Making the IoT smarter, safer

Many of the things we interact with have intelligence, but still don't have a way to communicate with us, says **Kristopher Ardis**

There is no slowing down the pace of innovation. Did anyone imagine 10 years ago that voice-controlled portable speakers would turn house lights on and off, buy things online, or answer random questions? Or that televisions, kitchen appliances, and even cars would be able to function somewhat autonomously?

When something that has valuable data is enabled by technology, we should still be able to interact with it in the usual ways – we should not notice much fundamental difference between the smart device and its 'dumb' counterpart.

For example, consider a thermostat. A smart version would still require us to set the dial, but because of its intelligence, it would gradually learn our temperature preferences and react accordingly.

The decision to unleash the invisible intelligence around us requires us to address a few important questions. First, can we provide and manage the processing capability to produce smart devices that deliver true value? Second, how can we efficiently power all of our connected devices? And third, can we design devices that people will trust enough to use them?

A closer look can reveal how industry's responses to each of these areas will shape the future of the internet of things (IoT).

The right amount of intelligence

Making sure that IoT devices have the right amount of intelligence calls for consideration of three principles of invisible intelligence.

The first is to think about how we interact with smart devices. We won't want to upgrade connected devices every few years as we do with smartphones. Devices will need to be upgraded easily, even invisibly, over time, and they will need to be able to accommodate the updated firmware.

Second, the appearance of the device should strike a balance between sophistication and advanced without being too intimidating.

And finally, the device should be designed with the right amount of processing power and memory – enough to extract value from the data in the device and to accommodate future features, but not so much that device cost increases.

IoT devices need to be able to run multiple algorithms, which means that the processor needs to be able to perform signal processing and lots of computations and have a lot of intermediate storage.

Simple smoke detectors typically use 8-bit microcontrollers with a few kilobytes of code memory. A smart, connected version would require that 8-bit microcontroller to execute more instructions and, thus, use more power to perform its operations than a 32-bit microcontroller.

Alternatively, the smart smoke detector designed with a 32-bit microcontroller is a better choice for the intelligent version, since it also would need to run a network stack, an operating system to manage core resources like processor bandwidth and memory allocation, and security for the data and commands.

Smart thermostats follow the principles of invisible intelligence: interaction, appearance, and processing power (plus memory)

Choosing the right processor for an IoT design requires careful consideration of performance power, signal processing and floating-point acceleration, memory capacity, memory expandability and security capabilities. A low-power microcontroller would provide the processing horsepower for many IoT designs.

IoT power demands

In addition to delivering the processing capacity, low-power microcontrollers would also efficiently power connected devices. Powering the invisible intelligence around us does, however, require overcoming some tough challenges.

From the interaction and appearance perspectives, a good user experience calls for devices that are untethered to a power source and for long-lasting batteries and other energy-harvesting solutions that are not too big or bulky. Also, to ensure that the IoT device delivers a good return on investment, the cost of the power delivery mechanism should be low.

Fitness watches are a good example of a connected device that adheres to the three principles. They provide valuable data in a format that looks and behaves like a conventional watch. They are also evolving, integrating more sensors to track more parameters and delivering the insights in more graphical ways. This also presents one of the power challenges – more sensors, connectivity, and algorithms require more power.

How can we enable these applications to manage their power budgets while providing more data and extending the life of the device?

Most embedded applications will need multiple ICs, each potentially requiring different voltage supplies as well as multiple supply rails. It does not make sense to have one battery for each supply rail; it will have to be established how to use a single battery with a single voltage to support all of the supply rails.

It will be necessary to address methods of determining battery characteristics like voltage drops over the battery's lifetime. Linear regulators and switched-mode power supplies are options, but they do come with trade-offs.

There are also many characteristics to consider in the low-power microcontroller itself.

Low-power sleep mode is a key consideration, especially when it comes to influencing the longevity of an application. Many chips support multiple low-power sleep modes. When using these modes it is beneficial to have SRAM retention, to preserve important data like datalogs and operating system state.

Another useful capability is fast wake-up times to minimise wasted power when transitioning between low-power and active modes. Finally,

A hacked road sign can be both humorous and a source of risk


The capabilities of fitness watches have typically overpriced the product for its market

a simple state machine can perform routine tasks while the microcontroller is asleep.

Trust in the IoT

Considering all of the sensitive data managed by IoT devices, protecting these products against hacking, cloning, unauthorised reuse, and other breaches is critical in encouraging wide adoption. Yet, adoption of security technologies has been slow. "It's too expensive", "it's complicated", and "I'll deal with it later", are common reasons for the delays.

So what if we didn't focus on the negative angle of security? What if we considered security to be an enabler of new business models, innovative applications, and also of invisibly intelligent products becoming trusted parts of a new economy based on data?

The burden of managing security should not fall to the consumer. Relying on consumers to change default passwords is not a fail-safe method.

Regarding appearance, integrating security technology into a product should not change that product's fundamental appearance, nor compromise the IP inside.

Finally, there's the essential matter of securing the connected device's valuable data. We all need to trust the data we will use to make decisions.

Security as an enabler

What if security technology could help you to reduce your manufacturing costs? Microcontrollers with secure bootload capabilities can enable companies to manufacture at the most cost-effective, efficient locations available. Since the secure bootloader can be customised, companies can send encrypted firmware, which cannot be copied or reverse-engineered, to the manufacturer. Unique ID numbers in the secure microcontrollers could ensure that only the intended number of devices are manufactured.

Another example is customers upgrading a product in the field. They would pay a fee to enable advanced features, and the integrated security technology would allow the company to ensure that the upgrade is activated only once the fee has been paid.

Key techniques to secure an IoT design involve authenticity, confidentiality, and integrity: authenticity proves that a message or command comes from a trusted source, and confidentiality protects data from unauthorised access, while integrity refers to the fact that the data is well formed and has not been altered since it was sent. Cryptographic tools such as encryption, hashing, and signatures can be used to apply these security techniques.

While these algorithms can be implemented in software, hardware implementations have a number of advantages. They consume less code and data space, they execute faster, usually by an order of magnitude, they consume less power and they are better at resisting common timing and power-analysis attacks.

There is a variety of embedded security ICs on the market, including secure authenticators with physically unclonable function (PUF) technology, cryptographic coprocessors, and secure microcontrollers. These ICs provide robust, cost-effective ways to implement security, even for designers without a background in cryptography.

If the IoT is to thrive connected products will have to be built with sufficient intelligence, power, and security to meet all these challenges. Only then will we be able to unleash the invisible intelligence around us. ❑

About the author

Kristopher Ardis is executive director of the micros, security and software business unit at Maxim Integrated Products

WINMATE

Rugged Computing Tough Conditions

Industrial PDA & Rugged Tablets

Vehicle Mount Computers

Panel Computers & Embedded Systems

Winmate is a world-class manufacture of industrial grade, rugged tablets and computers

Winmate, Inc.
+886-2-8511-0288
sales@winmate.com.tw
www.winmate.com

Learn more