Silicon, Security, and the Internet of Things

White Paper

maxim integrated™

Keywords: security, smart grid, Internet of Things (IoT)

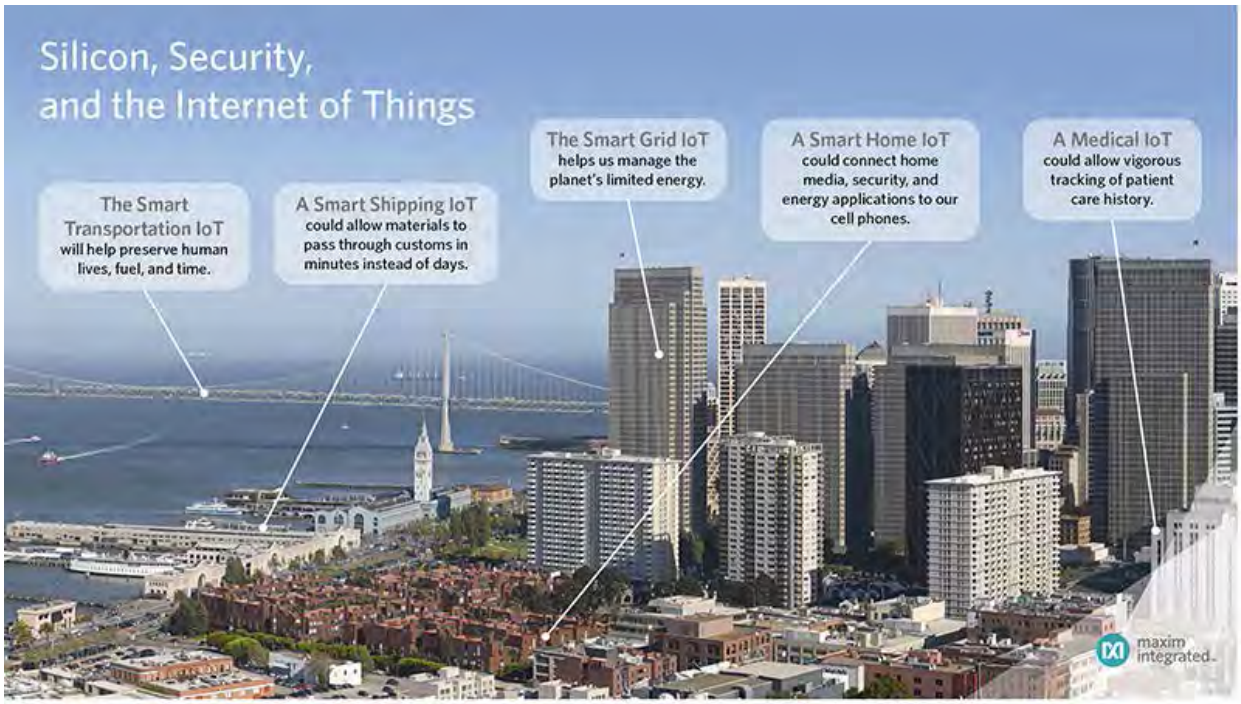
Silicon, Security, and the Internet of Things

By: Kris Ardis, Director of Energy Solutions
Feb 01, 2014

Abstract: The smart grid has broken from the fantasies of the Internet of Things (IoT) to provide something useful. In this article we discuss why the smart grid does not follow the pervasive IoT fantasy projections. We will show how real IoT deployments are made to better manage valuable resources and how an IoT creates a critical need for security.

A similar version of this article appears on *Smart Grid News* November 26, 2013.

A Google search on the Internet of Things (IoT) suggests that a multitude of smart devices will soon be talking to each other and deciding how the world operates without our (human) intervention. Fantasy stories on the Internet want us to believe that every atom on earth could be chattering away on a network someday. This sounds futuristic and completely detached from reality, but the IoT is already here, in the form of the smart grid.



To realize the true potential of IoT deployments, security needs to be designed into the web of sensors that will monitor and control the planet's resources.

IoT—Fantasy and Reality

The fantasy of the IoT is quite grand: everything on the planet can be smart and communicate. The idea is both powerful and impractical. What if every moving part in your car could monitor itself and offer you truly predictive maintenance? That is a powerful vision. What if

every brick in my house could communicate its location to my cell phone? It would certainly tell me whether bricks had fallen off the house, but is this a practical use of technology?

The fantasy of IoT tells us that millions of "intelligent" devices should be connected and talking, controlling the world around us. Yes, the falling brick could call the local mason for repair and tell the HVAC to turn up the heat. But this IoT application is not likely to be implemented in our lifetime. Why?

The IoT is only enabled because of two things: the ability of networks to reach countless nodes, and the availability of cost-effective embedded processors to attach to a multitude of devices. Let's talk about both.

The first IoT enabler is today's multitude of network technologies. Wireless technologies such as ZigBee or Bluetooth® LE allow remote sensors to join a network and provide further information about the state of the world. With IPv6 as the backbone, there are enough unique addresses (theoretically, there are 340 trillion trillion trillion) for everything on earth to have a unique address. Each person on earth could have zillions of sensors with unique addresses, and we would not exhaust our address space.

The second enabling technology for the IoT is increasingly capable silicon. But we need to face reality: this silicon has a cost. A device participating in the IoT needs to have a measurement component to interact with the real world and a communication component to share its information. Let's consider the smart grid. To truly realize its full promise, grid sensors should make decisions based on collected data or take action based on a decision from the cloud. This much intelligence in distributed nodes comes with a cost.

The intersection of IoT fantasy and reality lies in a return on investment (ROI). We have the technology to make a truly smart world, but what actually makes financial sense to do? Who will pay for the smart brick? A completely smart world—a fully populated IoT—will not happen in our lifetime. Instead, the IoT will be rolled out one bit at a time, in specific applications where the costly additional technology improves our world in a *financially* rewarding way.

The First Tangible IoT: the Smart Grid

The smart grid provides the strongest example of a current IoT deployment. It uses advanced sensors and gives us better information for controlling our energy world. It also illustrates the challenges and dangers inherent in an IoT.

The story starts with smart meters. For the last several years, U.S. electric utilities have installed solid-state electricity meters that can report data on consumption at nearly real time. Many other countries are deploying smart-meter technologies as well. Smart meters allow consumers to access their consumption data so they can better manage their electricity usage.

For utilities, the ROI on smart meters is difficult to calculate, but some benefits are clear and tangible: lower cost of data collection, since meters report their data automatically; quicker reaction to outages, leading to less lost-revenue downtime; better monitoring of electricity theft; and better ability to link the actual costs of generation with consumption through time-of-use pricing.

The smart grid promises to go far beyond the benefits that smart meters provide. The smart grid also encompasses technologies that monitor transmission lines; manage substations; integrate microgeneration (such as solar or wind) on the grid; and utilize large-scale batteries. These technologies will allow utilities to identify outage problems quicker, delay capital expenses associated with new power plants, and better manage the power before it is even delivered to the customer. The utilities' ROI in these activities tends to be obvious: more uptime, less capital expenses, and better efficiency. The ROI in solar, wind, and storage technologies is not always as obvious for utilities, but there is mounting political pressure (and regulations) to integrate these technologies. Utilities have little choice but to invest.

The smart grid is an IoT network of embedded machines that sense and control the behavior of the energized world. It leads to more efficient use of resources based largely on machine-to-machine interactions.

Learning from the Smart Grid IoT

There are lessons to learn from ongoing deployments of the smart grid. An IoT will not be implemented without an acceptable ROI. IoTs will roll out sporadically and should anticipate flexibility for future applications. There is also an important lesson that is not about efficiency or finances: without adequate security, an IoT could become a technological disaster affecting everyone.

Critical Role of Security

We are well on our way to a smarter grid. About half of the houses in the U.S. already have advanced, communicating electricity meters. Utilities worldwide are installing distribution automation equipment that controls power delivery. Water and gas utilities are beginning to investigate similar technologies. Despite the momentum and progress of this market, there are fundamental gaps in the security of the deployments.

The smart grid provides an incredibly lucrative target for attack. If unfriendly organizations could control some portion of the smart grid, they could cause catastrophic damage. By controlling a utility's communication network, they could mount attacks like a massive underreporting of electricity consumption or falsifying sensor data to induce a power shutdown.

Security is a hot topic today for the smart grid, and there has been some progress. Most communications now use standard cryptographic algorithms such as AES-128 to protect the data and commands on the utility network. However, there is an alarming lack of standards to address the protection of the secret keys or the life cycle of embedded smart grid devices. This is a dangerous situation. The cryptographic algorithms are a good first step to ensure secure communications networks, but the lack of key and life-cycle security mean that alternate attack points are likely. An attacker might try to get communication keys by physically inspecting a smart meter.

Securing the IoT

Ultimately, the smart grid should teach us that security must be designed in from the start of any IoT deployment. Let's look at the characteristics of an IoT and why it demands built-in security,

- A multitude of remote, distributed sensors and control devices are deployed where they will not be supervised. Unlike an ATM with a security camera nearby, there is no oversight on a smart meter. This makes it easy for an attacker to acquire devices for study.
- An IoT is likely to be deployed to help manage the health and safety of an important asset more efficiently. For example, a network of health sensors might monitor human lives and better control health-care costs. A network of automated vehicles could create safer and more energy-efficient transportation. These cases impact human health, associated medical costs, transportation safety, and energy efficiency. Such valuable targets increase the likelihood that attackers will try to exploit that IoT.
- There are risks with machine-to-machine communication. When devices are communicating with each other with little human interaction, tampering may be difficult to detect until something catastrophic happens.[1]

Just as silicon is one of the agents empowering the IoT, it is also a key factor in securing the IoT. Silicon integrating proven algorithms such as AES and elliptic curve cryptography provide toolboxes for designers to build secure applications. More advanced silicon like the MAXQ1050 and MAX32590 secure microcontrollers also have both secure bootloaders to protect the entire life cycle of products and physical attack detection to determine when someone is trying to pry secrets from a product. The silicon is available to secure the IoT, and it remains for product designers to secure future IoT deployments.

The Future of the IoT

The next question is not, "when will the IoT get here?" The smart grid IoT is already with us. Instead, the question should be, "what is the next IoT and how will it benefit people?" Security lies at the heart of an IoT and if an IoT can be adequately protected, the rewards to society could be dramatic.

Let's look at one of the next potential IoTs: smart transportation. Recall again the smart, connected car described at the outset. In its infancy, the idea of a smart car might be limited to delivering media content to vehicles on demand, and perhaps automatically requesting roadside assistance with specifics about a breakdown. But the promise of smart transportation has far more potential. Can we build a sensor grid and vehicles that talk to each other? Then with enough data cars can drive themselves, thereby improving safety. Furthermore, can these cars practice techniques like drafting at high speeds to drastically improve fuel efficiency? Can a sensor network with smart vehicles automatically direct traffic to the most effective route for fuel and time efficiency? We see news daily about autonomous vehicles that are approaching this goal, and the benefits would definitely help preserve precious resources: human lives, fuel, and time.

No one could argue against improving our management of those resources. But to get there, this Internet of Automobiles must be secure. An untrusted smart transportation system would be an unused transportation system! The good news is that the technology to secure both the smart grid and the Internet of Automobiles exists. Now it is up to the visionaries for the next IoT to embrace that technology and make sure that our future is secure.

References

[1]Recall the Stuxnet attack in 2011. Tampered control systems were operating centrifuges slightly out of allowable parameters, but reporting that all was well. Eventually, the centrifuges were damaged and the nuclear processing capability of an entire plant was destroyed. In this case a tampered machine reported that everything was fine to another machine that did not have any other means of validating centrifuge status. No problem was reported until the centrifuges became physically damaged. See Maxim Integrated application note 5445, "Stuxnet and Other Things that Go Bump in the Night."

The Bluetooth word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Maxim is under license.

Related Parts		
71M6542FT	Energy Meter ICs	Free Samples
MAX32590	DeepCover Secure Microcontroller with ARM926EJ-S Processor Core	Free Samples
MAXQ1050	DeepCover Secure Microcontroller with USB and Hardware Cryptography	

More Information
For Technical Support: http://www.maximintegrated.com/support
For Samples: http://www.maximintegrated.com/samples
Other Questions and Comments: http://www.maximintegrated.com/contact