



Implementation of Wireless Sensor Networks for Industrial Monitoring Applications

Myeong Dahalbahadur

Department of Electrical and Computer Engineering, Kavir Polytechnic University of Technology, Iran
 myeong.dahalbahadur@kput-ir.net

Peer Review Information

Submission: 25 Jan 2017
 Revision: 11 Feb 2017
 Acceptance: 26 March 2017

Keywords

Wireless Sensor Networks,
 Industrial Monitoring, IEEE
 802.15.4, WirelessHART,
 Condition Monitoring

Abstract

Wireless sensor networks (WSNs) provide a practical alternative to extensive cabling for monitoring industrial assets, process variables, and environmental conditions. Their adoption, however, is constrained by radio interference, metallic obstructions, limited energy, deterministic reporting requirements, and the need for secure and reliable data delivery. This paper presents a methodology for implementing a low-cost industrial WSN that acquires temperature, humidity, vibration, and pressure data and forwards them to a monitoring station for visualization and alarm generation. The proposed architecture uses distributed sensor nodes, a low-power IEEE 802.15.4-class radio interface, multi-hop communication where required, and a gateway connected to a supervisory computer. The methodology covers node selection, sensor interfacing, packet formation, network association, channel selection, threshold-based event detection, data logging, and performance evaluation. Reliability is assessed using packet delivery ratio, end-to-end latency, link quality, sensing error, and alarm-detection performance. An illustrative prototype evaluation indicates that a carefully planned deployment can maintain high packet delivery under normal industrial interference while preserving sub-second alarm reporting. The approach emphasizes modularity, low deployment cost, and compatibility with industrial wireless design principles established before 2018. The methodology can therefore be adapted to equipment-condition monitoring, utility supervision, safety sensing, and predictive-maintenance data acquisition in small and medium industrial facilities.

Introduction

Industrial plants rely on continuous measurement of physical variables such as temperature, pressure, humidity, vibration, flow, gas concentration, and equipment state. Conventional wired instrumentation offers predictable performance, but installing additional measurement points often requires cable trays, junction boxes, conduit, plant shutdowns, and repeated maintenance. Wireless sensor networks reduce this infrastructure burden by distributing compact sensing devices that communicate measurements over radio

links. The basic WSN concept combines sensing, embedded processing, wireless communication, and energy-constrained operation, allowing large numbers of nodes to cooperate in monitoring tasks [1]. In factory environments, however, the radio channel is affected by metal surfaces, moving machinery, electromagnetic noise, shadowing, and multipath propagation. Consequently, industrial WSNs require stronger attention to reliability, latency, redundancy, security, and deployment planning than many conventional environmental WSNs [3].

Early work on wireless networking for factory automation showed that cable replacement cannot be treated simply as a consumer wireless problem because industrial traffic includes periodic measurements, alarms, control messages, and maintenance data with different timing requirements [2]. Later research defined industrial wireless sensor networks as systems that must combine self-organization and flexible deployment with dependable operation in harsh environments [3]. Standards such as WirelessHART and ISA100.11a introduced time-synchronized communication, channel diversity, mesh routing, and centralized network management to address these requirements [5]. Comparative studies have also shown that ZigBee, WirelessHART, ISA100.11a, and WIA-PA differ substantially in determinism, routing, coexistence strategy, and target application [9].

The purpose of this paper is to present a step-by-step implementation methodology for an industrial monitoring WSN rather than to propose a new radio standard. The design focuses on a practical monitoring layer in which sensors acquire machine and environmental data, local embedded nodes perform basic validation and event checking, and wireless packets are delivered to a gateway for logging and visualization. The main objectives are: to define an economical node architecture, establish a reliable wireless topology, reduce unnecessary transmissions through local processing, and quantify performance using repeatable metrics. The resulting method is intended for non-safety-critical monitoring and maintenance applications, while recognizing that safety-critical or closed-loop control functions require stricter certification and deterministic guarantees.

Literature Review

Akyildiz et al. [1] established the foundational architecture of WSNs and identified energy, topology, communication, and application constraints that continue to influence industrial deployments. For factory-level use, De Pellegrini et al. [2] examined wireless communication at low levels of automation and emphasized the need to relate radio technology to traffic deadlines and reliability requirements. Gungor and Hancke [3] later consolidated industrial WSN design challenges, including hardware robustness, energy management, network architecture, protocol design, interference, and standardization. Their work is particularly relevant because it links generic sensor-network design to the operational realities of industrial plants.

Security is equally important because industrial sensor data may affect maintenance decisions or trigger supervisory actions. Alcaraz and Lopez [4] analyzed security for wireless sensor mesh networks in highly critical systems and highlighted authentication, key management, integrity, and availability concerns. Their findings support the inclusion of device identification, protected commissioning, packet integrity checking, and controlled gateway access in an implementation methodology. At the protocol level, Petersen and Carlsen [5] compared WirelessHART and ISA100.11a, explaining why both standards use mechanisms such as time synchronization, channel hopping, centralized configuration, and mesh communication to improve coexistence and dependability.

Practical industrial experiments are important because propagation behavior in factories is difficult to predict solely from theory. Mikhaylov et al. [6] reported real-life evaluation results for WSNs in industrial environments and demonstrated that link quality can vary considerably with location, obstacles, and activity around equipment. This reinforces the need for site surveys and link-quality testing during deployment. Ikram et al. [7] addressed transmission-power control for industrial wireless instrumentation, showing that power adaptation can help balance energy consumption, interference, and fading. Nobre et al. [8] surveyed routing and scheduling in WirelessHART and emphasized that graph routing, time-slot scheduling, retransmission, and channel allocation are central to dependable industrial wireless communication.

By 2016, the literature had moved from individual protocol mechanisms toward broader comparisons and mixed-criticality operation. Wang and Jiang [9] compared the architectures of major industrial WSN standards and provided a useful basis for selecting a protocol according to determinism, coexistence, security, and network scale. Jin et al. [10] proposed mixed-criticality scheduling for industrial WSNs, illustrating the importance of assigning higher communication priority to urgent industrial data than to routine monitoring packets. Sukhanov et al. [11] demonstrated a self-organizing sensor platform for industrial safety and ecological monitoring, supporting the feasibility of modular nodes that integrate multiple sensing functions.

Industry 4.0 research further strengthened the role of wireless networks as part of connected manufacturing. Li et al. [12] reviewed industrial wireless networks in the context of Industry 4.0

and concluded that flexible connectivity is essential for integrating machines, sensors, and information systems. At the same time, reliability modeling became more comprehensive. Deif and Gadallah [13] proposed a WSN reliability metric that considers coverage, connectivity, and component failures, which is useful when a monitoring system must remain functional

despite node or link degradation. Collectively, the literature indicates that an effective industrial WSN implementation must combine appropriate sensing hardware with deliberate topology design, interference-aware communication, security, redundancy, and measurable performance criteria.

Table 1. Selected literature supporting the proposed methodology

Reference	Year	Main contribution	Use in this methodology
[3] Gungor & Hancke	2009	Industrial WSN challenges and design principles	Defines reliability, interference and architecture requirements
[5] Petersen & Carlsen	2011	WirelessHART and ISA100.11a comparison	Guides industrial protocol features and coexistence design
[6] Mikhaylov et al.	2012	Real-life industrial WSN evaluation	Motivates site survey and link-quality testing
[7] Ikram et al.	2014	Adaptive transmission power control	Supports link/energy tuning in harsh radio channels
[9] Wang & Jiang	2016	Comparison of industrial WSN standards	Supports protocol and topology selection
[12] Li et al.	2017	Industrial wireless networks for Industry 4.0	Connects WSN monitoring with smart manufacturing

Methodology

1. System Requirements and Design Scope

The methodology begins by defining what must be monitored, how quickly abnormal conditions must be reported, and what level of communication reliability is acceptable. For the reference implementation, four physical variables are considered: temperature, relative humidity, vibration, and pressure. Temperature and vibration represent machine-condition variables, while humidity and pressure represent environmental or process variables. The WSN is designed for monitoring and alarm generation rather than direct safety shutdown. A routine sampling interval of 5 s is used, but event packets are transmitted immediately when a threshold is exceeded. This mixed reporting strategy reduces network traffic while preserving fast notification of abnormal conditions, consistent with the mixed-criticality perspective described by Jin et al. [10].

The design targets a small industrial area containing approximately 10-20 sensor nodes and one gateway. Each node must operate from a local low-voltage supply or battery, support at least one digital or analog sensor, provide a unique node identifier, and communicate through the 2.4 GHz IEEE 802.15.4 physical layer. A star topology is acceptable when every node has a strong direct path to the coordinator; a star-mesh topology is used when machinery or walls create shadowed areas. The gateway provides

protocol termination, time stamping, buffering, and forwarding to the supervisory computer.

2. Sensor Node and Gateway Architecture

Each sensor node contains four functional blocks: sensing, signal conditioning, processing, and radio communication. A low-power microcontroller samples the connected sensors through analog-to-digital converter channels or digital buses. Raw values are converted into engineering units using calibration coefficients stored in non-volatile memory. A simple moving-average filter is applied to temperature, humidity, and pressure measurements, whereas vibration data are summarized using root-mean-square magnitude over a short acquisition window. Local threshold comparison is performed before wireless transmission so that abnormal events can be assigned priority. This distribution of processing reduces unnecessary communication, which is important because radio activity is a major contributor to sensor-node energy consumption [1,7].

The gateway consists of an IEEE 802.15.4 coordinator interface connected to a single-board computer or industrial PC through serial or USB communication. Gateway software validates the packet checksum, associates the node identifier with its installation location, records the reception time, and stores the values in a local database. A dashboard displays current values and trends, while an alarm service compares incoming event flags with configured

severity levels. Gateway access should be authenticated, and node commissioning keys or network credentials should be protected to

reduce the security risks described in industrial mesh networks [4].



Figure 1. Proposed WSN architecture for industrial monitoring applications.

3. Communication and Network Formation

Before installation, the available 2.4 GHz channels are scanned near the production equipment to identify persistent interference from Wi-Fi, Bluetooth, or other industrial radios. The deployment begins with the coordinator at an elevated, electrically quiet location close to the monitoring computer. Sensor nodes then join the network using their unique identifiers. For low-latency monitoring, acknowledgments and bounded retransmissions are enabled. Neighbor information and received-signal-strength indication (RSSI) are recorded during commissioning. Links weaker than the deployment threshold are improved by relocating the node, changing antenna orientation, adjusting transmission power, or adding a router node. Industrial standards commonly use channel diversity and scheduled access for improved dependability [5,8,9]; the proposed low-cost implementation adopts the same principle conceptually by selecting the least congested channel and retaining redundant paths where possible.

4. Data Packet, Firmware Logic, and Alarm Handling

A compact application packet is used to minimize airtime. The packet contains a start byte, node identifier, sequence number, sensor type, measured value, status flags, battery or supply indicator, and checksum. The sequence number allows the gateway to detect lost or duplicated packets. Sensor firmware operates as a state machine with initialization, sensing, processing, transmission, acknowledgment, and low-power waiting states. If a routine transmission fails, the packet is retried up to a predefined limit. If an abnormal threshold is detected, the node transmits an event packet immediately and repeats the notification after a short-randomized delay if an acknowledgment is not received. This mechanism provides higher urgency to alarm

traffic without requiring continuous high-rate transmission.

Thresholds should be established from machine manuals, process limits, baseline measurements, or maintenance policy. To avoid repeated alarms caused by measurement noise, each threshold incorporates hysteresis and a persistence condition. For example, a high-temperature alarm may be generated only if the measured value exceeds the limit for three consecutive samples. Similarly, a vibration warning may be based on a percentage increase from the learned baseline rather than one instantaneous peak. All threshold changes are logged at the gateway. This approach makes the system useful for condition-based maintenance while ensuring that the wireless network is not overloaded by transient spikes.

5. Experimental Procedure and Performance Metrics

The implementation is evaluated in three stages. First, each sensor is calibrated against a reference instrument and its mean absolute error is recorded. Second, radio links are characterized at representative plant locations with machinery in both idle and operating states. Third, the complete network is run continuously while routine and event packets are generated. At least 1,000 packets per test condition are recommended to obtain a stable estimate of communication performance. Tests are repeated at different distances and obstruction levels because industrial propagation can vary sharply over short spatial intervals [6].

The principal network metric is packet delivery ratio (PDR), defined as the percentage of transmitted packets correctly received at the gateway: $PDR = (N_{received} / N_{transmitted}) \times 100$. End-to-end latency is the time between packet creation at the sensor node and verified reception at the gateway. Link quality is described using RSSI and retry count. Sensor

accuracy is assessed using mean absolute error against a calibrated reference. Alarm performance is evaluated using detection rate and false-alarm rate. Reliability is interpreted at

both communication and system levels because a monitoring network may fail if either coverage or connectivity is lost, as emphasized by Deif and Gadallah [13].

Table 2. Reference prototype configuration and evaluation parameters

Item	Reference setting	Purpose
Sensor nodes	12 nodes	Covers multiple machine/environment points
Radio technology	IEEE 802.15.4, 2.4 GHz	Low-power short-range industrial monitoring
Topology	Star-mesh	Maintains connectivity around metallic obstacles
Routine sampling	5 s	Limits airtime and energy use
Alarm transmission	Immediate event packet	Reduces abnormal-condition reporting delay
Test duration	8 h per deployment condition	Captures interference and link variability
Evaluation	PDR, latency, RSSI, sensor MAE, alarm rate	Quantifies communication and sensing quality

Step-by-Step Implementation Procedure

Step 1 - Identify monitoring points and variables. Mark each machine or process location and define normal, warning, and alarm ranges.

Step 2 - Select sensor and node hardware. Match sensor range and accuracy to the industrial variable, and select a microcontroller/radio platform with adequate interfaces.

Step 3 - Calibrate and validate sensing channels. Compare each sensor against a reference instrument and store calibration coefficients.

Step 4 - Survey the radio environment. Record interference, RSSI, obstructions, and likely gateway/router positions before permanent mounting.

Step 5 - Configure network and security parameters. Assign node IDs, channel, network identifier, keys, acknowledgment policy, retry limit, and reporting interval.

Step 6 - Deploy nodes and verify connectivity. Mount sensors safely, check packet reception, and add relay nodes or reposition antennas where links are weak.

Step 7 - Implement database, dashboard, and alarm logic. Store time-stamped readings, visualize trends, and configure threshold notifications.

Step 8 - Conduct performance testing. Measure PDR, latency, retries, sensing error, and alarm behavior under normal and high-interference conditions.

Results

Because no user-supplied laboratory dataset accompanies this methodology paper, the values in this section are presented as an illustrative prototype-evaluation dataset for a 12-node implementation following the procedure above. They demonstrate how results should be reported and interpreted; empirical publication should replace them with measurements from the actual installation. The evaluation considers four representative radio conditions: short-range line of sight, moderate range with partial obstruction, operation near active machinery, and a metal-rich area with a weak direct path.

Table 3. Illustrative communication performance of the prototype WSN

Condition	Mean RSSI (dBm)	PDR (%)	Mean latency (ms)	Mean retries/packet
5 m, line of sight	-49	99.2	82	0.04
15 m, partial obstruction	-63	97.8	116	0.11
25 m, machinery operating	-72	94.6	171	0.27
30 m, metal-rich weak path	-80	90.8	238	0.44

The illustrative results show the expected relationship between received signal strength and packet delivery. The strongest line-of-sight condition maintains a PDR above 99%, while operation near machinery and in a metal-rich zone increases retries and latency. Even when the weakest path remains usable, a PDR near 91% would be inadequate for high-confidence industrial alarming unless redundancy or route improvement were introduced. In practice, such

a link would trigger corrective action during commissioning, such as relocating the node, increasing antenna separation from metal surfaces, or adding a relay. This agrees with real-life industrial observations that propagation quality is highly location dependent [6] and with the design philosophy of industrial mesh standards that use path and channel diversity [5,8].

Table 4. Illustrative sensing and alarm-validation results

Measured variable	Illustrative MAE	Alarm detection rate	False-alarm rate
Temperature	0.38 °C	98.0%	1.8%
Relative humidity	1.9 %RH	96.0%	2.5%
Vibration RMS	0.06 g	96.7%	2.4%
Pressure	0.7% of span	97.3%	1.9%

The sensor-side results indicate that calibration and local filtering can keep measurement error within a practical monitoring range for general condition monitoring. Alarm-detection performance is improved by persistence checking and hysteresis because isolated noise excursions are rejected. Event packets also experience lower practical reporting delay than a purely periodic system because abnormal measurements are transmitted immediately rather than waiting for the next routine interval. The approach therefore supports a two-level traffic model: low-rate periodic data for trends and high-priority event traffic for abnormal conditions. This principle is compatible with the differentiated scheduling requirements discussed for industrial WSNs [10].

From an implementation perspective, the most significant observation is that communication quality cannot be guaranteed solely by choosing a nominal radio range. Link behavior depends on installation height, orientation, metal proximity, machinery state, and competing 2.4 GHz traffic. Adaptive transmission power can reduce excessive energy use on strong links while improving margin on weak links [7], but power adjustment should not replace good physical deployment. For locations that remain unreliable, additional routing redundancy is preferable. The design therefore uses a commissioning criterion in which weak or highly variable links are corrected before the network is accepted for routine monitoring.

The illustrative network meets the intended non-safety-critical monitoring objective under the first three conditions, where PDR remains above approximately 94% and average latency is below 200 ms. The weakest condition is treated as a deployment failure requiring topology modification. This result highlights a key

methodological point: industrial WSN performance should be accepted against explicit thresholds rather than assumed from successful network association alone.

Discussion

The proposed methodology translates established industrial wireless principles into a practical implementation sequence. Its main advantage is modularity. Sensors can be changed without redesigning the complete network, and the gateway separates the low-power WSN from the database and visualization layer. This is useful for small and medium plants that need additional monitoring points but cannot justify extensive new cabling. The architecture also supports incremental deployment: a few nodes can be commissioned first, and additional nodes or routers can be added after link-quality measurements are available.

The literature demonstrates that industrial wireless communication is fundamentally a reliability problem as well as a connectivity problem. Gungor and Hancke [3] stressed harsh-channel effects and system-level design, while Petersen and Carlsen [5] and Wang and Jiang [9] showed how industrial standards use time synchronization, hopping, routing, and network management to counter these effects. The low-cost reference design in this paper does not reproduce every feature of WirelessHART or ISA100.11a, but it adopts their key engineering lessons: avoid single weak links, control channel use, confirm delivery, distinguish urgent traffic, and continuously observe network health. For applications with stronger determinism or certification requirements, the same sensing methodology can be migrated to a fully compliant industrial wireless protocol.

Security must also be treated as part of implementation rather than an optional software feature. Unauthorized joining, forged readings, replayed packets, or gateway compromise could cause incorrect maintenance decisions. The security analysis by Alcaraz and Lopez [4] supports the use of authenticated commissioning, network keys, integrity checks, and restricted gateway services. The design should additionally isolate the monitoring network from business IT systems through controlled interfaces. When the system is used only for monitoring, a compromise should not directly command actuators or bypass independent safety systems.

Energy consumption is another design trade-off. Short sampling intervals and frequent retries increase radio duty cycle. Conversely, very long intervals can delay detection of gradual changes if local event logic is poorly configured. The proposed 5 s routine interval is therefore only a reference setting; slower environmental variables can be sampled less frequently, while high-frequency vibration analysis may require local feature extraction rather than continuous transmission of raw waveforms. Transmission-power adaptation, as investigated by Ikram et al. [7], is useful when nodes experience large link-margin differences. However, lifetime estimates should be validated from measured current profiles and the actual supply arrangement.

A final limitation is that WSN reliability depends on both node health and network structure. Deif and Gadallah [13] showed that coverage and connectivity must be evaluated together and that component failures can change node function over time. Accordingly, periodic maintenance should include battery or supply checks, sensor calibration checks, link-quality trend review, and confirmation that each critical monitoring point has an adequate communication path. This transforms the WSN from a one-time installation into a maintainable industrial instrumentation system.

Conclusion

This paper presented a step-by-step methodology for implementing wireless sensor networks for industrial monitoring applications using distributed sensing nodes, a low-power IEEE 802.15.4-class wireless network, and a gateway-based monitoring layer. The method begins with requirement definition and calibration, proceeds through radio-site assessment, network configuration, deployment, security setup, and dashboard integration, and ends with quantitative acceptance testing. Packet

delivery ratio, latency, RSSI, sensing error, and alarm-detection metrics provide a practical basis for judging whether the installed network is suitable for service. The literature up to 2017 shows that dependable industrial wireless monitoring requires more than simple radio connectivity. It requires interference-aware deployment, redundancy, priority handling, security, and continued evaluation of network health. The illustrative prototype results show how these metrics can be used to identify acceptable links and to reject weak deployment locations before routine operation. For non-safety-critical condition monitoring, the proposed architecture can lower cabling effort and support flexible expansion while providing timely data for maintenance and operational awareness. Future implementation work should replace the illustrative dataset with measurements from the target plant and may extend the design using standardized WirelessHART or ISA100.11a networks, energy harvesting, edge analytics, and integration with industrial maintenance platforms.

References

- I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002. DOI: 10.1016/S1389-1286(01)00302-4.
- 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, 2006. DOI: 10.1109/TII.2006.872960.
- V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: challenges, design principles, and technical approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, 2009. DOI: 10.1109/TIE.2009.2015754.
- C. Alcaraz and J. Lopez, "A security analysis for wireless sensor mesh networks in highly critical systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, vol. 40, no. 4, pp. 419–428, 2010. DOI: 10.1109/TSMCC.2010.2045373.
- S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a: the format war hits the factory floor," *IEEE Industrial Electronics Magazine*, vol. 5, no. 4, pp. 23–34, 2011. DOI: 10.1109/MIE.2011.943023.

K. Mikhaylov, J. Tervonen, J. Heikkilä, and J. Käsäkoski, "Wireless sensor networks in industrial environment: real-life evaluation results," in 2012 2nd Baltic Congress on Future Internet Communications, pp. 1–7, 2012. DOI: 10.1109/BCFIC.2012.6217971.

W. Ikram, S. Petersen, P. Orten, and N. F. Thornhill, "Adaptive multi-channel transmission power control for industrial wireless instrumentation," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 978–990, 2014. DOI: 10.1109/TII.2014.2310594.

M. Nobre, I. Silva, and L. A. Guedes, "Routing and scheduling algorithms for WirelessHART networks: a survey," Sensors, vol. 15, no. 5, pp. 9703–9740, 2015. DOI: 10.3390/s150509703.

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, 2016. DOI: 10.1109/COMST.2016.2548360.

X. Jin, C. Xia, H. Xu, J. Wang, and P. Zeng, "Mixed criticality scheduling for industrial wireless sensor networks," Sensors, vol. 16, no. 9, art. 1376, 2016. DOI: 10.3390/s16091376.

A. V. Sukhanov, I. V. Prokofev, and A. V. Ivanov, "A universal digital platform for the construction of self-organizing wireless sensor networks for industrial safety and ecological monitoring systems," Russian Microelectronics, vol. 45, pp. 137–141, 2016. DOI: 10.1134/S1063739716020098.

X. Li, D. Li, J. Wan, A. V. Vasilakos, C.-F. Lai, and S. Wang, "A review of industrial wireless networks in the context of Industry 4.0," Wireless Networks, vol. 23, no. 1, pp. 23–41, 2017. DOI: 10.1007/s11276-015-1133-7.

D. S. Deif and Y. Gadallah, "A comprehensive wireless sensor network reliability metric for critical Internet of Things applications," EURASIP Journal on Wireless Communications and Networking, vol. 2017, art. 145, 2017. DOI: 10.1186/s13638-017-0930-3.