

IoT Growth Banks on Reliable Communication

To meet the needs of the Industrial Internet of Things (IIoT), communication systems must demonstrate a high level of reliability while maintaining low costs.

According to technology industry researcher Gartner, the number of “things” in the Internet of Things (IoT) increases by 5.5 million each day. By 2020, the total number is expected to reach 20.8 billion. Given such explosive growth, it’s imperative to examine the internet that will connect and enable communication between all of these things. Creating reliable wireless connectivity among devices is proving to be one of the IoT’s greatest challenges.

The reliability of a communications system can be defined by the performance of two critical components: a radio transceiver and a communications microcontroller. This article discusses how components and solutions are able to maximize system-level reliability, enabling high-impact applications that provide mission-critical quality and integrity of data and insights.

WHAT’S GOOD NOW IS NOT GOOD ENOUGH

Existing wireless-connectivity technologies for consumer devices do not always satisfy the performance demands of industrial and healthcare systems. The different priorities in these systems—including safety, accuracy, and time-sensitivity—heighten the need for increased reliability. Cellular systems come close, but are often unsuitable in terms of battery, cost, and data-throughput requirements.

Extremely reliable systems exist today for niche industrial and military applications. However, these are designed with reliability being the top priority and cost appearing further down the list. With the Industrial Internet of Things (IIoT), the challenge becomes delivering the same high level of reliability at a much lower system cost.

Let’s consider several scenarios in which wireless capability was added to enhance the effectiveness of a system and mission-critical reliability of connectivity:



1. Smart factories have the potential to significantly enhance manufacturing.

Smart Factory: Production Process Control for Industry 4.0

Connected devices are attractive in the manufacturing arena due to the potential improvements in overall yield. To achieve this, it is often necessary to gain remote control of various devices in the production chain to implement adjustments. An example is a control valve for a boiler operating in a chemical production process. Immediate and autonomous control of this valve can make real-time adjustments based on feedback from other stages in the process, leading to more optimized overall efficiency.

Smart Healthcare: Vital Signs Monitoring

Hospitals and care centers are looking to wireless connectivity to monitor patient vital signs. Clunky wired solutions can be replaced with wireless sensor patches connected through a local gateway. Such systems enable more effective patient monitoring while reducing the burden on healthcare



2. Wireless communication systems simplify the monitoring of patients in hospitals.

staff.

Smart City: Event Sensing for Emergency Response

With advanced image and acoustic sensing and processing methods, systems mounted in public spaces (for example, on lampposts) can detect events like vehicle accidents and criminal activity with a high degree of confidence. This information can be relayed via wireless communications to the appropriate agency or unit, along with the location information, thus quickening the emergency response.

CHALLENGES IN BUILDING RELIABLE WIRELESS CONNECTIVITY IN COMPLEX ENVIRONMENTS

RF Obstacles Cause Missed Packets

Each of the examples mentioned above is subject to distinct environmental challenges that can negatively affect wireless communication. For example, the steel construction and thick walls of factories create large obstacles that may degrade the power of an RF signal to the point where it cannot be received by the target device. The radio's receiver sensitivity used in the target device will determine the tolerance level of signal degradation. A change in sensitivity that is as low as 2 dB could be the difference between successful or unsuccessful reception of a signal. Communication-system designers must pay close attention to receiver sensitivity when selecting a radio.

Crowded Frequency Bands Cause Missed Packets

Connected devices will typically operate in the relevant industrial-scientific-medical (ISM) band for a given region. ISM bands are license-free and can be used for a wide range of applications that require wireless connectivity. The 2.4-GHz band is standardized globally and extensively used by Wi-Fi and Bluetooth devices. ISM spectrum is also available in sub-1-GHz bands—a common destination for IoT applications. The sub-1-GHz band is centered at 868 MHz in Europe and

915 MHz in the U.S.

A challenge arises when multiple devices located in close proximity share the same ISM band. Transmitting devices can interfere with nearby receiving devices, such as in public hospitals that have multiple machines within the same ISM band. A radio's ability to function properly in the presence of such interferers is measured by the blocking specification.

However, the challenge extends beyond devices operating within the ISM band. Without sufficient blocking capability, mobile phones or tablets operating nearby could cause a loss of communication in the system. In military and aerospace applications, very costly components are incorporated to mitigate the effect of interferers. Radios being used for mission-critical data, such as the applications mentioned, must achieve similar performance to military and aerospace without incurring the high cost of additional external components. Such radios will continue to receive messages with multiple interferers operating nearby.

Environmental Effects Degrade Performance

Radio transceivers are built on processes prone to performance variations that depend on their surrounding environment. Such variations include temperature changes, voltage-supply reductions as batteries discharge, and silicon manufacturing variations across devices. These real-life events can cause changes in the device's operating stability.

Let's look at an event-sensing emergency-response system operating on a street light. Cold winter temperatures could cause the output power of a device to vary or the receiver sensitivity to degrade, resulting in a loss of communication. While less of a concern for a consumer device—which is rarely used in such extreme conditions—it would be unacceptable for an emergency-response system. At best, the cost is reputational damage to the end product, ending up in a service call to replace the faulty device. System designers must ensure that



3. Smart cities can take advantage of wireless communications to respond to emergency situations.

the components selected for the sensing and communication system are robust over changing environmental conditions.

Corrupted Memory Can Lead to Unexpected Outcomes

Reliability is also a concern for the communications microcontroller. Although extremely reliable, both flash and non-volatile memory can occasionally become corrupted. This may occur as a result of unintended effects caused by the operating environment, or intentionally through malicious hardware hacking.

Regardless of the mechanism, it is imperative that microcontrollers are equipped with the necessary integrity features to identify when a device has been corrupted. Once identified, the microcontroller can either correct the error or shut the device down, ensuring that the security of the wider system is not breached.

DESIGNING FOR RELIABILITY

Analog Devices' ADF7030-1 radio transceiver and ADuCM3029 Cortex-M3 microcontroller both help overcome the aforementioned challenges. They target performance levels and functionality features that lead to more robust communication links.

In many cases, the ADF7030-1 will be able to receive radio signals that are 3 dB lower than other similar radios. And with blocking numbers in excess of 100 dB, the ADF7030-1 can achieve a level of interference resilience comparable to military and aerospace equipment—without the need for ad-

ditional costly external components. This ultimately lowers overall cost while ensuring communication is maintained in the noisiest RF environments.

Through generations of collaboration with leading industrial manufacturers, Analog Devices has developed methods for coping with real-life environmental effects on radio transceivers. As an example, the output power transmitted by a device using the ADF7030-1 varies by less than 0.2 dB over the full operating temperature range. Competing radios, on the other hand, often vary by up to 2 dB.

The ADuCM3029 is designed with flash and error-correction-code (ECC) parity checks to ensure errors caused by memory corruption are identified and corrected where possible. The microcontroller also comes with battery-monitoring capability in sleep mode. This ensures that unexpected drops in voltage are detected, and that the processor is in turn alerted to a possible malicious threat or power-supply malfunction. The end device can then take appropriate action, either by alerting an administrator or entering a safe mode to ensure the wider system is not compromised.

Technologies developed by Analog Devices inhabit every stage of the IoT signal chain, from sensing and measuring to interpreting and connecting the data. Ensuring the quality and integrity of the information created through this chain is a core design principle, and a fundamental requirement to fulfill the true potential of the IoT.

