Intelligence at the Edge Part 3: Edge Node Communication

Ian Beavers
Analog Devices, Inc.

Introduction

Connected industrial machines can sense a wide array of information used to make key decisions within the Industrial Internet of Things (IIoT). A sensor within an edge node can be spatially far removed from any data aggregation point. It must connect through a gateway that links edge data with a network. Sensors form the front-end edge of the IIoT ecosystem. Measurements transform sensed information into quantifiable data such as pressure, displacement, or rotation. The data can be filtered to connect only the most valuable information beyond the node for processing. Low latency connections allow critical decisions as soon as the key data is available.

Sense, Measure, Interpret, Connect

The edge node typically must be connected to a network, either through a wired or wireless sensor node (WSN). Data integrity remains key in this block of the signal chain. Optimum sensed and measured data is of little value if communication is inconsistent, lost, or corrupted. Ideally, a robust communication protocol will be designed as a forethought during system architecture design. The best choice will depend upon connectivity requirements: range, bandwidth, power, interoperability, security, and reliability.

Wired Devices

Industrial wired communications play a key role when the robustness of the connection is paramount, such as is the case with EtherNet/IP®, KNX, DALI, PROFINET®, and Modbus® TCP. Far reaching sensor nodes may use a wireless network to communicate back to a gateway that then relies upon a wired infrastructure. Relatively few connected IoT nodes will exclusively use wireline communications as the bulk of these devices will connect wirelessly. An effective IIoT connection strategy enables sensors to be located anywhere valuable information can be sensed, not only where incumbent communications and power infrastructure reside.

Sensor nodes must have a method of communication with the network. Ethernet tends to dominate the wired realm as IIoT frameworks map higher level protocols on this type of connectivity. Ethernet implementations range from 10 Mbps up to 100 Gbps and beyond. The high end generally targets the backbone of the internet to link server farms in the cloud.[1]

Slower speed industrial networks such as KNX operate over a twisted copper pair using differential signaling and a 30 V supply with a total bandwidth of 9600 bps. While a constrained number of addresses (256) can be supported per segment, addressing can support 65,536 devices. The maximum segment length is 1000 m with the option to have line repeaters support up to 4 segments.

Industrial Wireless Challenges

When considering which communications and network technologies to adopt, IIoT wireless system designers face many challenges. As such, the following constraints should be held under high level review:

- Range
- Intermittent vs. continuous connectivity
- Bandwidth
- Power
- Interoperability
- Security
- Reliability

Range

Range describes the distances over which data is transmitted by IIoT devices attached to the network. A short-range personal area network (PAN) where ranges are measured in meters can make sense for commissioning equipment over BLE. A local area network (LAN) up to hundreds of meters can be used for automation sensors installed within the same building. A wide area network (WAN) is measured in kilometers, and its applications include agricultural sensors installed across a large farm.

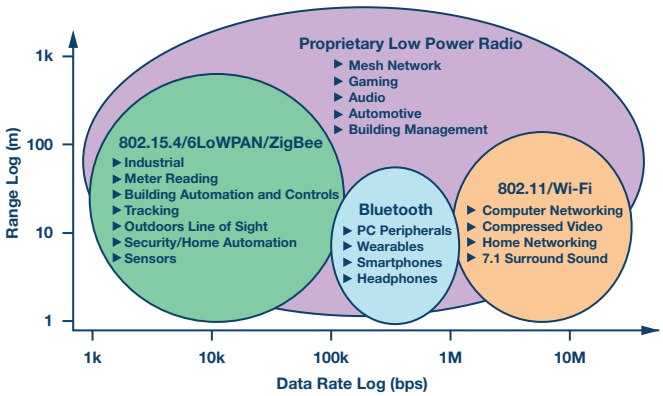

Figure 1. Short-range wireless connections.

The network protocol selected should match the range required for the IIoT use case. For example, a 4G cellular network would be inappropriate in complexity and power for an indoor LAN application operating over tens of meters. When transmitting data over the required range presents a challenge, edge computing can be a viable alternative. Perform data analysis within the edge nodes, rather than moving data elsewhere for processing.

Transmitted radio waves follow an inverse square law for power density. The signal power density is proportional to the inverse square of the distance the radio wave has travelled. As the transmitted distance is doubled, the radio wave retains only ¼ of its original power. Each 6 dBm increase in transmit output power doubles the possible range.

In ideal free space, the inverse square law is the only factor affecting transmit range. However, real-world range can be degraded by obstacles such as walls, fences, and vegetation. Air humidity can absorb RF energy. Metal objects can reflect radio waves, causing secondary signals to reach the receiver at different times, and creating destructive interference as an additional power loss.

Radio receiver sensitivity will dictate the maximum signal path loss that can be realized. For example, in the 2.4 GHz industrial scientific and medical (ISM) band, the minimum receiver sensitivity is –85 dBm. RF radiator energy propagates uniformly in all directions to form a sphere ($A = 4\pi R^2$), where R is the distance from the transmitter to the receiver in meters. Free-space power loss (FSPL) is proportional to the square of the distance between the transmitter and receiver and the square of the radio signal frequency based on the Friis transmission equation set.[2]

$S = \frac{Pt}{4 \times \pi \times R^2}$ where Pt = transmitted power in watts and S = power at distance R

$Pr = \frac{s \times \lambda^2}{4 \times \pi}$ where Pr = received power in watts

λ (transmitted wavelength in m) = c (speed of light)/f (Hz) = 3×10^8 $(m/s^2)/f(Hz)$ or 300/f (MHz)

$$FSPL\ (dB) = \frac{Pt}{Pr} = \frac{4 \times \pi \times R^2}{\lambda^2} = \frac{(4 \times \pi \times R \times f)^2}{c^2} =$$

$$20 \log \frac{4 \times \pi \times R \times f}{c}$$ where f = transmitted frequency

Given the known transmit frequency and required distance, the FPSL can be calculated for the transmit and receive pair of interest. The link budget will take the form in the following equation:

$$Received\ power\ (\text{dBm}) = Transmitted\ power\ (\text{dBm}) + gains\ (\text{dB}) - losses$$

Bandwidth and Connectivity

Bandwidth is the data rate that can be transmitted within a specific period of time. It limits the maximum rate at which data can be collected from IIoT sensor nodes and transmitted downstream. Consider these factors:

- Total amount of data each device is generating over time
- Number of nodes deployed and aggregated within a gateway
- Available bandwidth needed to support peak periods of burst data sent in either a constant stream or as intermittent bursts

The packet size of the networking protocol should ideally match with the size of the data being transmitted. It is inefficient to send packets padded with empty data. However, there is also overhead in splitting larger chunks of data up across too many small packets. IIoT devices are not always connected to a network. They may connect periodically in order to conserve power or bandwidth.

Power and Interoperability

If an IIoT device must operate on a battery to conserve power, the device can be put into sleep mode whenever it is idle. The energy consumption of the device can be modeled under different network loading conditions. This can help ensure the device's power supply and battery capacity match the consumption required to transmit necessary data.[3]

Interoperability across an array of different possible nodes within a network can be a challenge. Adopting standard wired and wireless protocols has been the traditional approach for maintaining interoperability within the internet. Standardization for new IIoT processes can be a struggle to keep up with the rapid pace of new released technologies. Consider the IIoT ecosystem around the best technologies that fit the solution at hand. If the technology is widely adopted, there is a higher probability of long-term interoperability.

Security

IIoT network security has three important aspects within the system: confidentiality, integrity, and authenticity. Confidentiality relies upon network data staying only within the known framework without allowing data to be compromised or intercepted from outside devices. Data integrity depends upon message content remaining exactly the same as what was transmitted, without altering, subtracting, or adding information.[4,5] Authenticity relies upon receiving data from an expected, exclusive source. Erroneously communicating with a spoof is an example of a false authentication.

A secure wireless node interfacing to an unsecure gateway is a vulnerability hole and provides potential for a breach. A data timestamp can help identify if any signal has been hopped and retransmitted through a side channel. Time stamping can also be used to correctly reassemble out of order time critical data across a myriad of unsynchronized sensors.

Security support for AES-128 encryption can be achieved within IEEE 802.15.4 and AES-128/256 within IEEE 802.11. Key management, cryptographic-quality random number generation (RNG), and networking access control lists (ACLs) all help raise the security barriers for the communication network.

Frequency Bands

IoT wireless sensors may use licensed frequency bands within the cellular infrastructure, but these can be power hungry devices. Vehicular telematics is an application example where mobile information is gathered and short-range wireless communication is not a viable option. However, many other low power industrial applications will occupy the unlicensed spectrum in the ISM band.

The IEEE 802.15.4 low power wireless standard can be ideal for many industrial IoT applications. Operating within the 2.4 GHz, 915 MHz, and 868 MHz ISM bands, it provides 27 total channels for multiple RF channel hopping. The physical layer supports the unlicensed frequency bands depending upon global location. Europe offers a 600 kHz Channel 0 at 868 MHz, while North America has 10, 2 MHz bands centered at 915 MHz. Worldwide operation is available across 5 MHz Channel 11 through Channel 26 within the 2.4 GHz band.

Bluetooth® Low Energy (BLE) offers a significantly reduced power solution. BLE is not ideal for file transfer but more suitable for small chunks of data. A major advantage is its ubiquity over competing technologies given its widespread integration into mobile devices. The Bluetooth 4.2 core specification operates in the 2.4 GHz ISM band with a range from 50 m to 150 m and data rates of 1 Mbps using Gaussian frequency shift modulation.

Table 1. IEEE 802.15.4 Frequency Bands and Channelization

	Frequency Band (MHz)		
	868.3	902 to 928	2400 to 2483.5
Number of Channels	1	10	16
Bandwidth (MHz)	0.6	2	5
Data Rate (kbps)	20	40	250
Symbol Rate (kbps)	20	40	62.5
Unlicensed Geography	Europe	America	World
Frequency Stability	40 ppm		

When deciding upon the optimum frequency band for an IIoT solution, the pros and cons of a 2.4 GHz ISM solution should be considered:

Pro

- License-free in most countries
- Same solution for all geographic markets
- Bandwidth of 83.5 MHz allows separate channels at high data rates
- 100% duty cycle is possible
- Compact antenna compared to bands below 1 GHz

Con

- Given same output power, shorter range compared to sub-1 GHz
- Ubiquitous proliferation creates many interferering signals

Communications Protocol

A set of rules and standards to format data and control data exchange are utilized within communications systems. The open systems interconnect (OSI) model breaks the communication into functional layers for easier implementation of scalable interoperable networks. An OSI model implements seven layers: the physical (PHY), data link, network, transport, session, presentation, and application layer.

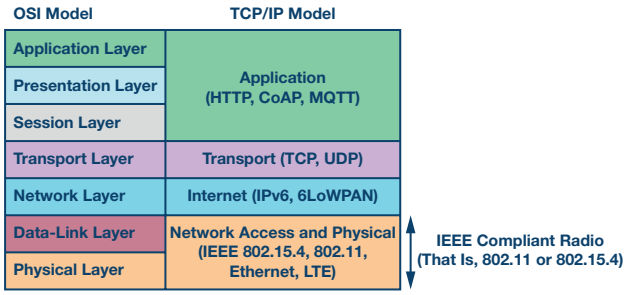

Figure 2. OSI and TCP/IP models.

The IEEE 802.15.4 and 802.11 (Wi-Fi) standards reside in the media access control (MAC) datalink sublayer and PHY layers. 802.11 access points located in close proximity should each use one of the nonoverlapping channels to minimize interference effects (Figure 3). The modulation scheme used in 802.11g is orthogonal frequency-division multiplexing (OFDM), a more complex scheme than that of IEEE 802.15.4, which will be described later.

The link layer provides the conversion of radio signal waves to bits and vice versa. This layer takes care of the data framing for reliable communication and manages access to the radio channel of interest.

The network layer routes and addresses data through the network. It is within this layer that internet protocol (IP) provides an IP address and carries IP packets from one node to another.

Between application sessions running on two ends of the network, the transport layer generates the communications sessions. This permits multiple applications to run on one device, each using its own communications channel. Connected devices on the internet predominantly use transmission control protocol (TCP) as the transport protocol of preference.

The application layer formats and governs data to optimize the flow for the specific application of the node sensor. One popular application layer protocol within the TCP/IP stack is hypertext transfer protocol (HTTP) that was developed to transfer data over the internet.

The FCC Part 15 rules limit the effective power of transmitters in the ISM bands to 36 dBm. An exception is provided for a fixed point-to-point link in the 2.4 GHz band to use an antenna with a 24 dBi gain and a transmit power of 24 dBm for a total EIRP of 48 dBm. Transmit power should be capable of at least 1 mW. For a packet error rate of <1%, receiver sensitivity should be able to accept –85 dBm within the 2.4 GHz band and –92 dBm in the 868 MHz and 915 MHz bands.

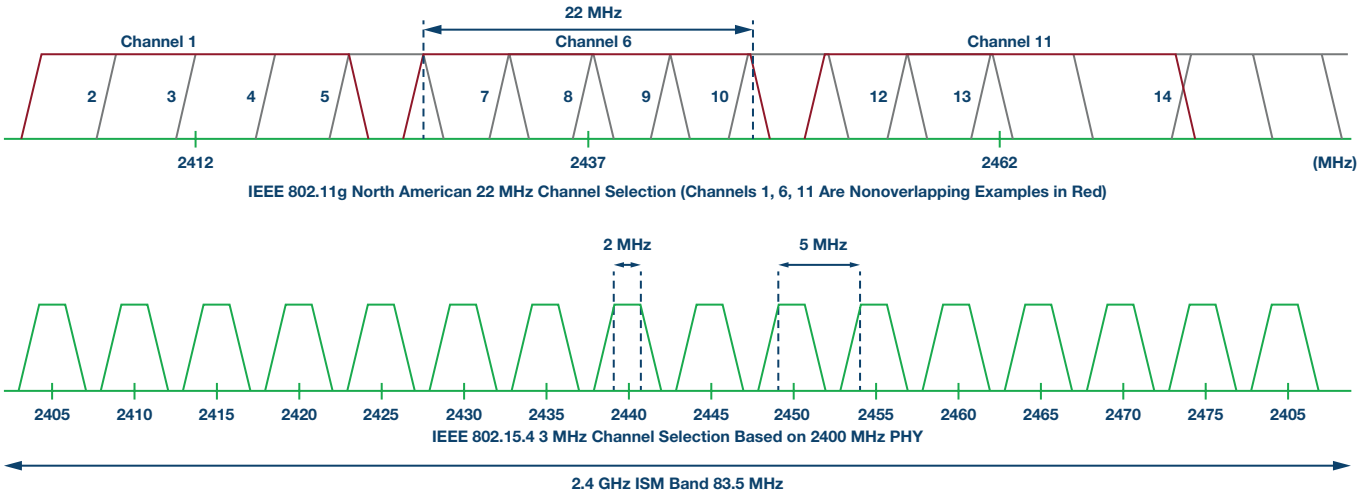

Figure 3. Worldwide IEEE 802.15.4 PHY, Channel 11 through Channel 26 and IEEE 802.11g, Channel 1 through Channel 14.

Brownfield vs. Greenfield

The IIoT implies wide connectivity with many wired and wireless standards to make it happen. However, for an installation into an existing network system, the options may not be as plentiful. The new IIoT solution may need to be adapted to fit the network.

A Greenfield installation is one created from scratch within a totally new environment. No constraints are mandated by legacy equipment. For example, when a new factory or warehouse is built, the IIoT solution can be considered within the framework plans for its optimum performance.

A Brownfield deployment refers to an IIoT network installed within an incumbent infrastructure. Challenges become more accentuated. The legacy network may not be ideal, yet the new IIoT system must coexist with any installed base of interferer RF signals. Developers inherit hardware, embedded software, and previous design decisions within a constrained context. The development process therefore becomes arduous and requires meticulous analysis, design, and testing.[6]

Network Topologies

The IEEE 802.15.4 protocol provides two device classes. A full function device (FFD) can be used in any topology to talk to any other device as a PAN coordinator. A reduced function device (RFD) is limited to a star topology as it cannot become a network coordinator. It talks only to a network coordinator in simple implementations of IEEE 802.15.4. Several network models exist, depending upon the application: peer-to-peer, star, mesh, and multihop.

A peer-to-peer network links two nodes together easily but does not leverage any intelligence to lengthen the network range. This offers rapid installation, but no redundancy if one node is not able to function.

A star model extends its total radial range to the transmission distance of two nodes as it uses an FFD as the master to communicate with several RFD. However, each RFD is still only able to communicate to the router. It can accommodate a single point of failure as long as it is not the FFD.

A mesh network allows any node to communicate or hop through any other node. This provides redundant communication paths to reinforce the strength of the network. An intelligent mesh network can route communications through the fewest hops to reduce power and latency. An ad-hoc self-organization topology adapts as the environment changes by allowing nodes to arrive within or depart from the network environment.

Reliability

IIoT customers value reliability and security at the top of the order winner list. Organizations are often reliant upon large complex clusters for data analytics that can become rife with bottlenecks including data transport, indexing, and extracting, as well as transform and load processes. Efficient communication of each edge node is paramount to prevent bottlenecks within downstream clusters.[5]

Industrial environments can often be harsh for effective RF wave propagation. Large, irregularly shaped, dense metal factory equipment, concrete, partitions, and metal shelving can all create multipath wave propagation. After, a wave leaves the transmit antenna in all directions, and "multipath" describes how the wave is modified by its environmental propagation before arriving at the receiver. Incident waves seen at the receiver are categorized into three types—reflected, diffracted, and scattered. Multipath waves experience changes in magnitude and phase, resulting in a composite wave with either constructive or destructive interference seen at the destination receiver.

CSMA-CA Channel Access

Carrier-sense multiple access with collision avoidance (CSMA/CA) is a data link layer protocol in which carrier sensing is used by network nodes. Nodes attempt to avoid collisions by transmitting their entire packet data only when the channel is sensed to be idle. Hidden nodes in a wireless network are out of range from the collection of other nodes. Figure 5 shows an example where nodes at the far edge of the range can see access point "Y," but may not see a node on the opposite end of the range, X or Z.[7]

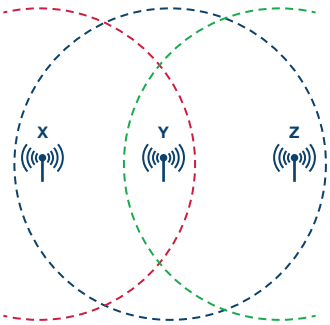

Figure 5. Hidden nodes X and Z cannot communicate directly.

Handshaking using RTS/CTS implements virtual carrier sensing with a short request to send and clear to send messages for WLANs. Although 802.11 mainly relies on physical carrier sensing, IEEE 802.15.4 uses CSMA/CA. To overcome the hidden node problem, RTS/CTS handshaking is implemented in tandem with CSMA/CA. If permissible, increasing the hidden node transmission power can lengthen its observation distance.

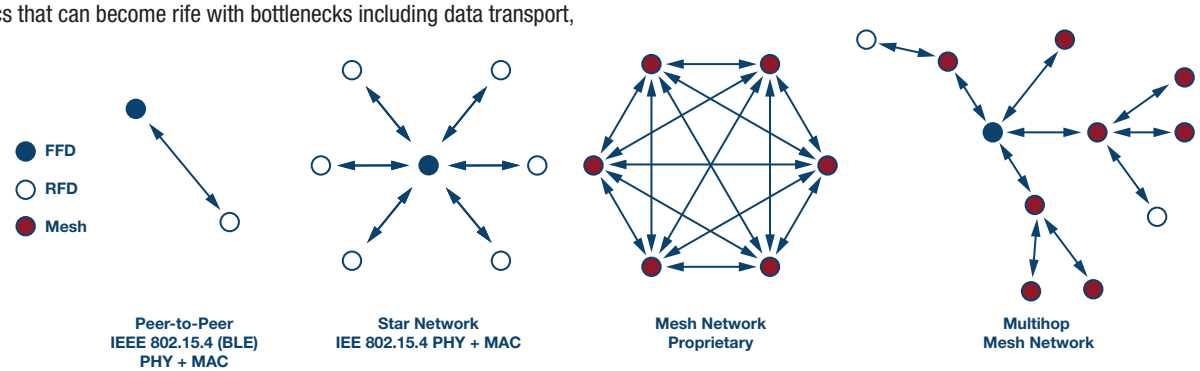

Figure 4. Network models: peer-to-peer, star, mesh, and multihop topology

Protocol

In order to improve bandwidth, advanced modulation schemes modulate phase, amplitude, or frequency. Quadrature phase shift keying (QPSK) is a modulation scheme using four phases to encode two bits per symbol. Quadrature modulation uses a mixing architecture that provides a phase shift to reduce the signal bandwidth requirement. Binary data is subdivided into two consecutive bits and modulated on the quadrature phases of the ω_c carrier, $\sin\omega_c t$, and $\cos\omega_c t$.

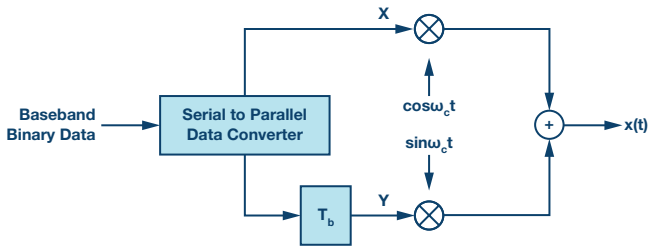

Figure 6. Offset QPSK modulator architecture.

IEEE 802.15.4 transceivers operating in the 2.4 GHz ISM band employ a physical layer variant of QPSK, called offset QPSK, O-QPSK, or staggered QPSK. A single data bit (T_{bit}) offset time constant is introduced into the bit stream. This offsets the data in time by half of the symbol period, which avoids simultaneous transitions in waveforms at nodes X and Y. Consecutive phase steps never exceed ±90°. One downside is that O-QPSK does not allow differential encoding. However, it does remove the challenging technical task of coherent detection.

Modulation used within IEEE 802.15.4 reduces the symbol rate to transmit and receive data. O-QPSK requires a ¼ symbol rate vs. bit rate by transmitting two encoded bits simultaneously. This allows a 250 kbps data rate using 62.5 ksymbols/sec.

Scalability

Not all IoT nodes require external IP addresses. For dedicated communication, sensor nodes should have the capacity for a unique IP address. While IPv4 supports 32-bit addressing, it was evident decades ago that addressing for only 4.3 billion devices would not support internet growth. IPv6 increases address size to 128 bits to support 240 undecillion globally unique address (GUA) devices.

Mapping data and management of addresses from two dissimilar domains of IPv6 and an IEEE802.15.4 network presents design challenges. 6LoWPAN defines encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4-based networks. Thread is an example of a standard based on a closed-documentation, royalty free protocol running over 6LoWPAN to enable automation.

Analog Devices provides a full selection of wireless transceivers along with wired protocols for the ADuCx family of microcontrollers and Blackfin® family of DSPs. The low power ADF7242 supports the IEEE 802.15.4 with programmable data rates and modulation schemes using the global ISM band at 50 kbps to 2000 kbps. It achieves compliance against the FCC and ETSI standards. The ADF7023 operates in the worldwide license-free ISM band at 433 MHz, 868 MHz, and 915 MHz from 1 kbps to 300 kbps. Analog Devices provides a complete WSN development platform to design a custom solution. RapID® Platform is a family of modules and development kits to embed industrial networking protocols. SmartMesh® wireless sensors are chips and precertified PCB modules with mesh networking software that enabling sensors to communicate in tough Industrial IoT environments.

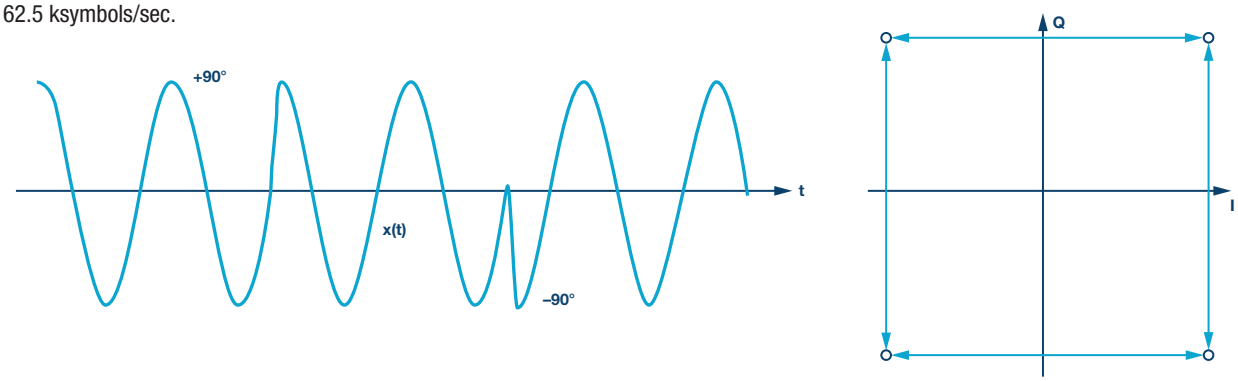

Figure 7. Phase transition ±90° (left) with I/Q O-QPSK options (right).

References

[1] Brijesh Kumar. "Connectivity Options for the Internet of Things (IoT)." *IoT Daily*, March, 2015.

[2] Chris Downey. "Understanding Wireless Range Calculations." *Electronic Design*, April, 2013.

[3] Bob Karschnia. "Industrial Internet of Things (IIoT) Benefits." *Control Engineering*, June, 2015.

[4] Joy Weiss and Ross Yu. "Wireless Sensor Networking for the Industrial IoT." *Electronic Design*, 2015.

[5] Ross Yu. "SmartMesh IP Wireless Mesh Networks Expand to Address Industrial IoT Networks." *Sensors Online*, January, 2017.

[6] Sanjay Manney. "Stringent Requirements Needed for the Industrial IoT." *EETimes*, 2014.

[7] Rana Basheer. "High Density Wireless Sensor Network: Future of Industrial IoT." *LinkedIn.com*, July, 2016.

About the Author

Ian Beavers is a product engineering manager for the Automation Energy and Sensors Team at Analog Devices (Greensboro, NC). He has worked for the company since 1999. Ian has over 19 years of experience in the semiconductor industry. Ian earned a bachelor's degree in electrical engineering from North Carolina State University and an M.B.A. from the University of North Carolina at Greensboro. He can be reached at *Ian.Beavers@analog.com*.

Online Support Community

EngineerZone™ SUPPORT COMMUNITY

Engage with the Analog Devices technology experts in our online support community. Ask your tough design questions, browse FAQs, or join a conversation.

Visit *ez.analog.com*

Analog Devices, Inc.
Worldwide Headquarters

Analog Devices, Inc.
One Technology Way
P.O. Box 9106
Norwood, MA 02062-9106
U.S.A.
Tel: 781.329.4700
(800.262.5643, U.S.A. only)
Fax: 781.461.3113

Analog Devices, Inc.
Europe Headquarters

Analog Devices GmbH
Otl-Aicher-Str. 60-64
80807 München
Germany
Tel: 49.89.76903.0
Fax: 49.89.76903.157

Analog Devices, Inc.
Japan Headquarters

Analog Devices, KK
New Pier Takeshiba
South Tower Building
1-16-1 Kaigan, Minato-ku,
Tokyo, 105-6891
Japan
Tel: 813.5402.8200
Fax: 813.5402.1064

Analog Devices, Inc.
Asia Pacific Headquarters

Analog Devices
5F, Sandhill Plaza
2290 Zuchongzhi Road
Zhangjiang Hi-Tech Park
Pudong New District
Shanghai, China 201203
Tel: 86.21.2320.8000
Fax: 86.21.2320.8222

TA16321-0-1/18(A)

analog.com

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™