

# Future Research Challenges in Wireless Sensor and Actuator Networks Targeting Industrial Automation

Johan Åkerberg

ABB AB

Corporate Research

Email: johan.akerberg@se.abb.com

Mikael Gidlund

ABB AB

Corporate Research

Email: mikael.gidlund@se.abb.com

Mats Björkman

Mälardalen University

School of Innovation, Design, and Technology

Email: mats.bjorkman@mdh.se

**Abstract**—A growing trend in the automation industry is to use wireless technologies to reduce cable cost, deployment time, unlocking of stranded information in previously deployed devices, and enabling wireless control applications. Despite a huge research effort in the area of wireless sensor networks (WSNs), there are several issues that have not been addressed properly such that WSNs can be adopted properly in the process automation domain.

This article presents the major requirements for typical applications in process automation and we also aim to outline the research direction for industrial wireless sensor networks (IWSNs) in industrial automation. The major issues that need to be addressed are safety, security and availability before industrial wireless sensor networks will be adopted in full scale in process automation.

## I. INTRODUCTION

Reliable wireless communications systems and particularly industrial *wireless sensor and actuator networks* (WSANs) are removing the physical and economical barriers that previously made it difficult or impossible to access many types of information in the process industry. The main concerns about reliability, security, and integration along with the lack of device interoperability have hampered the deployment rate. There exists a lot of work on employing IEEE 802.15.4 and ZigBee in process automation. However, ZigBee seems unsuitable for this application field as it has not been specifically designed for reliable real-time cyclic communication [1]. One of the major problems with using the complete IEEE 802.15.4 standard is for large networks where synchronization is a huge problem. WirelessHART [2], the first open and interoperable wireless communication standard designed specifically for real-world applications in process automation, was approved and released in 2007. ISA 100.11a [3] is likely to become a standard for process and factory automation. Both WirelessHART and ISA 100.11a adopt the complete IEEE 802.15.4 PHY layer, but they propose a new MAC layer which combines TDMA and channel hopping to control access to the network. Both WirelessHART and ISA 100.11a are mainly targeting applications such as condition monitoring which has quite relaxed requirements on latency. However, for more time critical applications it is likely that some improvements in current standards are needed.

There exists a significant research work done with respect to wireless mesh networks in general. Willig [4] discuss in

detail many recent and emerging topics in general for wireless industrial communications. However, many of the research opportunities foreseen are too general in order to address the urgent needs for process automation domain. Akyildiz and Wang present a detailed investigation of current state-of-art protocols and algorithms for wireless mesh networks [5]. Furthermore, they outline some open research issues in all protocol layers. However, their survey is targeting more consumer applications, where the requirements are different compared to large scale industrial manufacturing. Yick *et al.* [6] present a similar but updated overview of the work by Akyildiz and Wang. Zheng describes very briefly the current situation of IWSN and ongoing standardization activities [7]. Hou and Bergmann present a brief survey of design requirements for condition monitoring using commercial *industrial wireless sensor networks* (IWSNs) systems [8]. Nevertheless, their article does not discuss several important requirements such as safety, security, and availability. Gungor and Hancke present a brief overview of technical challenges and design principles in terms of hardware and software development, system architectures, and protocols for IWSNs [9]. Specifically, radio technologies, energy-harvesting techniques, and cross-layer designs for IWSNs are discussed. As can be seen, there exist some good research work outlining challenges for wireless sensor networks in industrial automation but most of them lack discussions about issues related to safety, security and how to handle actuators which are the main concerns in process automation today. Routing is an important area of research with respect to IWSN. Heo *et al.* [10] address routing with respect to real-time performance and energy awareness.

This article presents typical requirements from process automation for some different applications intended to be used in industrial wireless sensor and actuator networks. Given these requirements, it is obvious that today's commercial WSN are not tailored for the needs of industrial automation, since they are mostly influenced upon requirements derived from the consumer market or other applications. Furthermore, with the requirements for process automation in mind we describe the major challenges that need to be solved in order to utilize the WSANs to the extent the market foresees.

The rest of this paper is organized as follows. In Section II, we discuss the main drivers and benefits of using wireless sensor networks in industrial environments and highlight some

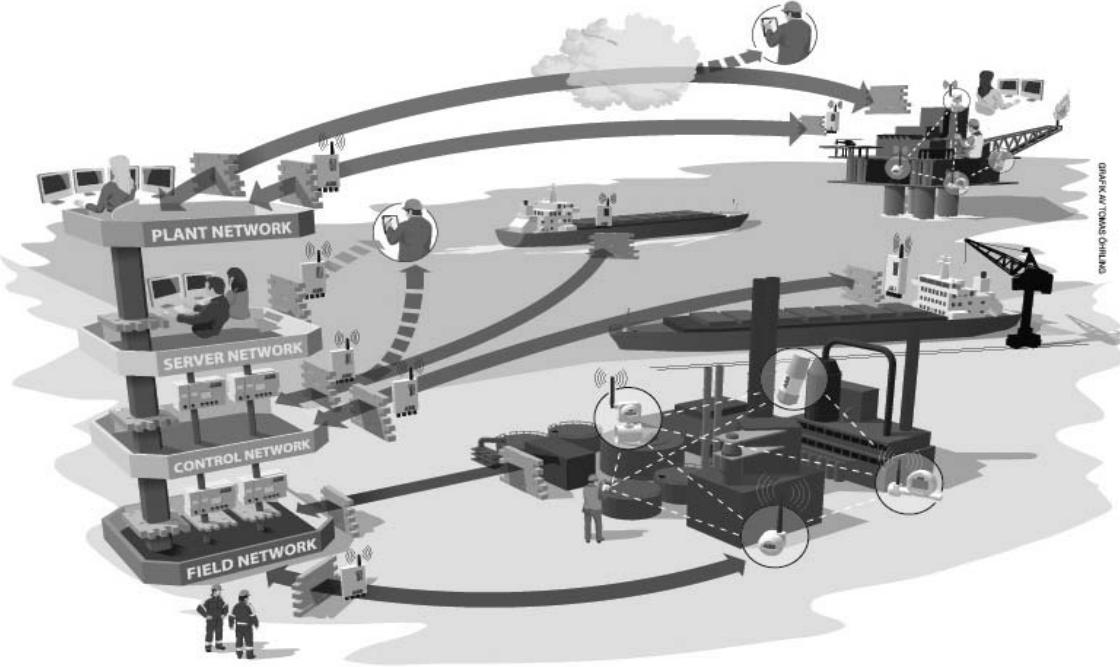


Fig. 1. Future wireless infrastructure and its applications in the process automation domain.

emerging wireless applications. Section III briefly describes the process automation domain and we define the most important requirements for industrial WSANs with respect to process automation. In Section IV, we outline and discuss in detail the major research challenges for industrial WSANs becoming the huge success the industry anticipate. Finally, the paper is concluded in Section V.

## II. THE BENEFITS OF INDUSTRIAL WIRELESS SENSOR AND ACTUATOR NETWORKS

Wireless technology and especially wireless sensor networks has the potential to contribute significantly in areas such as cable replacement, mobility, flexibility and scalability. It offers competitive advantages such as lower life-cycle cost and reducing connector failures which is one of the most common reliability problems. Below we summarize the major advantages of industrial wireless sensor networks.

- *Cost* - With capital at a premium, process manufactures are looking for quick investments that cost little and save even more. The major incitement for adoption of IWSN in process automation (all automation business) is that they are easier and less costly to install than traditional wired systems. Consider a green field installation today, it cost roughly \$200 per meter to install wires in an ordinary process plant, and approximately \$1000 per meter in offshore installations. As wires age they crack or fail. Furthermore, inspecting, testing, troubleshooting, and upgrading wires require time, labor, and materials.
- *Flexibility* - Many secondary process variables have long gone unmeasured, and expensive pieces of critical rotating equipment remain non-instrumented. With the advent

of IWSN, we are able to unlock stranded information in instruments, gather information from where it previously has been economically unfeasible, such that the process can be enhanced with respect to quality and quantity, and reducing the possibility of mechanical failures. Furthermore, another advantage is that IWSN enables temporary measurements of certain process values and quality indicators without installation of additional wires.

- *Emerging Applications* - With the advent of wireless infrastructure and IWSN in process automation several new wireless applications are emerging such as empowering mobile workers, location of assets, safety muster- ing, integration on nontraditional signals such as video, bridging remote or isolated control systems, enabling wireless control applications [11], and allow connectivity for equipment that is “sealed-for-life”.
- *Availability* - Industrial applications require availability and determinism in the automation systems to avoid serious consequences such as injury, explosions, and material losses. Industrial wireless sensor networks can offer built in redundancy and capabilities for anticipatory system maintenance and failure recovery. This could for example be achieved by designing meshed networks where there always exist available links to the control system.

## III. IWSN REQUIREMENTS

In this section we highlight some important requirements that need to be met for a successful large scale deployment of IWSNs in process automation and discrete manufacturing. Some typical examples of process automation industries are: oil and gas, mining, steel, pulp and paper to mention some.

TABLE I  
TYPICAL REQUIREMENTS FOR INDUSTRIAL WIRELESS SENSOR AND ACTUATOR NETWORKS IN THE PROCESS AUTOMATION DOMAIN

Sensor Network Applications	Delay	Range	Battery Lifetime	Update Frequency	Security level
<b>Monitoring and supervision</b>					
Vibration sensor	s	100 m	3 years	sec - days	low
Pressure sensor	ms	100 m	3 years	1 sec	low
Temperature sensor	s	100 m	3 years	5 sec	low
Gas detection sensor	ms	100 m	3 years	1 sec	low
<b>Closed loop control</b>					
Control valve	ms	100 m	> 5 years	10 – 500 ms	medium
Pressure sensor	ms	100 m	> 5 years	10 – 500 ms	medium
Temperature sensor	ms	100 m	> 5 years	500 ms	medium
Flow sensor	ms	100 m	> 5 years	10 – 500 ms	medium
Torque sensor	ms	100 m	> 5 years	10 – 500 ms	medium
Variable speed drive	ms	100 m	> 5 years	10 – 500 ms	medium
<b>Interlocking and Control</b>					
Proximity sensor	ms	100 m	> 5 years	10 – 250 ms	medium
Motor	ms	100 m	> 5 years	10 – 250 ms	medium
Valve	ms	100 m	> 5 years	10 – 250 ms	medium
Protection relays	ms	100 m	> 5 years	10 – 250 ms	medium

The main characteristic that groups them together is that the products are produced in a continuous manner, i.e. the oil is produced in a continuous flow. In discrete manufacturing, the products are produced in discrete steps, i.e. the products are assembled together using sub assemblies or single components. Typical examples of discrete manufacturing industries are automotive, medical, and the food industries. Discrete manufacturing heavily relies on robotics and belt conveyors for assembly, picking, welding, and palletizing. To generalize, discrete manufacturing normally have stricter requirements with respect to latency and real-time requirements compared to process automation. However, as always there are cases when this general assumption is not true. The main reason for this generalized assumption is that in order to pick, assemble, or palletize at high speed, the latency, refresh rates, and real-time requirements are stricter compared to a tank level control in process automation to achieve the required production quality. However, in this paper we focus of process automation, while keeping in mind that requirements might be even stricter for discrete manufacturing.

In Table I, the different types of applications are grouped and listed in three sub-categories:

- *Monitoring, supervision* - this sub-category collects different types of sensors that provide diagnostics and supervision that normally can be pre-processed and transmitted and updated on a period time from 1 second and more. This information is generally not sensitive for packet losses and jitter as it is used for supervision and condition monitoring. However, in some cases data consistency might be important.
- *Closed loop control* - sensors and actuators are connected to PID controllers that control the process with respect to the actual set-point. The purpose of the control loop is to continuously stabilize the (instable) process by controlling the actuators based on the actual sensor readings. Generally, closed loop control is sensitive to jitter and delays.

- *Interlocking and control* - normally the major part of control applications in process control require discrete signaling. For example, before a start command can be issued to a machine, several start conditions have to be fulfilled. A machine might have start, stop, and safety-interlocks. Therefore, interlocking and control signaling are sensitive to delays.

The reason for the separation of closed loop control and interlocking and control is that when closed control is used, the controller can compensate for delays and retransmissions without major degradation of control performance. On the other hand a process interlock, that should for instance stop a machine, is less tolerant for delays and retransmissions as the consequences of delays are most likely to introduce spurious problems in the production or even dangerous situations.

#### IV. RESEARCH CHALLENGES

As previously introduced there are advantages of using IWSNs in process automation. However, there are important requirements that cannot be met in an efficient way today, or cannot be met at all. In this section we discuss some major issues that need to be addressed in order to achieve a large scale deployment of IWSNs. In order to be competitive and cost efficient, we have to consider that the IWSNs needs to solve all requirements that is met today using wired field-buses. The end users will not afford to invest and maintain parallel infrastructures. Secondly, if we cannot meet most of the requirements with IWSNs we need to wire up the field equipment, which is far from optimal. The rest of this section will address some of the most important remaining challenges for a full scale deployment of IWSNs. In addition, we touch upon some research areas that are of less importance in process automation in short to medium term.

##### A. Safety

Safety of humans, environment, and property should always be the number one priority. In process automation some

functions are safety-critical by definition, but most of them are not safety-critical. This does not mean that only the safety-critical functions should be designed, developed, and certified with care [12], as most process automation equipment depend on that the rest of the system operates within the boundaries of the specifications. Even if the functionality is not safety-critical by definition, there can be substantial production losses or damages to the property if the automation equipment is not designed to reduce the risk of uncontrolled or dangerous situations.

The prevention of uncontrolled processes is extremely important. As an example, if a set point from the control system to a control valve cannot be transmitted, the valve should fall back into a safe state (normally closed) after a time out. The time out depends on how long time the process can tolerate a malfunction of the actuator before a possibly dangerous situation occurs, ranging from milliseconds to seconds. In addition to this, the control system should detect this communication loss and indicate the failure. In this way, the rest of the equipment that depend on the correct operation of the control valve is signaled to avoid dangerous situations due to error propagation. Non safety-critical automation equipment is designed such that if a problem can occur, it should be detected and force the process into a safe state. One of the worst scenarios that can occur is that the operator's view in the control room is not consistent with the actual state of the equipment on the factory floor. This implies that field devices cannot have extremely small duty cycles to preserve battery since both the operators and control system will neither get any life sign from the field devices, nor meet the required update frequency.

Some work with safety-critical communication using Wireless HART and PROFINET IO has been done in [13] and the main result is that the IWSNs need to have deterministic and synchronized communication in both the uplink and the downlink in order to avoid spurious fail-safe timeouts.

#### B. Security

Most information that is transmitted to and from field devices is usually normalized valued of the measured entity, i.e. 0-100% of the range of the measuring instrument. In some cases the actual measurement is transmitted along with the SI unit. The control system is collecting information of the state of the process, and the process is controlled based on the collected measurements and the control strategy by transmitting set points for actuators based on the actual state of the process. However, the main point is that it is not confidential information as such that is transmitted. As the confidential information resides inside the control system, i.e. recipes or control strategies, and those are not transmitted on the field networks. However, from a security perspective authentication, integrity, availability, and non-repudiation are important security objectives. With respect to this, the current situation is that confidentiality, authentication and integrity are provided. Here optimizations can be made with respect to security to improve energy consumption, latency, and security

overhead. The most problematic situation besides deliberate manipulation of control data is denial-of-service attacks, which cannot be prevented by cryptography at all. In case of a denial-of-service attack, the automation system will transition into a safe state, if designed correctly.

Secondly, how to integrate the security mechanisms in the overall automation system in an efficient way with respect to key management and replacement of faulty field devices is an important issue. Users of control systems today are used to exchange faulty devices during operation without any additional configuration, i.e. "hot swap", to minimize the downtime.

#### C. Availability

In industrial large-scale production availability is of significant importance. Even short and transient communication errors can cause significant production outages. This is mainly due to that the process has to be stopped in a controlled manner in case of a single communication problem, and it can take up to several hours to achieve full production rate again, with production losses in the range of hundreds of thousands dollars per hour. Self-healing mesh networks are appealing to use in industrial automation for several reasons, i.e. for redundancy, availability, etc [14]. However, in literature it is commonly assumed that routing protocols in industrial settings should be able to deal with mesh networks containing thousands or tens of thousands nodes. Furthermore, it is assumed that all of the devices are battery operated, thus energy aware routing protocols are of significant importance in order to distribute the routing load in a fair manner amongst the nodes [4]. The first assumption is not correct, even though there are tens of thousands of instruments that need to communicate, they do not belong to the same network because of the availability concern. The nodes are distributed over a set of process controllers, divided in several process sections, in order to avoid a complete production stop in case of for example a non-fail-silent situation in one node. Furthermore, energy optimized routing protocols might have a severe and negative impact on the latency and real-time performance of end-to-end communication using mesh networks in the case of link problems caused by fading. In industrial automation the mesh networks would rather benefit of rapid adoptions in routing, in the case of for example fading, while meeting the real-time constraints. Flooding might be one feasible alternative for usage in mission-critical wireless sensor networks [15].

#### D. Latency/retransmission

Due to the nature of automation the data transmitted in the field networks is only valid for a short time. If the data is delivered too late it is of limited use, as in most real-time systems. Therefore new data should be propagated through the network instead of guaranteeing delivery of all transmissions. This is an important area of research, especially within the area of IWSN where it can be mesh networks, multi-hop situations, and synchronized communication in both directions between the nodes. In addition, the automation

systems will download configuration data to the field devices both at startup and during operation that should be end-to-end acknowledged and retransmitted to be able to guarantee delivery in case of communication losses. To decrease the number of retransmissions in the IWSN one can use some error control techniques such as *forward error correcting* (FEC) codes [16]. In the commercial IEEE 802.15.4 based IWSN today, FEC has been omitted mainly due power consumption of decoding operation. Nevertheless, by using FEC the overall energy consumption will become less since we will spend less energy on retransmission [17] and re-scheduling our network. The major trade off between the additional processing power and the associated coding gain need to be optimized in order to have a power, energy-efficient and low-complexity FEC schemes in industrial wireless sensor networks. In addition to that, we need to consider memory constraints in the embedded system and not jeopardizing the IWSN requirements given in Table I.

With respect to retransmissions in mesh networks and multi-hop situations, it has to be guaranteed that data is delivered in the correct order. It can easily occur that data is received in the wrong order if packets are not discarded in the mesh before the next periodic data is transmitted and delivered. The consequences can be substantial, as a single bit is used to start and stop electric motors ranging from kilowatts to megawatts.

#### E. Lack of Support for Actuators

One great advantage with IWSNs is that it is not required to route a communication cable from each sensor and actuator to the dedicated controller. Usually different sections of the process are distributed over several, sometimes redundant, controllers to avoid that a failure in one part of the process affects other process sections. The main reason is to limit the consequences in case of a failure, and to increase the availability of the plant by using buffers between the different process sections. However, actuators would gain the same advantage as for sensors with respect to this matter. Today, most standards lack support for actuators and therefore limits this advantage, as a parallel wired infrastructure for actuators has to be designed, deployed, and maintained. Of course, this have a major impact on the overall cost when deploying IWSNs today, and the cost benefit is partly eliminated due to this.

Actuator support demands deterministic communication from the automation system down to the actuators, and in addition as described in Section IV-A the need for deterministic communication in both directions, as well as failsafe states [18]. One of the main arguments against support for actuators today, is that actuators need to be connected to the main grid as a battery cannot provide sufficient energy to the actuator. What you seldom read in literature is that many actuators actually are pneumatic. We will elaborate more on this matter in Section IV-I.

#### F. System Integration

In order to make a smooth and efficient integration of IWSNs into existing automation infrastructures, the most critical point to consider is the gateways. Today there exist a small number of GW vendors and they are proposing proprietary solutions, which prevents an open and efficient integration to existing infrastructure. All commercially available solutions today provide web-based configuration, everything is done manually, which slows down the engineering, commissioning, and maintenance of the system.

Today, most wired fieldbuses have services to download configuration and to simplify the integration work in general. What is currently missing is a standardized approach for IWSN integration to the different fieldbuses in the IEC standards [19]. Some standardization efforts are currently ongoing [20], [21] as well as proposals for integration [22]. Therefore it is essential that the services provided by the IWSN are possible to integrate efficiently in the automation system to have a seamless transition from wired to wireless communication, as well as simple deployment, commissioning, and maintenance.

#### G. Network Size

One important requirement for IWSN is scalability and the networks capability to adapt to changing networks size. Without this kind of support the network performance will degrade significantly as the network size increases. In most research work it is envisaged that the network (e.g., the gateway) should be scalable and able to support 1000 sensor nodes. That assumption is not valid in a process automation context where it is more likely that the network will contain a maximum of 50 nodes in order to meet the required refresh rates. This points to that research needs to be focused on routing algorithms aimed for smaller networks that are optimized for the requirements given in Table I, and where the key parameter is latency.

#### H. Coexistence and Interference Avoidance

Industrial plants often contain many different wireless communication technologies that operate in the same frequency band that operate in the 2.4 GHz ISM band. Thus, it is very important that a solution can coexist in a radio environment with a large amount of interferences as well as limit its own disturbance. The obvious countermeasure for interference is the use of different diversity (time, frequency, and space) schemes [23] but also some more fancy innovative techniques such as interference cancellation, effective radio resource management and software defined radios. WirelessHART [2] combines channel hopping (frequency diversity) and TDMA but more sophisticated algorithms considering the combination of multiple diversity schemes and scheduling of slots is needed in the future. It is indeed important to guarantee real-time services for IWSN [24] and therefore more research on real-time scheduling for IWSN is of high priority.

#### I. Energy Consumption

Research on energy consumption and energy harvesting / scavenging is a hot topic today. However, due to refresh

rates required in process automation it is difficult to save much energy by minimizing the duty cycle of a wireless field device. Secondly, as previously mentioned actuators are a mandatory part of process automation and they are sometimes pneumatic. Therefore, true wireless field devices are not foreseen in the near future in process automation. However, temporal installations of sensors used for validation of possible process optimization will greatly benefit since they can be true wireless, operated on battery power. Future research in energy scavenging will improve the situation and more kind of field devices can become true wireless. However, many devices are unlikely to become true wireless using today's technology, both sensors (i.e. acoustic or laser) and actuators (i.e. large valves or pneumatic control valves). Nevertheless, the advantages are still significant even if power supplies have to be wired to the sensors and actuators as the fieldbuses are not necessary to route between all sensors, actuators, and controllers in the specific process sections. Power is almost always found close to the field devices today and is likely to remain there, even in green field installations.

Assume for a while that all field devices could be battery operated today, a new significant problem would occur, namely scheduled battery maintenance of tens of thousands of nodes in a typical process industry. This would cause serious problems for the industries that are expected to operate flawlessly 24/7 with a few short schedule maintenance periods per year. In addition, the end-users need to keep batteries of various size and capacity on stock in order to quickly replace exhausted batteries. That means in the end that the life-cycle cost for a true wireless device would be more expensive compared to a device that only communicates wireless.

## V. CONCLUSION

Industrial wireless sensor networks (IWSNs) have been gaining acceptance during the last decade, largely due to the greatly increased flexibility, lower cost and scalability that they have been shown to provide. Nevertheless, still there exist several open areas in IWSNs that has not been addressed properly in existing research work.

In this article, we outline the most important research issues that need to be solved immediately such that IWSNs can meet the expected market requirements. Safety is by far the most important feature to consider and there are several issues that need to be addressed before we can offer a safe and secure communication over wireless sensor and actuator networks. For instance, it is important with downlink support for actuators otherwise we cannot support safety applications. Other important research topics are interoperability between different wireless systems, availability and meeting real-time guarantees where latency is an important parameter to pay attention to.

## REFERENCES

- [1] T. Lennvall, S. Svensson, and F. Hekland, "A comparison of wirelesshart and zigbee for industrial applications," in *IEEE International Workshop on Factory Communication Systems*, May 2008, pp. 85–88.
- [2] (2010) Hart 7 specification. [Online]. Available: <http://www.hartcomm.org/>
- [3] (2010) Isa 100, wireless systems for automation. [Online]. Available: <http://www.isa.org/isa100>
- [4] A. Willig, "Recent and emerging topics in wireless industrial communications: A selection," *IEEE Transactions on Industrial Informatics*, vol. 4, no. 2, pp. 102 –124, May 2008.
- [5] I. Akyildiz and X. Wang, "A survey on wireless mesh networks," *Communications Magazine, IEEE*, vol. 43, no. 9, pp. S23 – S30, Sept. 2005.
- [6] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292 – 2330, 2008.
- [7] L. Zheng, "Industrial wireless sensor networks and standardizations: The trend of wireless sensor networks for process automation," in *Proceedings of SICE Annual Conference 2010*, Aug. 2010, pp. 1187 –1190.
- [8] L. Hou and N. Bergmann, "System requirements for industrial wireless sensor networks," in *IEEE Conference on Emerging Technologies and Factory Automation (ETFA'10)*, Sept. 2010, pp. 1 –8.
- [9] V. Gungor and G. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258 –4265, Oct. 2009.
- [10] J. Heo, J. Hong, and Y. Cho, "Earq: Energy aware routing for real-time and reliable communication in wireless industrial sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 5, no. 1, pp. 3 –11, 2009.
- [11] M. De Biasi, C. Snickars, K. Landernas, and A. Isaksson, "Simulation of process control with wirelesshart networks subject to packet losses," in *IEEE International Conference on Automation Science and Engineering (CASE)*, Aug. 2008, pp. 548 –553.
- [12] *IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems*. International Electrotechnical Commission, 2005.
- [13] J. Åkerberg, F. Reichenbach, and M. Björkman, "Enabling safety-critical wireless communication using wirelesshart and profisafe," in *IEEE Conference on Emerging Technologies and Factory Automation (ETFA'10)*, Sept. 2010, pp. 1 –8.
- [14] F. De Pellegrini, D. Miorandi, S. Vitturi, and A. Zanella, "On the use of wireless networks at low level of factory automation systems," *IEEE Transactions on Industrial Informatics*, vol. 2, no. 2, pp. 129 – 143, May 2006.
- [15] M. Soyturk and D. Altilar, "Reliable real-time data acquisition for rapidly deployable mission-critical wireless sensor networks," in *IEEE INFOCOM Workshops*, 2008, pp. 1 –6.
- [16] L. Li, R. G. Maunder, B. M. Al-Hashimi, and L. Hanzo, "An energy-efficient error correction scheme for ieee 802.15.4 wireless sensor networks," *Transactions on Circuits and Systems II*, vol. 57, no. 3, pp. 233–237, March 2010.
- [17] M. Vuran and I. Akyildiz, "Error control in wireless sensor networks: A cross-layer analysis," *IEEE/ACM Transactions on Networking*, vol. 17, no. 4, pp. 1186 – 1199, Aug. 2009.
- [18] J. Åkerberg, M. Gidlund, J. Neander, T. Lennvall, and M. Björkman, "Deterministic downlink transmission in wirelesshart networks enabling wireless control applications," in *36th Annual Conference on IEEE Industrial Electronics Society (IECON'10)*, Nov. 2010, pp. 2120 –2125.
- [19] *IEC 61784-1. Industrial Communication Networks - Profiles - Part 1: Fieldbus profiles*. International Electrotechnical Commission, 2007.
- [20] (2010) Wireless cooperation team. [Online]. Available: [http://www.hartcomm.org/hcf/news/pr2008/press\\_conf\\_interkama2008.pdf](http://www.hartcomm.org/hcf/news/pr2008/press_conf_interkama2008.pdf)
- [21] (2010) Tc2/wg12 wireless sensor/actor networks. [Online]. Available: [http://www.profibus.com/index.php?id=1314&tcwg\\_tc\\_uid=2&tcwg\\_wg\\_uid=14](http://www.profibus.com/index.php?id=1314&tcwg_tc_uid=2&tcwg_wg_uid=14)
- [22] J. Åkerberg, M. Gidlund, T. Lennvall, J. Neander, and M. Björkman, "Integration of wirelesshart networks in distributed control systems using profinet io," in *8th IEEE International Conference on Industrial Informatics (INDIN'10)*, July 2010, pp. 154 –159.
- [23] D. Yang, M. Gidlund, and Y. Xu, "Coexistence of ieee 802.15.4 based networks: A survey," in *36th Annual Conference on IEEE Industrial Electronics Society (IECON'10)*, Nov. 2010, pp. 2107 – 2113.
- [24] S.-E. Yoo, P. K. Chong, D. Kim, Y. Doh, M.-L. Pham, E. Choi, and J. Huh, "Guaranteeing real-time services for industrial wireless sensor networks with ieee 802.15.4," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 11, pp. 3868 –3876, Nov. 2010.