Security and Reliability Are Key in Wireless Networks for Industrial IoT

Ross Yu, Product Marketing Manager
SmartMesh® Products, Analog Devices

The Industrial Internet of Things (IoT) calls for wireless sensing and control nodes for use in a wide range of applications from factories and industrial process plants to building energy efficiency, smart parking applications and commercial agriculture. In all of these applications, Industrial IoT wireless solutions are expected to operate for many years, often in harsh RF environments and extreme atmospheric conditions. Unlike consumer applications, where cost is often the most important system attribute, industrial applications typically rate reliability and security at the top of the list.

In *ON World's* global survey of industrial wireless sensor network (WSN) users, reliability and security are the two most important concerns cited.[1] This is not surprising, considering that a company's profitability, the quality and efficiency with which they produce goods, and worker safety often relies on these networks. Indeed, Industrial IoT solution providers identified the selection of WSN platform to be pivotal to the success of their wireless Industrial IoT business. This article explains the importance of data reliability and network security in Industrial IoT applications, examines real-life case studies, and discusses key considerations when selecting an Industrial IoT wireless solution.

Data Reliability in a Wireless Sensor Network

In an industrial plant or factory, the need for high reliability is well understood since a single missing data point may result in a factory shutdown or safety issues. In the broader set of industrial applications, although the intermittent loss of data packets may be tolerated, extended periods of communications outage are not acceptable. Even a 1% data failure rate is too high, since it translates to 3.65 days per year of unscheduled downtime. Industrial IoT solution providers have noted that one half-day of communications outage would result in irate customers and the cost of an on-site technician visit. If a second such outage were to occur, there is a high likelihood of losing their customer. Therefore, industrial applications demand >99.999% data reliability to overcome the wide variety of RF problems they will likely experience over years of operation.

In order for a wireless network to run virtually maintenance-free for many years, it must be architected with multiple means of overcoming problems. One general principle in designing a network for reliability is redundancy, where failover mechanisms for likely problems enable systems to recover without data loss. In a wireless sensor network, there are two basic opportunities to harness this redundancy. First is the concept of spatial redundancy, where every wireless node has at least two other nodes with which it can communicate, and a routing scheme that allows data to be relayed to either node, but still reach the intended final destination. A properly formed mesh network—one in which every node can communicate with two or more adjacent nodes—enjoys higher reliability than a point-to-point network by automatically sending data on an alternate path if the first path is unavailable.

The second level of redundancy can be achieved by using multiple channels available in the RF spectrum. The concept of channel hopping ensures that pairs of nodes can change channels on every transmission, thereby averting temporary issues with any given channel in the ever changing and harsh RF environment typical of industrial applications. Within the IEEE 802.15.4 2.4GHz standard, there are fifteen spread spectrum channels available for hopping, affording channel hopping systems much more resilience than non-hopping (single channel) systems. There are several wireless mesh networking standards that include this dual spatial and channel redundancy known as Time Slotted Channel Hopping (TSCH), including IEC62591 (WirelessHART) and the forthcoming IETF 6TiSCH standard.[2] These mesh networking standards, which utilize radios in the globally available unlicensed 2.4GHz spectrum, evolved out of work by Analog Devices' SmartMesh team, which pioneered the use of TSCH protocols on low power, resource constrained devices since 2002 with SmartMesh products.

[1] Industrial Wireless Sensor Networks: Trends and Developments, https://www.isa.org/standards-publications/isa-publications/intech-magazine/2012/october/web-exclusive-industrial-wireless-sensor-networks/

[2] 6TiSCH Wireless Industrial Networks: Determinism Meets IPv6: Maria Rita Palattella, Pascal Thubert, Xavier Vilajosana, Thomas Watteyne, Qin Wang, and Thomas Engel. Published in: Communications Magazine, IEEE (Volume: 52, Issue: 12).

While TSCH is an essential building block for data reliability in harsh RF environments, the creation and maintenance of the mesh network is key for continuous, problem-free multi-year operation. Over its lifetime, an industrial wireless network will be subject to vastly different RF challenges and data transmission requirements. Therefore, the final ingredient required for wire-like reliability is intelligent network management software that dynamically optimizes the network topology, continuously monitoring link quality to maximize throughput despite interference or changes to the RF environment.

Case Study #1: TSCH Network at Semiconductor Wafer Fabrication Facility

Analog Device' TSCH-based SmartMesh IP™ has been deployed at their wafer fabrication (fab) facility in Silicon Valley to monitor pressure for hundreds of specialty gas cylinders used in the various etching and cleaning stages of wafer fabrication. Previously, each cylinder's pressure was checked manually three times a day, for a total of 4 hours of manual work per day. A SmartMesh IP network was deployed to automate the measurements and send the readings directly to the facility's control center software. In the gas bunker, 32 wireless nodes were deployed with each node measuring a pair of cylinders for tank pressure and regulated pressure. The network generates an aggregate of 3kbps of sensor data. RF conditions in the fab are typical of an industrial environment, with wireless nodes surrounded by metal, concrete and with work crew and equipment moving in the area throughout the day. The network has been in operation over 83 days continuously, has sent over 18.8Gbits of data and has experienced over 7 nines (>99.99999%) of reliability.

Table 1. Network Statistics—SmartMesh IP Network at Analog Devices' Wafer Fab Facility

Number of Wireless Nodes	32 (Each with 4 Sensors Generating Data)
Mesh Network Depth	4 Hops from Furthest Node to Gateway
Data Generation Rate of Entire Network	3kbps
Total Data Sent	>18.8Gbits Over 83 Days
Data Reliability	>99.999996% Data Reliability – Seven Nines of Reliability

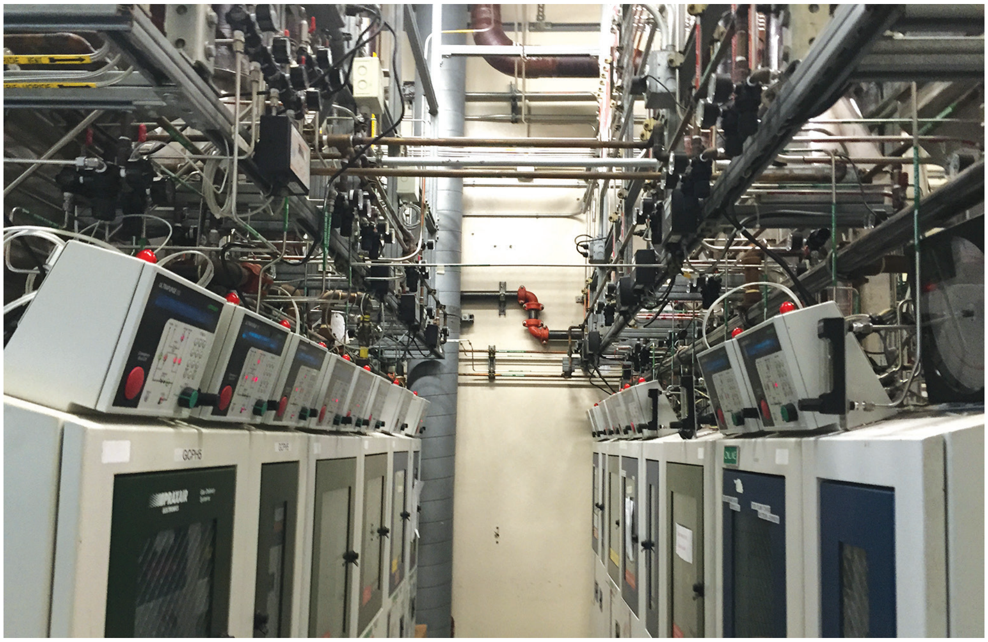


Figure 1. Dense Metal and Concrete—Wireless Nodes Must Perform Reliably Even When Located Among Metal Equipment and Gas Distribution Pipes

Case Study #2: TSCH Network at Electronica 2016

Trade show exhibition floors are notoriously noisy RF environments and therefore excellent benchmarks for WSN reliability. At Electronica 2016, the world's largest electronic component trade show, VersaSense[3] from Belgium demonstrated their SmartMesh IP based wireless system. The RF environment was extremely busy with 52 Wi-Fi networks in operation, in addition to the many thousands of cellular and Bluetooth devices carried by attendees. Over the course of the three-day exhibition the VersaSense system sent over 75.5Mbits of data at 100% data reliability in this saturated RF environment.[4]

The Importance of Network Security

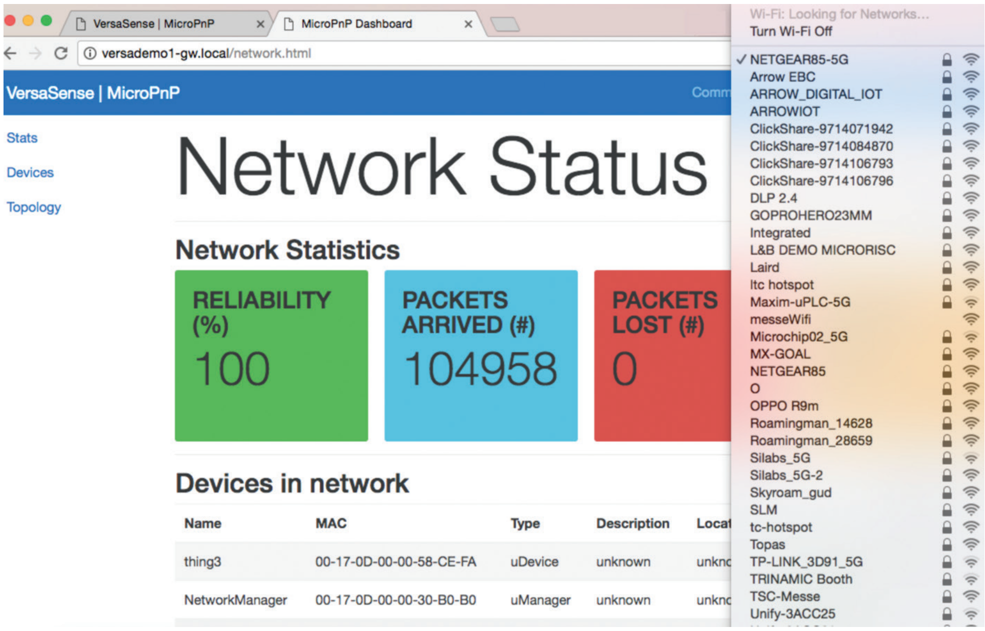
Security is another critical attribute of industrial wireless sensor networks. The primary goals for security within a WSN are:

- *Confidentiality:* Data transported in the network cannot be read by anyone but the intended recipient.
- *Integrity:* Any message received is confirmed to be exactly the message that was sent, without additions, deletions or modifications of the content.
- *Authenticity:* A message that claims to be from a given source is, in fact, from that source. If time is used as part of the authentication scheme, authenticity also protects a message from being recorded and replayed.

Confidentiality is required, not only for security-related applications, but also for common everyday applications. For example, sensor information regarding production levels or equipment status may have some competitive sensitivity—e.g., the National Security Agency (NSA) doesn't publish the power consumption of their data centers because this data might be used to estimate computing resources.

[3] www.versasense.com

[4] Video: SmartMesh IP Reliability at Electronica 2016: http://www.linear.com/solutions/7691



Network Status

Network Statistics

RELIABILITY (%)	PACKETS ARRIVED (#)	PACKETS LOST (#)
100	104958	0

Devices in network

Name	MAC	Type	Description	Locat
thing3	00-17-0D-00-00-58-CE-FA	uDevice	unknown	unknc
NetworkManager	00-17-0D-00-00-30-B0-B0	uManager	unknown	unknc

Figure 2. Network Reliability at Electronica 2016—Even in the Presence of Over 50 Wi-Fi Networks, the SmartMesh IP Network Delivered Over 75.5Mbits of Data (104,958 Packets of 90-Byte Payload) at 100% Data Reliability

Sensor data should be encrypted so that only the intended recipient can use it. Both sensing and command information needs to arrive intact. If a sensor says "the tank level is 72cm" or the controller says "turn the valve to 90 degrees," it could be very bad to lose one of the digits in either one of those numbers.

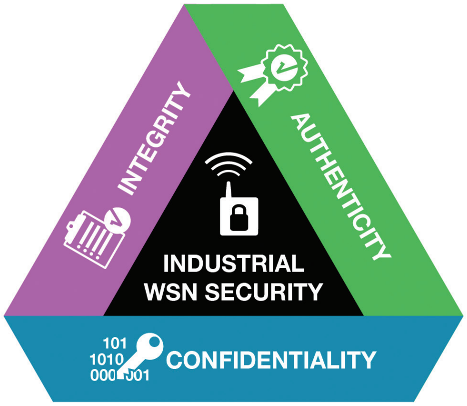


Figure 3. Industrial WSN Security—Provides Confidentiality, Integrity, Authentication of Industrial Data

Having confidence in the source of a message is critical. Either of the two messages above could have very bad consequences if they were sent by a malicious attacker. An extreme example is a message like "here's a new program for you to run."

The critical security technologies that must be incorporated into a WSN to address these goals include strong encryption (e.g., AES128) with robust keys and key management, cryptographic-quality random number generators to deter replay attacks, message integrity checks (MIC) in each message, and access control lists (ACL) to explicitly permit or deny access to specific devices. These state-of-the-art wireless security technologies may be readily incorporated in many of the devices used in today's WSNs, but not all WSN products and protocols incorporate all measures.[5] Note that connecting a secure WSN to an insecure gateway is another point of vulnerability, and end-to-end security must be considered in system design.

The consequences of poor security are not always easy to anticipate. For example, a wireless temperature sensor or thermostat might seem like a product with little need for security. However, imagine a newspaper headline describing how criminals used a radio to detect the "vacation" setting on the thermostat, and robbed those houses while the owners were gone. The impact on customer loyalty, let alone sales, would be dramatic. The safest course is to encrypt all data.

In industrial process automation, the consequences of an attack may be much more dire than the loss of a customer. With faulty process control information being delivered to the control system, an attacker could cause physical damage. For example, a sensor feeding data to a motor or valve controller saying that the motor speed or tank level is too low could result in a catastrophic failure, similar to what happened to the nuclear-enrichment program centrifuges in the Stuxnet attack.[6] On a purely practical level, even a failed attack or an academic revelation of a potential weakness is likely to lead to a loss of sales, urgent engineering effort, and a major public relations challenge.

Enabling New Industrial IoT Solutions

Highly reliability and network security are critical requirements, not only for security-related applications and industrial process settings, but for all Industrial IoT applications. Fortunately, field-proven WSN solutions are available, enabling Industrial IoT solution providers to deliver systems that work smoothly and reliably in challenging environments for many years.

[5] Secure Wireless Sensor Networks Against Attacks, Kristofer Pister and Jonathan Simon, http://electronicdesign.com/communications/secure-wireless-sensor-networks-against-attacks

[6] The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

All registered trademarks and trademarks are the property of their respective owners.

Information furnished by Analog Devices is believed to be accurate and reliable. However, no responsibility is assumed by Analog Devices for its use, nor for any infringements of patents or other rights of third parties that may result from its use. Specifications subject to change without notice. No license is granted by implication or otherwise under any patent or patent rights of Analog Devices.

LT 1117 REV A • PRINTED IN USA