Precision Counts in IoT

Grainne Murphy and Colm Prendergast
Analog Devices, Inc.

The Internet of Things (IoT) is simply the concept of connecting any device with a sensor or controller to the internet (and/or connecting devices to each other). This includes everything from cell phones, appliances, cars, machines, components of machines, wearable devices, and anything else you can think of. But the principle of IoT is that it is simply a measurement signal chain that connects and extends to the cloud.

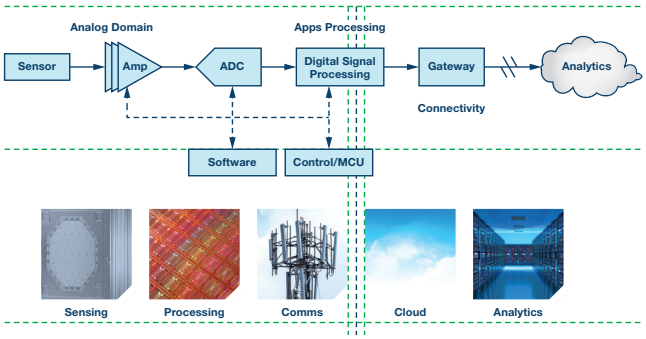

Figure 1. Sensor-to-cloud signal chain.

The sensing/measuring piece transforms an analog signal into a digital data stream. This digital format can then be taken, processed, transferred, analyzed, and then decisions can be made based on the outcome. The concept of transferring physical phenomena such as light, sound, pressure, and temperature into digital data is old. The evolution of IoT has transformed the decisions made based on this digital data by using metapatterns and the power of computation modeling that is enabled by the cloud and its massive storage and processing capabilities. Some traditional sensing capabilities like temperature measurement techniques are well understood and used as both a standalone measurement and a factor for other sensing. For example, in electrochemical sensing, temperature affects measurement and needs to be accounted for. Alternatively, there are also newer exciting sensor developments that can make a huge impact on the world of IoT.

One example of this is the MEMS accelerometer. These sensors form the basis for vibration detection over multiple axes and allow stabilization in systems such as drones, portable gaming devices, or cameras. Vibration is also used in health tracking devices to measure personal health. Health and fitness wearable sensors need to be permanently on, providing high accuracy body movement detection that can be analyzed accordingly—for example running, cycling, or walking—and deliver real-time data to a wide variety of portable health and fitness applications.

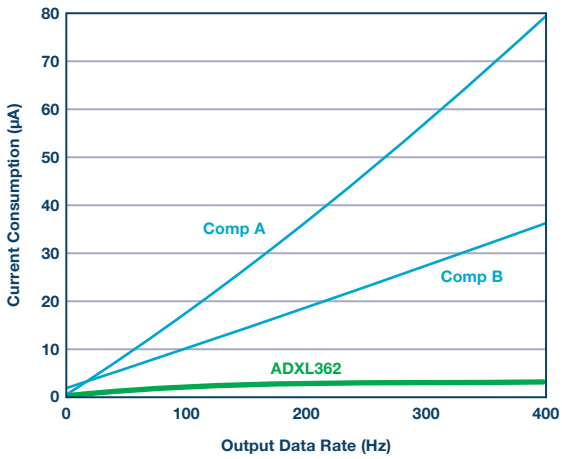

Figure 2. Industry's lowest power MEMS accelerometer.

Using an accelerometer as an example, what should you look for in an IoT device and what is the value of a more accurate measurement? Firstly, consider low power. The ADXL362 from Analog Devices is an ultralow power, 3-axis MEMS accelerometer that consumes less than 2 µA at a 100 Hz output data rate and 270 nA when in motion triggered wake-up mode (a MEMS accelerometer measures the static or dynamic force of acceleration). This allows for long battery life. Secondly, take into account bandwidth and resolution. The ADXL362 does not alias input signals by undersampling; it samples the full bandwidth of the sensor at all data rates and has low noise. This enables the smallest signals to be measured. For applications where a noise level lower than the normal 550 µg/Hz of the ADXL362 is desired, either of two lower noise modes (down to 175 µg/Hz typ) can be selected at minimal increase in supply current.

Better Quality Data Counts:

But what is the value of this precision measurement and why does it matter? Low noise, low drift components maximize sensor capability, enabling a wider dynamic range, which means that a greater variety of smaller signals can be measured by the hardware. This enables a more accurate, sensitive, and differentiated end system. This higher accuracy allows the development of platform hardware that can meet both present and yet to be defined measurement needs and guard banding for the future.

Therefore, the same hardware can be used for multiple generations of product with the associated benefit of lower cost of ownership, particularly as hardware replacement can be difficult and expensive. This is particularly true for IoT as the number of sensors and, therefore, associated hardware is forecast to explode in number. The analyst firm Gartner says that by 2020 there will be over 26 billion connected devices—that's a lot of connections. Additionally, due the benefit of wireless connectivity, as utilized through the IoT signal chain, units will be located in increasingly hard to reach or harsh environments like a factory. Finally, another factor to consider can be the increasingly stringent government regulations across multiple markets including gas emissions, power usage, and environmental control. A better measurement system provides the forward thinking to meet these possible new and changing regulations that will require more precise measurements within existing hardware. Being able to meet new future measurement needs could prove the difference in surviving in what is sure to be a crowded and competitive IoT market.

Therefore, the importance of a stable and precise hardware measurement platform cannot be overstated. Once this platform is set, system differentiation can then be achieved through software. In IoT, these capabilities are proving to be an area where companies can increasingly distinguish themselves within this competitive market. Additionally any system upgrade is easier, simpler, and can be done in real time.

Legitimate Data Really Counts

There are many factors to consider to ensure legitimate data is maintained within an IoT ecosystem. The Internet of Things can be explained as a number of layers, from the "Thing" all the way to the cloud. At each layer there can be a new external connection and its associated security risk. There is also a possible return path back through the layers to the "Thing." It's not just about the device, the network, or the clients—there are many surface areas involved and each could be interconnected. For example, from the device to cloud or from the device to gateway to cloud. The aim for legitimacy is to ensure security at every layer. As we connect more things, clouds, and gateways, we increase the amount of places that are vulnerable to security flaws.

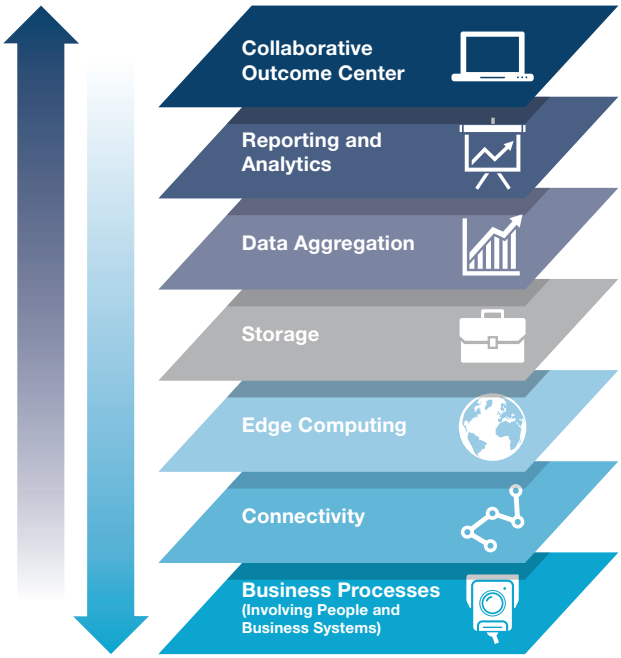

Figure 3.

The OWASP (Open Web Application Security Project) identifies the top 10 IoT securities vulnerabilities as:

- Insecure web interface (XSS, injection, phishing)
- Insufficient authentication/authorization
- Insecure network services (SSH, SFTP, Telnet)
- Lack of transport encryption
- Privacy issues/concerns
- Insecure cloud interface
- Insecure mobile interface
- Insufficient security configurability
- Insecure software/firmware
- Poor physical security

In the cloud, a security threat can manifest as a data breach but also as an accidental data loss or data theft. There is no doubt that cloud services will host multiple customers (multitenant), so the service needs to ensure secure segmentation from one customer to the next. Then there are additional questions to consider. What is the availability capabilities of the system, either to stay online locally or in cases of a possible data outrage? How is data shared and secured across multiple locations and what security standards are in place? Can you backup your data, especially as the volume of data explodes due to IoT? Application program interfaces (APIs) will be developed and stored for multiple customers via the same cloud service Therefore, how authentication and authorization are performed (as well as how to protect a privileged user such as an administrator) is vital.

There are many ways to review and evaluate a cloud service provider. One mechanism is via published security guidelines. These global cloud guidelines continue to be enhanced and service providers will increasingly be required to be certified to meet them.

But security concerns are not limited to the cloud. At each level of the stack there are associated threats and techniques to countermeasure. Physical IoT devices and gateways could be stolen or tampered with and the data could be manipulated or accessed by unauthorized users. Here tamper detectors, cryptography, or device registration are used as countermeasures. Software or firmware can be targets of phishing, malware attacks, or manipulation. This is where trusted operating systems, building security into the development lifecycle, and vulnerability testing is vital. It is also important to have a mechanism to securely update software after it is deployed to the field. As the data is transported, insecure channels could allow manipulation, eavesdropping, or attacks. Here encrypted transport channels, port/interface management, and continuous proactive monitoring are key. For data privacy, customer confidence needs to be especially high. A company's brand and reputation can be damaged as a result of even the smallest breach. Therefore, good practices such as data encryption techniques to minimize or obfuscate the stored data and data retention are important. Global privacy data policies continue to evolve and change. Having a flexible system to handle the regulation differences based on the different regions of the world, along with consent, are important. At the application level, it is not just about user authentication and authorization to stop unauthorized access, but to continuously test code for vulnerabilities. Also consider out of band protections such as WAF (web application firewalls) and the ability to isolate and lockout an account under attack. All of the countermeasures described today can be applied but security must be designed into the ecosystem and not retrofitted at the end.

An Intelligent Connected IoT System

Intelligence (or data processing) can be added at any stage along the IoT chain. For example, in vital signs monitoring (VSM), there is no need to send data on body temperature just to the cloud, when an immediate alert that body temperature is at a dangerous level can happen directly at the sensor. However, the same temperature may also be used in other biomedical data computations so it could also be used at the gateway or in the cloud as well.

When signal processing happens at a node, it has several advantages including enabling tight, integrated feedback control loops. The benefit of being tightly coupled to the sensor and/or actuator allows for immediate decisions to be made. For example, a vibration reaching a predetermined level enables an immediate power-down of a machine or motor or a rise in temperature in a greenhouse can actuate a motor to open a window. While the requirements at the node need to have both a small footprint and the lowest power consumption for a potential long battery life, components such as integrated analog microcontrollers like the ADuCM360 from Analog Devices, which combines an ARM® M3-MCU and 24-bit analog-to-digital converters, can realize these needs. In the future, energy independent devices that can use harvested energy will be key to success here. The limitations of node processing are in the very same space and power limitations. Additionally it is difficult to aggregate data from other sources. Low power at the node limits data transmission ranges and payloads. With difficult node management to monitor status and perform upgrades, there are associated network edge physical, software, and data security risks.

Gateway-based signal processing uses an IoT gateway device that has a short-range wireless sensor network (WSN) link on one side and a LAN or WAN link on the other. It is similar to a router and can also be a sensor hub. In addition to WSN network management and security functions, it is often used as a compute resource for local processing and analytics (which is commonly known as edge computing). The advantages of gateway-based processing are that potentially large processing resources are available with the ability to aggregate data from other sensors/sources. So combining the ability to run analytics close to the network edge with the development of these analytics by using off the shelf development tools make for a more IT friendly solution. It has the potential of being full stack OS capable and uses LAN/WAN network technologies with standard remote management tools with better security (although physical security can be a risk). Conversely, it is not typically low power, requiring a source of wired power and it has limited data storage.

So one of the key benefits of cloud connectivity is the ability to store, retrieve, and search large data records with historical data and/or data from across many devices. For cloud-based signal processing in many cases, data storage is closely coupled to big data processing and analytics. It is not just enough to store data. The need to be able to access and process data quickly has led to innovation resulting in many new methods to allow for the distributed processing of large data sets across clusters of computers using simple programming models with open-source framework. The obvious advantages of cloud-based processing are the potentially very large compute and storage resources with built-in security. There are a large and growing variety of open-source and commercial development tools and end solutions can be easily scaled.

Software as a service (SaaS) is now considered as a key offering within cloud computing, along with infrastructure as a service (IaaS), platform as a service (PaaS), desktop as a service (DaaS), mobile back end as a service (BaaS), and information technology management as a service (ITMaaS). Together these provide a range of options to suit end system needs. For cloud-based processing, server hosting is required (which can be on premises or remote). There is an associated cost for storage and services that can be expensive for communications and large data storage. Other disadvantages include internet communications channels, which can be unpredictable in terms of latency and throughput.

As IoT systems evolve, so too will smart system partitioning, to move more intelligence at the node. To never generate wisdom and knowledge at the node means that data stays data until it reaches the cloud, which is both power hungry and bandwidth intensive to convert and send all data. Intelligent smart sensing is where a node turns data into information which lowers overall power consumption, lowers latency, and reduces bandwidth waste. Simply put this enables the move from reactive IoT to predictive and real-time IoT.

The challenges of excellent IoT design are countless, including good measurement, security, and knowing where to use intelligence effectively across the full IoT path. Additionally there are may be multiple vendors across a full IoT solution from sensors, gateways, software, and storage providers. Here at ADI we are both IoT vendor and customer using our own ADXL362 accelerometer (among other sensors measuring temperature and humidity) to monitor fabrication equipment at our Limerick facility. By measuring the change in vibration patterns from a machine or motor, a fault can be detected before a system goes down. This has the benefit of allowing a predictive maintenance program, thereby increasing factory efficiency and capacity. ADI's IoT implementation provides a full monitoring and analytics system across multiple pieces of equipment (old and new and from many suppliers) within a complex manufacturing process. The system tracks and reports efficiencies in real time, alerting technicians to a possible problem before a system goes down. This has increased the wafer yield, which in turn has helped our customers plan better due to a more regular supply for their end requirements. This example demonstrates the real value of an IoT system. The sophistication and scope of IoT systems allow many options for signal processing. Moving processing in IoT systems from the cloud to the edge enables smarter sensors and information extraction closer to the source. Usable processing resources at network edge nodes, gateways, and in the cloud allow system designers the ability to optimize solutions trading of edge node power, data bandwidth, computation, and storage requirements.

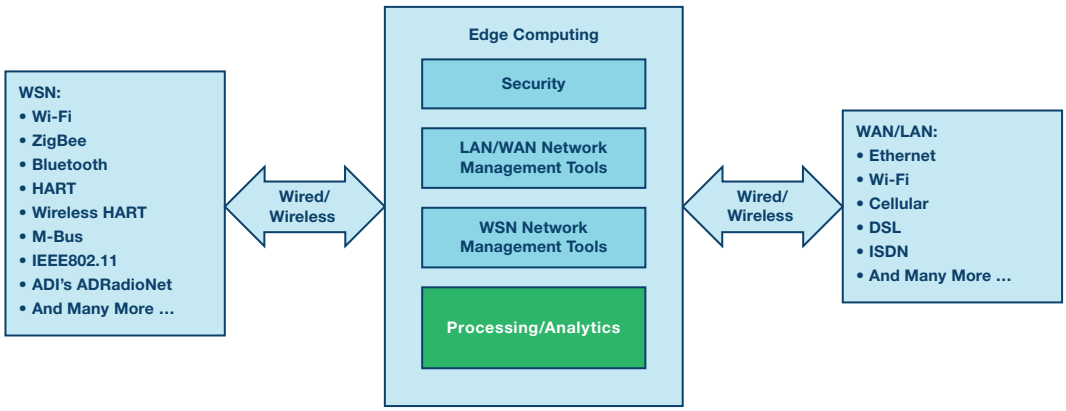

Figure 4. An example of an IoT gateway.

About the Authors

Grainne Murphy is the IoT market manager at Analog Devices. She holds a B.Eng. from University of Limerick and an M.B.A. from Oxford Brooks University.

Colm Prendergast is a principal engineer and director of IoT cloud technology at Analog Devices. Colm joined Analog Devices in 1989 as a design engineer in Limerick, Ireland. During his career at ADI Colm has worked on and led projects in a wide variety of applications areas, including digital video, audio, communications, DSP, and MEMS. Colm holds 11 U.S. patents and is a member of IEEE and SIGGRAPH. Colm sits on the Board of Trustees of the St. Joseph Preparatory High School in Brighton, MA, and is a FIRST robotics mentor. He received a bachelor's degree in electronics engineering from University of Limerick, Ireland, and a master's degree from University College Cork, Ireland.

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

TA14507-0-8/16

analog.com

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™