According to technology industry researcher Gartner, the number of things in the Internet of Things increases by 5.5 million each day. By 2020, the total number is expected to be 20.8 billion. Given that explosive growth, it's imperative to examine the internet that will connect and enable communication among all the things. Creating reliable wireless connectivity among these devices is proving to be one of the great challenges in IoT. The reliability of the communications system can be defined by the performance of two critical components: a radio transceiver and communications microcontroller. This article discusses how components and solutions from Analog Devices can maximize system-level reliability, enabling high impact applications where the quality, integrity of data, and insights are mission critical.

Reliable Communication Is a Key to IoT Growth

Michael Dalton
Analog Devices, Inc.

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 to this 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 industrial IoT, the challenge becomes delivering the same high level of reliability at a much lower system cost.

Let's consider some scenarios where wireless capability has been added to enhance the effectiveness of a system, and where reliability of connectivity can be mission critical.

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 staff.

Smart Factory: Production Process Control for Industry 4.0

A key attraction of connected devices in manufacturing includes the potential for yield improvements. 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, 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.
Reliable Communication Is a Key to IoT Growth

Smart City: Event Sensing for Emergency Response

With advanced image and acoustic sensing and processing methods, systems mounted in public spaces, such as on lamp posts, can detect events such as 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 to enable faster emergency response.

Environmental Effects Degrade Performance

Radio transceivers are built on processes that are prone to variations in performance, depending on the environment in which they’re operating. Some 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 operating stability of the device. 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. This can cause loss of communication under certain conditions. While this is 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 and a service call to replace the faulty device. System designers must ensure that 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 on the communications microcontroller. Although extremely reliable, both flash and nonvolatile memory can occasionally become corrupted. This can 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, appropriately ensuring that the security of the wider system is not breached.

Corrupted Memory Can Lead to Unexpected Outcomes

Reliability is also a concern on the communications microcontroller. Although extremely reliable, both flash and nonvolatile memory can occasionally become corrupted. This can 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, appropriately ensuring that the security of the wider system is not breached.

Corrupted Memory Can Lead to Unexpected Outcomes

Reliability is also a concern on the communications microcontroller. Although extremely reliable, both flash and nonvolatile memory can occasionally become corrupted. This can 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, appropriately ensuring that the security of the wider system is not breached.

Corrupted Memory Can Lead to Unexpected Outcomes

Reliability is also a concern on the communications microcontroller. Although extremely reliable, both flash and nonvolatile memory can occasionally become corrupted. This can 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, appropriately ensuring that the security of the wider system is not breached.

Corrupted Memory Can Lead to Unexpected Outcomes

Reliability is also a concern on the communications microcontroller. Although extremely reliable, both flash and nonvolatile memory can occasionally become corrupted. This can 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, appropriately ensuring that the security of the wider system is not breached.

Corrupted Memory Can Lead to Unexpected Outcomes

Reliability is also a concern on the communications microcontroller. Although extremely reliable, both flash and nonvolatile memory can occasionally become corrupted. This can 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, appropriately ensuring that the security of the wider system is not breached.
The ADuCM3029 is designed with flash and ECC parity checks to ensure errors due to memory corruption are identified and corrected where possible. The ADuCM3029 is also equipped with battery monitoring capability in sleep mode. This ensures that unexpected drops in voltage can be detected and the processor alerted to a possible malicious threat or power supply malfunction. The end device can then take appropriate action by either 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 is a fundamental requirement to fulfill the true potential of the IoT.

About the Author

Michael Dalton is a product marketing manager in the IoT Group at Analog Devices. Previously, Michael worked for five years in the RF Applications team supporting ADI’s ultralow power RF transceivers. He graduated from University College Dublin with a B.E in electronic engineering in 2007.

Online 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