Electronic Design

IAN BEAVERS | Product Engineering Manager, Automation Energy and Sensors, Analog Devices Inc.

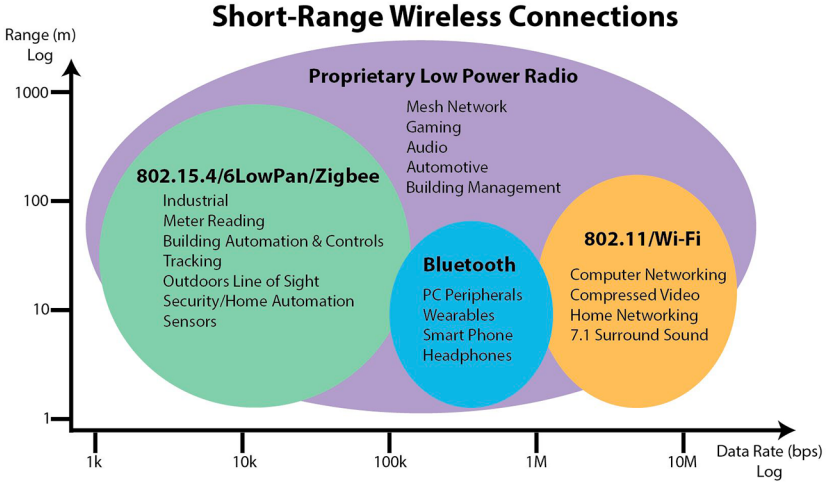
Communicating Effectively from the IIoT Edge Node

Because the value of data collected, measured, and analyzed at the edge node hinges on time and accuracy, one must understand the challenges of wireless communication when designing an IIoT ecosystem.

In an Industrial Internet of Things (IIoT) ecosystem, connected industrial machines use sensors to gather information that informs key decision-makers involved in operating efficiency, maintenance scheduling, and other mission-critical functions. Even though their physical placement is spatially removed from any specific data-aggregation point, sensors represent the front-end edge of the IIoT ecosystem, providing measurements that transform sensed information into quantifiable data such as pressure, displacement, or rotation.

This data can be filtered to connect only the most valuable information beyond the node for processing. All sensors within an edge node must connect through a gateway that links edge data with a network. Low-latency connections allow for critical decisions as soon as the key data is available. This is why the communication from the edge must be flawless for IIoT to reach its maximum potential. This article will explore the connection concepts that enable edge-node communication and the challenges that must be overcome to perfect transmission from the sensor to the network.

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



1. The graph illustrates how different short-range wireless connections vary in range and data rate.

WIRED CONNECTION

Industrial wired communications, such as Ethernet/IP, KNX, DALI, Profinet, and ModbusTCP, are the primary options when connection robustness is paramount. Far-reaching sensor nodes may use a wireless network to communicate back to a gateway that then relies on a wired infrastructure. However, relatively few connected IoT nodes will exclusively use wireline communications. An effective IIoT connection strategy places sensors anywhere valuable information can be sensed, irrespective of where incumbent communications and power infrastructure reside.

Ethernet tends to dominate the wired realm, with IIoT frameworks mapping higher-level protocols on this type of connectivity. Ethernet implementations range from 10 Mb/s up to 100 Gb/s and beyond. The high end generally targets the backbone of the internet to link server farms in the cloud *(Kumar 2015)*.

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 bits/s. While a constrained number of addresses (256) can be supported per segment, addressing can support 65,536 devices. The maximum segment length is 1,000 m with the option to have line repeaters support up to four segments.

WIRELESS CONNECTION

The majority of edge-node sensors will wirelessly communicate the collected, measured, and analyzed data to the network. Due to the value of this information being contingent on time and accuracy, it's imperative to understand the challenges of wireless communication and the several factors that must be kept in mind when designing an IIoT ecosystem. Let's take a closer look at each factor and the challenges within each.

Range

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

The network protocol selected should match the range required *(Fig. 1)*. For example, a 4G cellular network would be more complex and powerful than necessary 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. Performing data analysis within the edge nodes, rather than transmitting mass amounts of data, is more efficient.

Transmitted radio waves follow an inverse square law for power density. The signal power density is proportional to the inverse square of the distance traveled by the radio wave. As the transmitted distance is doubled, the radio wave retains only one-fourth 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—even air humidity will absorb RF energy. Also, metal objects can reflect radio waves, causing secondary signals to reach the receiver at different times, creating destructive interference as an additional power loss.

Radio receiver sensitivity will dictate the maximum signal-path loss. 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 *(Downey 2013)*:

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

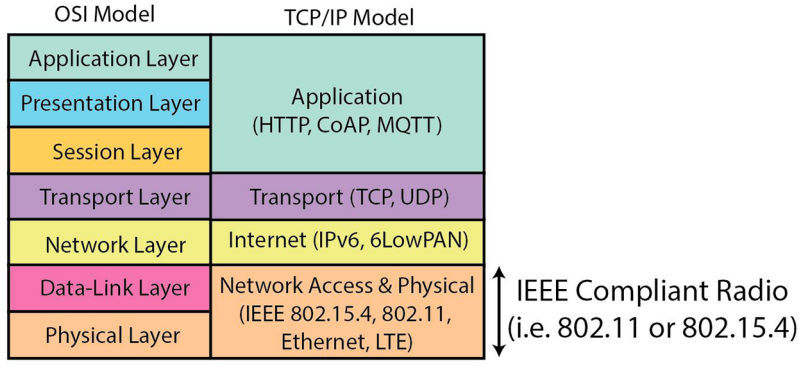
$$Pr = \frac{S*\lambda^2}{4*\pi}$$ where P_r = received power in watts

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

$$FSPL(dB) = \frac{Pt}{Pr} = \frac{4*\pi*R^2}{\lambda^2} = \frac{(4*\pi*R*f)^2}{c^2} = 20\log(\frac{4*\pi*R*f}{c})$$ where f = transmitted frequency

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

2. The IEEE 802.15.4 low-power wireless standard can be ideal for a wide array of industrial IoT applications.



3. The Open Systems Interconnect (OSI) model breaks the communication into functional layers for easier implementation of scalable interoperable networks.

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 of the equation below:

Received power (dBm) = Transmitted power(dBm) + gains(dB) - losses (dB)

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 the size of the data being transmitted. It's inefficient to send packets padded with empty data. However, there's also overhead in splitting larger chunks of data up across too many small packets. IIoT devices aren't 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 a sleep mode whenever it's idle. The device's energy consumption can be modeled under different network loading conditions. This ensures the device's power supply and battery capacity match the consumption required to transmit necessary data *(Karschnia 2015)*.

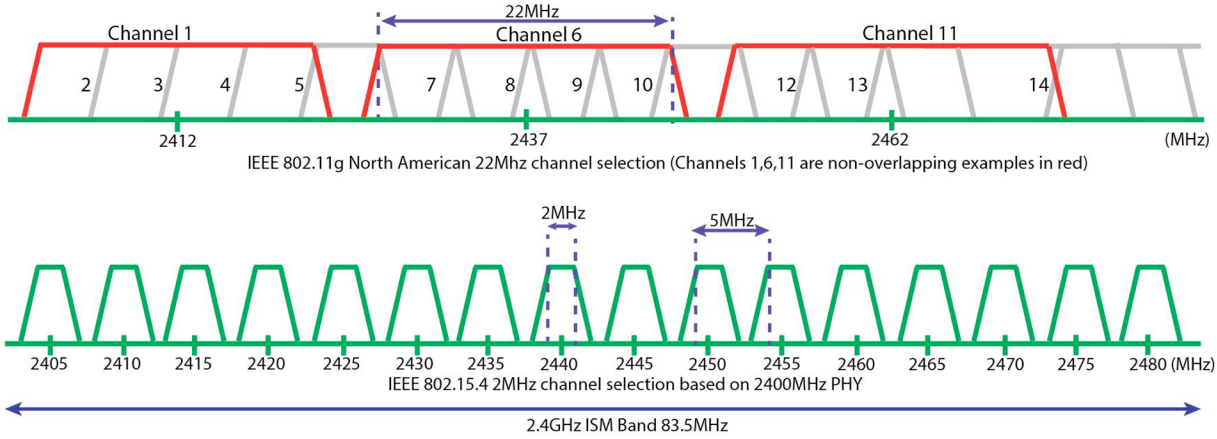
Interoperability across an array of different possible nodes within a network can be a challenge. Adopting standard wired and wireless protocols has been the traditional approach for maintaining interoperability within the internet. It can be a struggle to keep up with standardization for new IIoT processes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

Security

IIoT network security plays three important roles within the system: confidentiality, integrity, and authenticity. Confidentiality relies on network data staying within the known framework without allowing data to be compromised or intercepted from outside devices. Data integrity depends on message content remaining exactly the same as what was transmitted, without altering, subtracting, or adding information *(Weiss, Yu 2015)*. Authenticity relies on 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 re-transmitted through a side channel. Timestamping can also be used to correctly reassemble "out of order" time-critical data across a myriad of unsynchronized sensors.

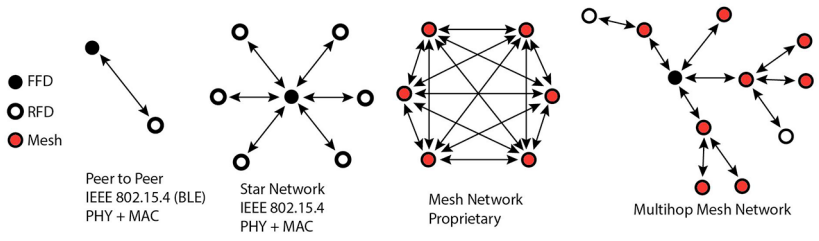
Security support for AES-128 encryption can be achieved within IEEE 802.15.4 and AES-128/256 within IEEE 802.11. Key management, cryptographic-quality random-number generation (RNG), and networking access control lists (ACL) all help raise the security barriers for the communication network.



4. The IEEE 802.15.4 and 802.11 (Wi-Fi) standards reside in the MAC data-link sublayer and PHY layers. Shown are Worldwide IEEE 802.15.4 PHY channels 11-26 and IEEE 802.11g channels 1-14.

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 isn't a viable option. However, many other low-power industrial applications will occupy the unlicensed spectrum in the ISM band.



5. Depending on the application, several network models—peer to peer, star, mesh, and multihop—are available.

The IEEE 802.15.4 low-power wireless standard can be ideal for many industrial IoT applications *(Fig. 2)*. 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 on 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 channels 11-26 within the 2.4-GHz band.

Bluetooth Low Energy (BLE) offers a significantly reduced power solution. BLE isn't 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 to 150 m and data rates of 1 Mb/s using Gaussian frequency-shift modulation.

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

Pros

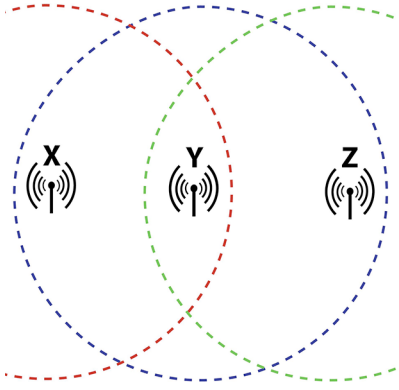
- License-free in most countries
- Same solution for all geography markets
- Bandwidth of 83.5 MHz allows for separate channels at high data rates
- 100% duty cycle is possible
- Compact antenna compared to bands below 1 GHz

Cons

- Given same output power, shorter range compared to sub-1-GHz
- Ubiquitous proliferation creates many interferer 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 *(Fig. 3)*. An OSI model implements seven layers: physical (PHY), data-link, network, transport, session, presentation, and application.



6. Hidden nodes X and Z—nodes at the far edge of the range—can't communicate directly even though they can see access point Y.

The IEEE 802.15.4 and 802.11 (Wi-Fi) standards reside in the media-access-control (MAC) data-link sublayer and PHY layers. The 802.11 access points located in close proximity should each use one of the non-overlapping channels to minimize interference effects *(Fig. 4)*. The modulation scheme used in 802.11g is orthogonal frequency-division multiplexing (OFDM).

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's 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 TCP (Transmission Control Protocol) 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 HTTP (Hyper-text Transfer Protocol), which was developed to transfer data over the internet.

The FCC part 15 rule limits 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- and 915-MHz bands.

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 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 *(Manney 2014)*.

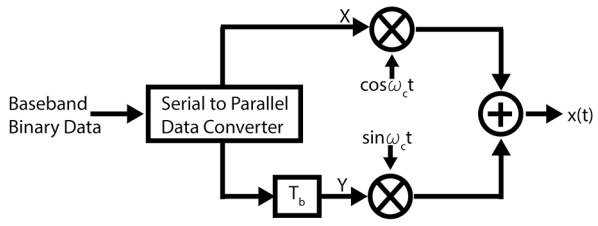
Network Topologies

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, since it can't become a network coordinator. It talks only to a network coordinator in simple implementations of IEEE 802.15.4. Several network models exist, depending on the application: peer to peer, star, mesh, and multi-hop (Fig. 5).

A peer-to-peer network links two nodes together easily, but doesn't leverage any intelligence to lengthen the network range. This offers rapid installation, but no redundancy if one node isn't 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 RFDs. However, each RFD is still only able to communicate to the router. It can accommodate a single point of failure as long as it's 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.



7. Shown is an offset QPSK modulator architecture, which is a physical-layer variant of QPSK.

Reliability

IIoT customers value reliability and security at the top of the order winner list. Organizations often rely on large complex clusters for data analytics that can become rife with bottlenecks, including data transport, indexing, and extract, as well as transform and load processes. Efficient communication of each edge node is paramount to prevent bottlenecks within downstream clusters *(Yu 2017)*.

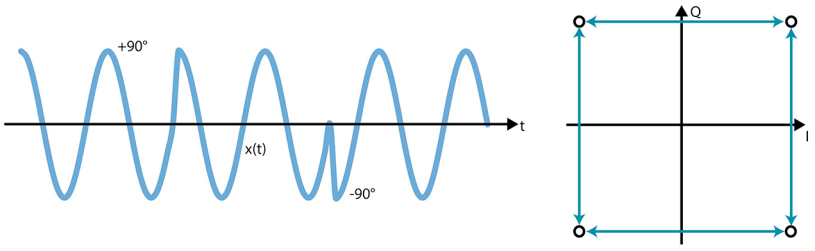
Industrial environments can often be harsh for effective RF wave propagation. Large, irregular-shaped, dense metal factory equipment, concrete, partitions, and metal shelving can all create multi-path wave propagation. After a wave leaves the transmit antenna in all directions, "multi-path" describes 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. Multi-path 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 6* 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" *(Basheer 2016)*.

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.



8. A phase transition of ±90 degrees (left) is shown with I/Q O-QPSK options (right).

Protocol

To improve bandwidth, advanced modulation schemes modulate phase, amplitude, or frequency. Quadrature phase-shift key (QPSK) is a modulation scheme that uses four phases to encode two bits per symbol. Quadrature modulation employs 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 $\cos\omega_c t$.

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 *(Fig. 7)*. 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 degrees *(Fig. 8)*. One downside is that O-QPSK doesn't allow for 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 enables a 250-kb/s data rate using 62.5k symbols/s.

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 make it possible to send and receive IPv6 packets 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.

Communication is Key

Due to the value of the information that sensors transmit back to the network, it's even more valuable to make sure the information is received efficiently and accurately. This article covered both wired and wireless connections for IIoT edge-node sensors and the possible challenges presented with each. Keeping these details in mind when designing an IIoT network rich with sensors at the edge will ensure that all information is sent and received as meticulously as it was collected, measured, and analyzed--leading to a harmonious IIoT ecosystem.

IAN BEAVERS is an Applications Engineer for the High Speed Converters team at Analog Devices Inc. in Greensboro, N.C. He has worked for the company since 1999. Ian has more than 15 years of experience in the semiconductor industry. He earned a bachelor's degree in electrical engineering from North Carolina State University and a MBA from the University of North Carolina at Greensboro. Ian is a member of EngineerZone's High-Speed ADC Support Community. Feel free to send your questions to IanB on the Analog Devices EngineerZone Online Technical Support Community.