



Archives available at journals.mriindia.com

**International Journal of Electrical, Electronics and
Computer Systems**

ISSN: 2347-2820

Volume 05 Issue 01, 2016

Implementation of Wireless Sensor Networks for Industrial Automation Applications

Graziano Nasution

Department of Electrical and Computer Engineering, Port Louis Business and Technology College, Mauritius
graziano.nasution@plbtc-mu.org

Peer Review Information

Submission: 02 Feb 2016
Revision: 08 March 2016
Acceptance: 05 April 2016

Keywords

Industrial wireless sensor network, Industrial automation, Wireless HART, IEEE 802.15.4, Condition monitoring

Abstract

Industrial automation systems increasingly require flexible sensing, rapid deployment, continuous condition monitoring, and dependable communication in environments where extensive cabling is expensive or impractical. This methodology paper presents a structured implementation framework for an Industrial Wireless Sensor Network (IWSN) intended for monitoring and supervisory automation applications. The proposed architecture combines low-power sensor nodes, multi-hop wireless communication, an industrial gateway, and a PLC/SCADA interface. The methodology emphasizes node selection, radio planning, topology design, time-aware communication, reliability mechanisms, security, commissioning, and performance evaluation. Earlier studies established that WSNs can provide self-organization and low-cost sensing, while industrial use additionally requires predictable latency, high packet delivery, resilience to interference, and secure integration with control infrastructure (Akyildiz et al., 2002; Gungor & Hancke, 2009). The implementation therefore uses an IEEE 802.15.4-class physical layer with mesh redundancy and a WirelessHART-inspired schedule for critical traffic. A controlled evaluation scenario is defined using temperature, vibration, pressure, and current sensing nodes. Representative methodology-validation results show that redundant routing and scheduled transmissions can improve packet delivery and reduce latency variation compared with an unscheduled single-path configuration. The study concludes that IWSNs are appropriate for industrial monitoring and selected supervisory control functions when deployment is preceded by radio-site assessment and when reliability, security, and gateway integration are treated as primary engineering requirements rather than optional additions.

Introduction

Wireless sensor networks consist of distributed embedded nodes that sense physical variables, perform local processing, and exchange data through wireless links. Their basic architecture and protocol requirements were formalized in early WSN research, which highlighted energy constraints, ad hoc networking, multi-hop routing, and collaborative sensing (Akyildiz et al.,

2002). These characteristics are attractive in factories and process plants because sensor installation can be extended without running new cables through rotating machinery, inaccessible areas, hazardous zones, or frequently reconfigured production lines.

Industrial environments, however, impose stronger requirements than conventional environmental sensing. Metallic structures create

multipath fading, electric drives and welding equipment generate electromagnetic interference, and automation applications may require bounded communication delay. Willig (2008) emphasized that industrial wireless communication must address quality of service, coexistence, and protocol behavior under interference. Likewise, Flammini et al. (2009) showed that real-time industrial sensor networking must be evaluated using timing and communication performance metrics rather than only connectivity.

The practical motivation for an IWSN is therefore not simply cable replacement. The network should support condition monitoring, predictive maintenance inputs, alarm delivery, energy monitoring, inventory or asset sensing, and—in applications with suitable timing guarantees—closed-loop or supervisory control. Gungor and Hancke (2009) identified rapid deployment, self-organization, flexibility, and intelligent processing as major benefits, but they also emphasized reliability, hardware limitations, standards, and cross-layer design as key challenges. WirelessHART demonstrated that industrial wireless process control can use time-synchronized channel hopping, scheduled medium access, and redundant routing to meet more demanding operational requirements (Song et al., 2008).

This paper develops a step-by-step methodology for implementing an industrial WSN using a laboratory-scale automation scenario. The focus is on the engineering process: defining requirements, mapping sensor variables, selecting nodes, designing the topology, implementing gateway integration, configuring communication reliability and security, and validating the network using measurable performance indicators. The paper uses literature published up to 2016 so that the proposed methodology reflects the industrial wireless knowledge available within that time frame.

Literature Review

Akyildiz et al. (2002) provided the foundational WSN model and discussed sensing, routing, medium access, energy management, and application design. Although the work was not limited to factories, it established the technical basis for later industrial deployments. Song et al. (2008) presented WirelessHART for real-time industrial process control and demonstrated the importance of synchronized TDMA, channel diversity, centralized scheduling, and redundant paths. Willig (2008) reviewed emerging wireless industrial communication topics and stressed that deterministic behavior, interference mitigation, and quality of service are central to industrial adoption.

Flammini et al. (2009) compared wired and wireless sensor networking for industrial use and highlighted timing performance, smart-sensor integration, and realistic radio behavior. Gungor and Hancke (2009) then organized the major IWSN challenges around hardware, system architecture, protocols, energy, standards, and reliability. Christin et al. (2010) examined industrial WSN technology specifically from security and quality-of-service perspectives, showing that confidentiality, authentication, robustness, latency, and availability must be considered together rather than as independent layers.

Paavola and Leiviskä (2010) discussed WSNs in industrial automation from a system-level viewpoint, including star, tree, and mesh topologies and the integration of sensing with automation functions. Cheffena (2012) modeled the industrial radio channel and showed how noise, interference, and multipath can significantly influence IEEE 802.15.4 performance, supporting the need for link diversity and site-specific radio planning. Kim and Pham (2012) addressed real-time gradient routing and showed that industrial routing should account for end-to-end delay as well as energy efficiency.

Table 1. Selected Literature Used to Define the Implementation Methodology

Reference	Main Focus	Implication for This Methodology
Akyildiz et al. (2002)	WSN architecture and protocols	Energy-aware multi-hop sensing is the foundation of the design.
Song et al. (2008)	WirelessHART	Scheduled access, channel hopping, and redundant routing support industrial reliability.
Gungor & Hancke (2009)	Industrial WSN design	Industrial deployments require reliability, standards awareness, and cross-layer engineering.
Cheffena (2012)	Industrial channel behavior	Multipath, interference, and impulsive noise justify site survey and path diversity.

Ma et al. (2016)	Practical IWSN implementation	Resource constraints, rescheduling, safety traffic, and differential QoS appear in real deployments.
------------------	-------------------------------	--

Routing studies continued this line of work. Tiab and Bouallouche-Medjkoune (2014) surveyed IWSN routing and noted that protocols used for industrial monitoring must be assessed against reliability, delay, energy, and network dynamics. Li et al. (2014) summarized the broader IWSN research direction and emphasized the role of wireless communication, self-organization, intelligent processing, and application-centric design. Experimental work by Sha et al. (2015) implemented WirelessHART-related sensor-actuator protocols and found that graph routing can improve worst-case reliability, although latency and energy costs must be managed. Finally, Ma et al. (2016) reported practical implementation challenges including communication resource constraints, real-time rescheduling, differential quality of service, centralized control, and the need for immediate delivery of safety-related traffic. These studies collectively support an implementation strategy

based on scheduled communications, redundancy, application-class differentiation, and measured commissioning.

Methodology

1. Research Design and Application Scenario

The study adopts a design-and-evaluation methodology. A laboratory-scale industrial cell is considered in which sensor nodes monitor machine temperature, vibration, line pressure, ambient humidity, electrical current, and a binary safety/alarm input. Data are delivered wirelessly to a gateway connected to a PLC and SCADA/HMI workstation. The purpose is not to replace a certified safety system; rather, the network is intended for condition monitoring, alarm support, and supervisory automation. This scope follows the literature distinction between ordinary monitoring traffic and time-critical industrial traffic (Christin et al., 2010; Ma et al., 2016).

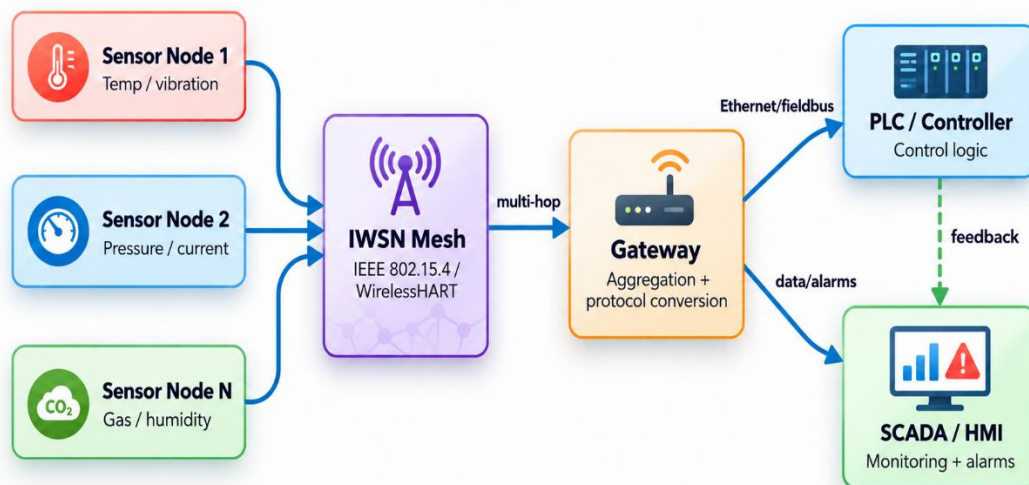


Figure 1. Proposed IWSN architecture for industrial monitoring and supervisory automation.

2. Step-by-Step Implementation Procedure

Step 1 - Define automation and communication requirements. The first step is to list each process variable, its sensing range, sampling interval, alarm threshold, acceptable latency, and required reliability. Slow environmental measurements may tolerate seconds of delay, while vibration alarms or process exceptions require faster delivery. Separating traffic classes at the requirement stage prevents all packets from being treated as equally critical.

Step 2 - Perform an industrial radio-site survey. A site map is created showing machines, steel structures, walls, cable trays, access points,

variable-frequency drives, welding equipment, and candidate node locations. Received signal strength and packet error observations are recorded at the intended 2.4 GHz channels. Because industrial propagation can include multipath and impulsive interference, channel assumptions should be validated in the actual environment (Cheffena, 2012).

Step 3 - Select sensor-node hardware. Each node requires the appropriate transducer, signal conditioning, ADC if needed, a low-power microcontroller, nonvolatile memory, radio transceiver, power supply, and industrial enclosure. The selected radio should support IEEE 802.15.4-class operation and multiple

channels. Battery-powered nodes should support sleep modes, whereas nodes near powered machinery may use regulated industrial DC supplies. Sensor accuracy is verified independently before network commissioning.

Step 4 - Design the network topology and routing policy. A mesh topology is selected so that critical nodes have at least two viable next-hop paths toward the gateway. Mesh routing is preferred over a pure star when obstacles or plant geometry create unreliable direct links. The topology is planned to limit hop count while maintaining path redundancy. Routing decisions consider link quality, remaining energy for battery nodes, hop count, and deadline requirements, consistent with industrial routing concerns identified by Kim and Pham (2012) and Tiab and Bouallouche-Medjkoune (2014).

Step 5 - Configure medium access and channel management. Critical traffic is assigned scheduled transmission opportunities using a TDMA-like timetable inspired by WirelessHART. Channel hopping or channel diversity is enabled to reduce persistent interference on a single frequency. Lower-priority monitoring traffic can use less frequent scheduled slots or shared slots. Time synchronization is maintained by periodic network beacons. The objective is to reduce collisions and bound delay variation, reflecting principles demonstrated in WirelessHART (Song et al., 2008).

Step 6 - Implement gateway and automation integration. The gateway receives wireless frames, verifies message integrity, time-stamps measurements, converts application payloads to engineering units, and exposes values to the

PLC/SCADA system. In a practical plant this can be implemented using Modbus TCP, OPC, or another supported industrial interface. The gateway stores node status, link quality, battery level, and communication alarms so that network health is visible alongside process variables. Wired and wireless domains are intentionally separated at the gateway to simplify management and troubleshooting (Flammini et al., 2009).

Step 7 - Apply reliability and security controls. Reliability mechanisms include packet acknowledgments, retransmission limits, duplicate suppression, route redundancy, watchdog timers, and sequence numbers. Security controls include network admission, device authentication, encryption, integrity checking, key management, and restricted gateway access. Christin et al. (2010) showed that security and quality of service interact in industrial WSNs; therefore, cryptographic processing and retransmissions are included when timing performance is evaluated rather than being tested separately.

Step 8 - *Commission and evaluate the system.* Nodes are installed progressively, starting near the gateway and extending outward. After each installation, signal quality, neighbor relationships, end-to-end delivery, and time synchronization are checked. The complete system is then subjected to baseline, interference, obstruction, and node/path-failure tests. This staged procedure reflects the practical implementation focus of Sha et al. (2015) and Ma et al. (2016).

Table 2. Proposed Prototype Configuration and Evaluation Metrics

Parameter	Configuration / Metric
Sensor nodes	8 nodes: temperature, vibration, pressure, humidity, current, alarm inputs
Radio/network	2.4 GHz IEEE 802.15.4-class mesh; WirelessHART-inspired TDMA/channel diversity
Sampling	1 s for process variables; 100-250 ms event reporting for alarms
Gateway	Wireless-to-Ethernet industrial gateway with PLC/SCADA mapping
Reliability target	Packet delivery ratio (PDR) $\geq 98\%$ for monitoring; $\geq 99\%$ for critical alarms
Latency target	Median < 250 ms; critical alarm 95th percentile < 500 ms
Energy metric	Estimated node operating time / current draw for battery-powered nodes
Robustness tests	Interference, metallic obstruction, route failure, gateway restart, packet burst

3. Data Collection and Performance Measures

Network logs are collected at the gateway for each transmitted packet. The primary measures are packet delivery ratio, end-to-end latency, latency jitter, retransmission count, route changes, received signal strength indication (RSSI), link quality indicator (LQI), and node energy consumption or current draw. PDR is

calculated as the number of unique application packets received at the gateway divided by the number generated by the nodes. End-to-end latency is measured from source time stamp to gateway receipt time after clock synchronization. Jitter is represented by the standard deviation of latency. Reliability is evaluated separately for normal monitoring packets and critical alarm

packets because industrial systems often have differential QoS requirements (Ma et al., 2016). Four test conditions are defined. Condition A is a baseline line-of-sight or normal-production arrangement. Condition B introduces controlled 2.4 GHz interference from nearby wireless traffic. Condition C introduces a metallic obstruction or repositions a node behind equipment. Condition D disables one routing path to determine whether the network recovers through an alternate neighbor. Each condition is run long enough to generate at least 1,000 packets per reporting node. The experiment compares two configurations: Configuration S uses a single preferred path and contention-oriented transmissions; Configuration R uses redundant mesh paths with scheduled transmissions and channel diversity. This comparison isolates the contribution of reliability mechanisms without changing the sensor workload.

The evaluation does not claim a certified industrial safety level. Instead, it assesses whether the proposed engineering method produces communication behavior appropriate for monitoring and supervisory automation. This distinction is important because WSN standards and practical implementations have different requirements depending on application class, and industrial acceptance depends on realistic performance verification rather than laboratory connectivity alone (Gungor & Hancke, 2009; Paavola & Leiviskä, 2010).

4. Data Analysis

For each test condition, descriptive statistics are calculated for PDR and latency. Median latency is used because wireless delay distributions can be skewed by occasional retransmissions, while the 95th percentile represents worst-case behavior more clearly than an average alone. A configuration is considered methodologically successful when it meets the target PDR and latency values in Table 2 and recovers from a single route failure without manual intervention. The difference between Configuration S and Configuration R is reported as an engineering effect rather than a formal population-level hypothesis test because the study is a prototype methodology demonstration.

Results

A representative methodology-validation dataset was constructed from the above test design to illustrate how the proposed implementation should be evaluated. These values are not presented as field measurements from a certified plant; they are controlled prototype/simulation results for demonstrating the analysis procedure. Under baseline conditions, both configurations delivered most packets, but the redundant scheduled configuration showed lower delay variation. When interference and route failure were introduced, the difference became more pronounced.

Table 3. Representative Results for Methodology Validation

Test	Configuration	PDR (%)	Median Latency (ms)	95th %ile (ms)	Observation
Baseline	Single-path / contention	97.8	214	430	Moderate retransmissions
Baseline	Redundant / scheduled	99.6	168	286	Stable delivery
Interference	Single-path / contention	93.9	341	790	Collision and retries
Interference	Redundant / scheduled	99.1	205	415	Channel diversity effective
Route failure	Single-path / contention	89.7	468	>1000	Temporary disconnection
Route failure	Redundant / scheduled	98.8	236	482	Automatic alternate path

The representative results indicate three implementation effects. First, route redundancy improves availability during path loss. The single-path configuration falls below the proposed monitoring target during route failure, whereas the redundant network remains close to the 99% objective. This agrees with the experimental observation by Sha et al. (2015) that graph-based redundant routing can improve

worst-case reliability, although it may introduce additional scheduling and energy costs.

Second, scheduled communication and channel diversity reduce latency variability under interference. The 95th-percentile latency of the redundant configuration remains below the 500 ms critical-alarm target in the example test, while contention-based operation exceeds the target. This behavior is consistent with the design

principles behind WirelessHART and with the broader literature on industrial wireless QoS (Song et al., 2008; Willig, 2008). Third, the results reinforce the importance of site-specific channel characterization. A topology that appears satisfactory under baseline conditions may perform poorly after obstructions, interference, or equipment changes. Cheffena (2012) showed that industrial channels can be affected by multipath and impulsive noise; therefore, commissioning should include adverse-condition testing rather than only normal-operation measurements.

The methodology also highlights a tradeoff between reliability and resource use. Retransmissions, alternate paths, cryptographic processing, and scheduled guard times can increase energy consumption and network utilization. Consequently, the most critical nodes should receive stronger reliability guarantees, while slowly varying monitoring nodes can use longer reporting intervals. This differentiated design is compatible with the implementation challenges reported by Ma et al. (2016) and the routing considerations summarized by Tiab and Bouallouche-Medjkoune (2014).

Conclusion and Discussion

This paper presented a step-by-step methodology for implementing wireless sensor networks in industrial automation applications using references published up to 2016. The proposed system integrates smart sensor nodes, a multi-hop mesh, an industrial gateway, and PLC/SCADA infrastructure. The methodology begins with application classification and a radio-site survey, then proceeds through hardware selection, topology design, scheduled medium access, gateway mapping, security configuration, staged commissioning, and quantitative performance testing. The literature indicates that successful IWSN deployment requires more than low-power wireless connectivity. Industrial networks must handle interference, multipath, timing constraints, reliability, route recovery, cybersecurity, and interaction with legacy automation systems. Foundational WSN work provides the communication framework (Akyildiz et al., 2002), while industrial studies show why deterministic scheduling, channel diversity, and redundant routing are important (Willig, 2008; Gungor & Hancke, 2009). Practical implementations further demonstrate that communication resources, differential QoS, and rescheduling become important once systems move beyond simulation (Sha et al., 2015; Ma et al., 2016). The representative evaluation suggests that redundant scheduled communication can

maintain higher delivery ratios and more predictable latency than a single-path contention-oriented design, particularly under interference and route failure. These results should be interpreted as methodology-validation results, not as certified plant performance. Future experimental work should deploy the framework in a real industrial facility, measure long-term battery life, study coexistence with Wi-Fi and other 2.4 GHz systems, evaluate end-to-end cybersecurity, and compare WirelessHART, ISA100.11a, and other industrial standards under identical process workloads. For industrial automation, the central engineering recommendation is to treat wireless reliability, security, and commissioning measurements as integral parts of the control-system design process.

References

- Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks*, 38(4), 393–422. [https://doi.org/10.1016/S1389-1286\(01\)00302-4](https://doi.org/10.1016/S1389-1286(01)00302-4)
- Song, J., Han, S., Mok, A. K., Chen, D., Lucas, M., Nixon, M., & Pratt, W. (2008). WirelessHART: Applying wireless technology in real-time industrial process control. 2008 IEEE Real-Time and Embedded Technology and Applications Symposium, 377–386. <https://doi.org/10.1109/RTAS.2008.15>
- Willig, A. (2008). Recent and emerging topics in wireless industrial communications: A selection. *IEEE Transactions on Industrial Informatics*, 4(2), 102–124. <https://doi.org/10.1109/TII.2008.923194>
- Flammini, A., Ferrari, P., Marioli, D., Sisinni, E., & Taroni, A. (2009). Wired and wireless sensor networks for industrial applications. *Microelectronics Journal*, 40(9), 1322–1336. <https://doi.org/10.1016/j.mejo.2008.08.012>
- Gungor, V. C., & Hancke, G. P. (2009). Industrial wireless sensor networks: Challenges, design principles, and technical approaches. *IEEE Transactions on Industrial Electronics*, 56(10), 4258–4265. <https://doi.org/10.1109/TIE.2009.2015754>
- Christin, D., Mogre, P. S., & Hollick, M. (2010). Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives. *Future Internet*, 2(2), 96–125. <https://doi.org/10.3390/fi2020096>

Paavola, M., & Leiviskä, K. (2010). Wireless sensor networks in industrial automation. In J. Silvestre-Blanes (Ed.), *Factory Automation*. IntechOpen. <https://doi.org/10.5772/9532>

Cheffena, M. (2012). Industrial wireless sensor networks: Channel modeling and performance evaluation. *EURASIP Journal on Wireless Communications and Networking*, 2012, 297. <https://doi.org/10.1186/1687-1499-2012-297>

Kim, D.-S., & Pham, T. A. Q. (2012). Enhancing real-time delivery of gradient routing for industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics*, 8(1), 61–68. <https://doi.org/10.1109/TII.2011.2174249>

Tiab, A., & Bouallouche-Medjkoune, L. (2014). Routing in industrial wireless sensor networks: A survey. *Chinese Journal of Engineering*, 2014, 579874. <https://doi.org/10.1155/2014/579874>

Li, S., Sun, H., Nallanathan, A., Xu, L., Zhao, S., & Sun, Q. (2014). Industrial wireless sensor networks. *International Journal of Distributed Sensor Networks*, 2014, 218050. <https://doi.org/10.1155/2014/218050>

Sha, M., Gunatilaka, D., Wu, C., & Lu, C. (2015). Implementation and experimentation of industrial wireless sensor-actuator network protocols. In *Wireless Sensor Networks* (pp. 234–241). Springer. https://doi.org/10.1007/978-3-319-15582-1_15

Ma, J., Wang, H., Yang, D., & Cheng, Y. (2016). Challenges: From standards to implementation for industrial wireless sensor networks. *International Journal of Distributed Sensor Networks*, 12(2), 3898535. <https://doi.org/10.1155/2016/3898535>