Pr. Loss, r	Scale, s
Monitoring	$l < 1000$	$r < 10^{-5}$	$s < 10,000$
Supervisory Control			
Flow-based	$l < 1000$	$r < 10^{-6}$	$s < 30$
Job-based	$l < 100$	$r < 10^{-7}$	$s < 10$
Feedback Control			
Flow-based	$l < 1000$	$r < 10^{-6}$	$s < 100$
Job-based	$l < 10$	$r < 10^{-7}$	$s < 10$
Safety	$l < 10$	$r < 10^{-7}$	$s < 10$

5) Security: Prescribing security controls within an automation system requires understanding of the risk of not implementing these controls and the impacts of them on the physical process. Work is being undertaken to measure the impacts of cybersecurity controls on the physical process as explained in [27] and [28]. In addition, the work is being undertaken to assess the impacts of stealthy attacks as described in [29]. NIST Special Publication 800-82 and IEC-62443 provide best practice guidelines for the implementation of a cybersecurity program in an automation system.

IV. WIRELESS TECHNOLOGY APPLICABILITY

Many existing wireless technologies could be applied to the use cases in Section II. Others may be applicable with limitations, and others are not applicable entirely. Table II captures mapping of technologies to applicable use cases. This table represents assertions by the authors of applicability of wireless technologies to industrial control systems problem domains based on industry practice and original intent of the technology. The authors assert that the problem domains and wireless technologies included within this table represent the majority of problems found within industry and the existing technologies that may be applied. Technologies were evaluated based on original design intent, latency, reliability, energy, and practicality. Modifications may be made to the listed technologies resulting in applicability to a specified problem; however, possible modifications were not considered. Very low bit rate (VLBR) wide area networks (WAN) are assumed to have an infrastructure-based topology and support a bit rate of under 600bps.

TABLE II
ASSERTED APPLICABILITY OF WIRELESS TECHNOLOGIES.

		Process Monitoring	Supervisory Control	Feedback Control	Alarm Conditions	In-situ Inspection	Factory Monitoring	Assembly: Sensing	Assembly: Actuation	Robots: Supervision	Robots: Feedback Control	Quality Inspection	Fall Prevention	Confined Spaces	Critical Event Detection	Human-Machine Colocation	Nearby or Indoor	Distant: LOS	Distant: BLOS	Geographically Remote	Indoor Machine Localization	Materials in Storage	Materials in Production	Tools	Personnel	Voice and Video Communication	Video Surveillience	Drone-based Surveillance	Grounds Control	Spectrum Monitoring Data	Personnel Authorization	Well-head Monitoring	Pipeline Monitoring	Tank Level Monitoring	Machine Health Monitoring	Building Automation	Augmented Reality
		Flow-based					Job-based						Safety				Back-haul				Tracking					Security						Remote			Maint.		
Home/Office	IEEE 802.11	●	●	◐	◐	-	●	◐	◐	◐	◐	◐	○	○	◐	○	●	●	●	-	◐	ϟ	ϟ	ϟ	ϟ	●	●	●	●	●	●	◐	○	◐	◐	●	●
	IEEE 802.15.1	○	○	○	○	○	○	◐	◐	◐	○	●	○	◐	○	○	○	○	○	○	○	○	ϟ	●	◐	▼	▼	▼	○	○	◐	○	○	○	◐	○	▼
Industrial	IEEE 802.15.4 TDMA	●	●	◐	◐	-	●	◷	◷	◷	◷	◐	◷	◐	◐	○	▼	▼	▼	▼	◐	ϟ	ϟ	ϟ	◐	▼	▼	▼	◐	▼	○	●	●	●	●	●	▼
	IEEE 802.15.4 CSMA	◐	◐	○	○	-	●	◷	◷	◷	◷	◐	◷	◐	◐	○	▼	▼	▼	▼	◐	ϟ	ϟ	ϟ	◐	▼	▼	▼	◐	○	○	◐	◐	◐	●	●	▼
	IEEE 802.11 TDMA	⚹	⚹	⚹	⚹	-	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	-	-	-	-	⚹	-	-	-	-	-	-	-	⚹	-	-	⚹	⚹	⚹	⚹	⚹	-
	VLBR WAN	●	●	○	◐	-	●	◷	◷	◷	◷	◷	◷	○	○	○	▼	▼	▼	▼	◐	◐	◐	◐	◐	▼	▼	▼	◷	○	○	○	○	○	◐	◐	○
Satellite	Geostationary	◐	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	○	○	○	○	○	◐	◐	○	◐	◐	◐	◐	◐	◐	○	○	◐
	Low-earth Orbit	◐	◐	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	◐	◐	○	○	○	○	○	◐	◐	◐	◐	◐	◐	◐	◐	◐	◐	○	◐
	VLBR WAN	◐	◐	○	◐	○	◷	◷	◷	◷	◷	◷	◷	○	○	○	▼	▼	▼	▼	○	○	○	○	◐	▼	▼	▼	◐	○	○	○	○	○	◐	○	▼
Tracking	RFID	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	○	●	●	●	●	-	-	-	-	-	-	-	-	-	-	-	-
Optical	Indoor Dispersive	⚹	⚹	⚹	⚹	○	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	○	○	○	⚹	ϟ	ϟ	ϟ	ϟ	⚹	⚹	○	○	⚹	○	○	○	○	⚹	○	○
	Free-space	◐	◐	◐	◐	○	○	○	○	○	○	○	○	○	○	○	●	●	●	○	◐	○	○	○	○	●	●	○	○	○	○	○	●	○	●	○	○	●
Cellular	Legacy	◐	◐	○	○	-	○	○	○	○	○	○	◷	◷	◷	◷	◐	◐	◐	◐	○	○	○	○	○	○	○	○	○	⚹	◐	◐	◐	◐	▼	▼
	4G	◐	◐	○	◷	-	○	○	○	○	○	○	◷	◷	◷	◷	◐	◐	◐	◐	○	○	○	○	○	●	●	◐	●	●	●	◐	◐	◐	○	○	○
	5G	⚹	⚹	⚹	⚹	-	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	●	●	●	○	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹	⚹
Land-mobile	All types	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	▼	▼	○	○	○	○	○	○	○	◐	○	○	●	○	◐	○	○	○	○	○	○
Specialty	Leaky Coax	◐	◐	-	◐	◐	◐	-	-	○	○	-	○	◐	◐	-	◐	○	○	○	◐	●	●	○	○	○	○	○	●	○	●	○	○	○	◐	◐	○

Legend: ●: Technology fully supports problem domain, ◐: Supports problem domain with practicality, throughput, latency, reliability, or energy limitations, ϟ: Energy requirements of assumed battery-powered devices prevent applicability, ◷: Latency prevent applicability, ▼: Throughput prevents applicability, ⚹: Emerging technology or evolution may support problem domain, ○: Not recommended, -: Not considered by authors.

V. CONCLUSIONS

This work represents a step toward employing wireless technologies in industrial environments where all classes of problems which wireless technologies can be used to solve have been comprehensively and collectively discussed. The success criteria and the technical aspects for employing wireless technologies in various scenarios have been considered briefly. More work is needed where success criteria are to be quantified and prioritized for various industrial scenarios. More detailed discussion is needed regarding technical considerations while employing wireless networking, including the physical environmental aspects such as the factory floor parameters, obstructions, data models, and interaction between various items within the factory floor. Finally, we have introduced a mapping between technologies and the discussed problem classes to highlight various industrial problems which can be solved or need more work while employing wireless technologies. Multiple comparisons between the current technologies exist in the literature. However, this work initiates consideration of the problem space where wireless technologies are employed. NIST has introduced this work while continuing to develop its capabilities as described in [28] to explore applicability of wireless technologies to specific industrial scenarios capable of replication within a laboratory space. An RF channel emulator is used to simulate the RF environment to include fading and multipath. A technical working group was created to directly address the needs of the wireless users employing wireless within their factories.

DISCLAIMER

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to

imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

ACKNOWLEDGMENT

The authors would like to thank the participants of the 2017 IEEE Applications Systems Symposium Industrial Wireless Workshop for valuable inputs and discussions regarding the topics covered in this article.

REFERENCES

[1] B. Galloway and G. P. Hancke, "Introduction to industrial control networks," *IEEE Communications Surveys Tutorials*, vol. 15, no. 2, pp. 860–880, Second 2013.

[2] J. R. Moyne and D. M. Tilbury, "The emergence of industrial control networks for manufacturing control, diagnostics, and safety data," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 29–47, January 2007.

[3] "What are industrial communication networks? an overview," http://www.electricaltechnology.org/2016/12/industrial-communication-networks-systems.html, accessed: 2017-04-20.

[4] P. Danielis, J. Skodzik, V. Altmann, E. B. Schweissguth, F. Golatowski, D. Timmermann, and J. Schacht, "Survey on real-time communication via ethernet in industrial automation environments," in *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*, Sept 2014, pp. 1–8.

[5] "Connectivity provides the lifeline of industrial control," http://electronicdesign.com/industrial/connectivity-provides-lifeline-industrial-control, accessed: 2017-04-20.

[6] W. Ikram and N. F. Thornhill, "Wireless communication in process automation: A survey of opportunities, requirements, concerns and challenges," in *UKACC International Conference on Control 2010*, Sept 2010, pp. 1–6.

[7] "Industrial communications professional services: Delivering high-performing communication network systems for industrial applications," https://www.gegridsolutions.com/Communications/Professional Services_GEA-12702B-E_160418_R001.pdf, accessed: 2017-04-20.

[8] D. Smith, B. Veitch, F. Khan, and R. Taylor, "Understanding industrial safety: Comparing fault tree, bayesian network, and {FRAM} approaches," *Journal of Loss Prevention in the Process Industries*, vol. 45, pp. 88 – 101, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0950423016304260

[9] W.-R. Chang, S. Leclercq, T. E. Lockhart, and R. Haslam, "State of science: occupational slips, trips and falls on the same level," *Ergonomics*, vol. 59, no. 7, pp. 861–883, 2016, pMID: 26903401. [Online]. Available: http://dx.doi.org/10.1080/00140139.2016.1157214

[10] R. Candell, "NIST-IR Report on Industrial Wireless Systems Workshop," 2017, to appear.

[11] F. Chraim, Y. B. Erol, and K. Pister, "Wireless gas leak detection and localization," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 768–779, April 2016.

[12] A. Huber and A. Weiss, "Developing human-robot interaction for an industry 4.0 robot: How industry workers helped to improve remote-hri to physical-hri," in *Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction*, ser. HRI '17. New York, NY, USA: ACM, 2017, pp. 137–138. [Online]. Available: http://doi.acm.org/10.1145/3029798.3038346

[13] A. M. Zanchettin, N. M. Ceriani, P. Rocco, H. Ding, and B. Matthias, "Safety in human-robot collaborative manufacturing environments: Metrics and control," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 2, pp. 882–893, April 2016.

[14] M. Jaber, M. A. Imran, R. Tafazolli, and A. Tukmanov, "5g backhaul challenges and emerging research directions: A survey," *IEEE Access*, vol. 4, pp. 1743–1766, 2016.

[15] "Wireless backhaul spectrum policy recommendations and analysis," http://www.gsma.com/spectrum/wp-content/uploads/2014/12/Wireless-Backhaul-Spectrum-Policy-Recommendations-and-Analysis-Report.-Nov14.pdf, accessed: 2017-04-20.

[16] A. Khudhair, S. Jabbar, M. Sulttan, and D. Wang, "Wireless indoor localization systems and techniques: Survey and comparative study," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 3, no. 2, pp. 392–409, August 2016.

[17] "Asset tracking and inventory systems market survey report," https://www.dhs.gov/sites/default/files/publications/Asset Tracking and Inventory Systems Market Survey Report December 2016.pdf, accessed: 2017-04-20.

[18] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep., jun 2015. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[19] "Industrial remote communication: Efficient remote access to plants, machines and mobile applications," https://www.industry.usa.siemens.com/automation/us/en/industrial-communications/remote/Documents/E20001-A660-P820-X-7600_WS_Remote_Communication_web.pdf, accessed: 2017-04-20.

[20] G. Philbrook, "Remote monitoring technologies lower costs, improve operations," http://www.plantengineering.com/single-article/remote-monitoring-technologies-lower-costs-improve-operations/8242e6952a7fd3ded0e608602cef4f3d.html, accessed: 2017-04-20.

[21] V. Paelke, "Augmented reality in the smart factory: Supporting workers in an industry 4.0. environment," in *19th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2014*, 2014.

[22] L. Zhang, H. Gao, and O. Kaynak, "Network-Induced Constraints in Networked Control Systems: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 403–416, 2013.

[23] R. Candell, C. Remley, J. Quimby, D. Novotny, A. Curtin, P. Papazian, G. Koepke, J. Diener, and M. Kashef, "Industrial wireless systems: Radio propagation measurements," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep., 2017. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1951.pdf

[24] A. F. Molisch, "IEEE 802.15.4a channel model-final report IEEE P802 15.04," Tech. Rep., 2004.

[25] B. Holfeld, D. Wieruch, T. Wirth, L. Thiele, S. A. Ashraf, J. Huschke, I. Aktas, and J. Ansari, "Wireless communication for factory automation: an opportunity for lte and 5g systems," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 36–43, June 2016.

[26] Q. Wang and J. Jiang, "Comparative examination on architecture and protocol of industrial wireless sensor network standards," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 2197–2219, thirdquarter 2016.

[27] R. Candell, T. Zimmerman, and K. Stouffer, "An industrial control system cybersecurity performance testbed," *National Institute of Standards and Technology. NISTIR*, vol. 8089, 2015.

[28] R. Candell and K. Lee, "Measuring the effect of wireless sensor network communications on industrial process performance," in *2015 ISA process control and safety symposium, Houston, TX*, 2015.

[29] D. I. Urbina, J. A. Giraldo, A. A. Cardenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, and H. Sandberg, "Limiting the impact of stealthy attacks on industrial control systems," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 1092–1105.