Building a secure Internet of Things

Enabling innovation while providing safety and reliability

Steve Hanna
Senior Principal Technical Marketing

www.infineon.com/IoT-Security

Abstract

The emerging Internet of Things (IoT) presents tremendous opportunities for innovative companies to deliver products and services to make industry more efficient, transportation safer and the everyday lives of people more convenient and fulfilling. But with great good there also can be great risk. Remote, intelligent monitoring and control for factories, homes, cities, and cars can increase efficiency and convenience. However, these same powerful tools can be misused by bad actors to disrupt critical infrastructure with dangerous and expensive results. At a personal level, the IoT potentially exposes our homes and personal information to malicious or criminal acts.

Fortunately, security techniques developed over the last few decades for other areas can be applied to the IoT. These techniques have a proven track record of providing effective, cost-efficient protection while enabling continuing innovation.

Many developers working in the IoT field are not security experts. They are experts in manufacturing, cars, home appliances, or other domains. These developers need to include security in their products but this security must also meet their domain requirements. That is why experts in security solutions such as Infineon are engaging with the many domains affected by the IoT to ensure that strong and appropriate security is built in from the start. Building in security will protect the values of Safety, Reliability, and Privacy that we all care about.

Contents

1. Motivation	4
2. Benefits of IoT	5
3. Risks of IoT	6
4. Managing and reducing risks	8
5. Best practices for IoT security	10
6. References	13

1. Motivation

The Internet of Things (IoT) may be the most important technology trend of the 21st century. By connecting billions of electronic sensors and control elements to each other and to interconnected networks, the IoT will contribute to increased efficiency, greater convenience and improved lifestyles for every citizen of the world. The impact will be seen from factory floors to office buildings and retail stores, mass transport systems to connected cars, and in our own homes.

As with past advances in technology, the IoT also has a dangerous side. Here is one possible scenario from the near future.

Maria Solano* was not having a great day. Unusually heavy commute traffic made her 15 minutes late to work. A news report she heard during morning break explained that the regional traffic coordination system experienced a computer crash that disabled traffic signal synchronization. During lunch, she was frustrated to be unable to log-in to her Internet-linked home video monitor to check on the doings of the twins. She called the nanny, who told her she had heard strange voices on the monitor and decided it was best to turn it off. She quickly called her husband (the family's informal IT specialist) to ask what could have gone wrong.

Then things got worse at the plant. An automated paint line on the shop floor began to randomly start/stop sprayers, causing an expensive line stop. Maria spent the afternoon working with her production manager and IT supervisor to track down what turned out to be planted malware. No one was sure, but it appeared that someone with knowledge of the network had altered production line control commands.

While driving home that evening (fortunately, with no flaws in the signal system) the evening news broadcast reported that the earlier traffic system crash had actually been a prank, which was discovered when one of the teenagers involved had gotten nervous and called it in to the local police. When she got home, her husband was busy boxing up the video baby monitor. He'd learned that an unreported back door in the monitor had been hacked and that the instructions for how to break-in to the connection were freely available on the Internet. While Marie's husband was confident they could find a more secure replacement, he was going to do a little more homework first.

Could this really happen? On the following pages of this paper we will see how everything described in this short scenario has already occurred. We will also see that industry has the ability to manage and minimize such risks using proven approaches used today to protect other technologically advanced systems.

This White Paper outlines techniques that can be used to build trust into devices and systems. It addresses the requirements and available technologies to protect the physical infrastructure of the IoT; the devices (or things), servers that both store information and manage applications, and the network that ties systems together. In turn, this secured physical infrastructure will allow the successful implementation of policies to protect personal privacy and the data that is collected and used by the IoT.

* fictional person

2. Benefits of IoT

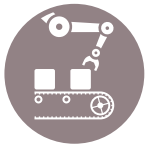
What is the Internet of Things? Simply put – the combination of connected things and intelligent services. Everything from cars to clothes to factory machines is being networked. The number of connected devices is projected to grow at a rate of 15-20% per year for the next five years [1] with incremental annual revenue in the trillions of U.S. dollars and almost no market left untouched. [2]

The benefits are tremendous, but not without risk. Remote, intelligent monitoring and control for factories, homes, cities, and transport can increase efficiency and safety. Yet these powerful tools can be misused by bad actors to disrupt either critical public infrastructure or personal and private systems, with dangerous and expensive results.

Let's first look at the benefits of the IoT. Real world deployments in the last few years have shown significant savings and exciting opportunities to further improve economic performance while making daily life more convenient and safer.

› Smart Cities: The city of Los Angeles' replacement of municipal street lighting with LED lamps led to annual savings of $8 million in electricity costs (60% reduction in energy use). Now, wireless connectivity to a network control center is expected to lead to further savings in maintenance while creating a dynamic system that improves safety. [3,4]

› Smart Buildings: In New York, smart building technology is helping a real estate firm save approximately $1 million in operating costs in a single office building. [5] This savings will add up quickly; the City of New York estimates that as much as 75% of energy related emissions in the city can be better managed through use of such smart building technology. Additionally, it was reported that the firm is working with technology providers to mirror these savings in smaller buildings it owns and ultimately find ways to make the technology available even to residential homes.



› Smart Factories: A project at one Intel chip manufacturing plant reduced costs to test a single product line by $3 million annually. The pilot system analyzed information from machines, sensors and factory staff to help the company improve the real-time control of manufacturing processes. Across all chips produced in the factory, the manufacturer estimates annual cost savings of $30 million. Similar IoT and big data analytics systems can be implemented in many other complex manufacturing processes. [6]

› Smart Homes: Smart home devices, which today represent about 25% of IoT devices, will see sales increase from $61 billion in 2015 to $490 billion in 2019, with home automation and security applications leading the way. The impact is difficult to measure at this early stage, though a recent report highlighted particular value for senior citizens and persons with disabilities. [7]

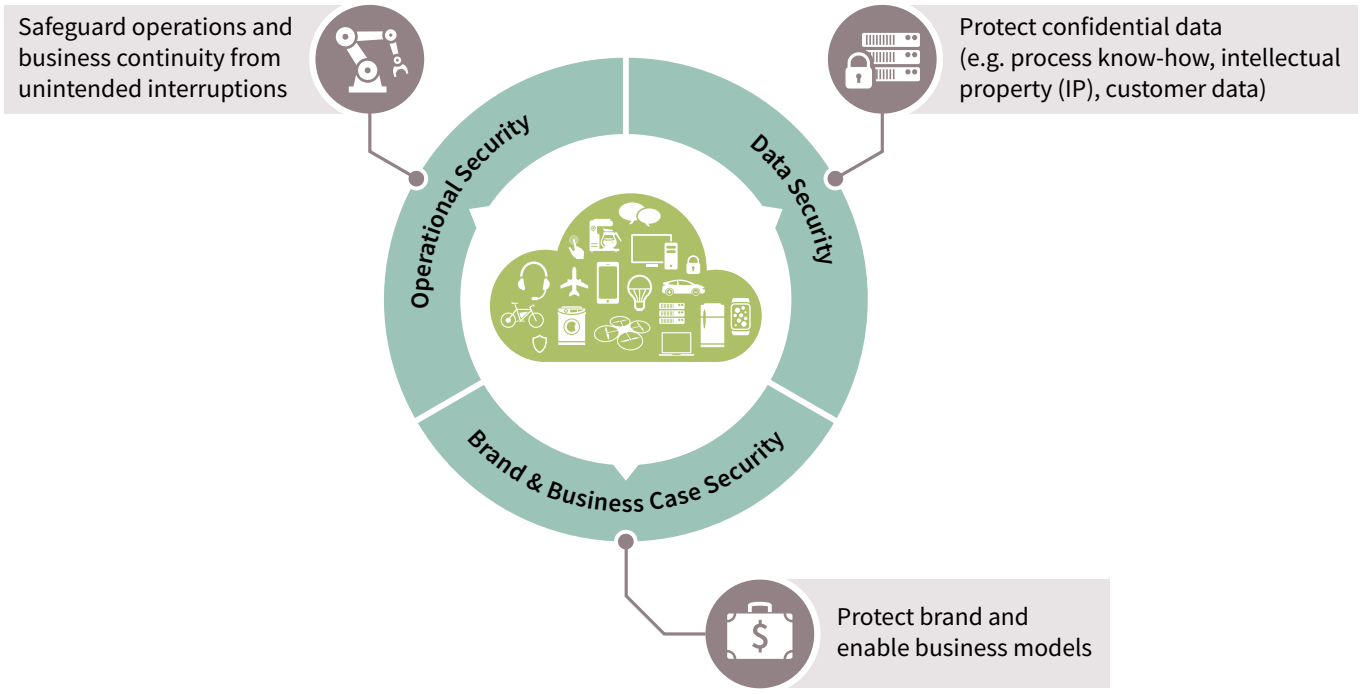
› Connected Cars: The most dramatic example of how the IoT can impact personal safety has been in the area of Connected Car technology. One report includes an estimate that if 90% of all vehicles in the US were fully autonomous (self-driving), "as many as 4.2 million accidents could be avoided each year, saving 21,700 lives and $450 billion in related costs." [8] It is believed that improved safety, as well as improvements in personal productivity and reduced stress from the transition to autonomous vehicles outweighs the risk of the successful attacks on connected cars recently demonstrated by several well-intentioned ("white hat") researchers.

Infineon agrees that the already realized and potential future benefits across all economic sectors and in each of our daily lives make the move to a smart, interconnected world inevitable. It is vital, however, that industry and policy makers recognize and address the security risks of the IoT.

3. Risks of IoT

The risks of IoT mirror those of any networked computer system. However, because the IoT will impact so many different sectors and have a role in controlling physical infrastructure and services, these risks are amplified.

A successful attack on an IoT device or system can have significant impact on users, device manufacturers and service providers by affecting the physical as well as the cyber world. It may expose confidential information such as private user data as well as know-how, intellectual property and process intelligence. In addition, it can lead to interruption of operations, compromise of business continuity and even danger to a company's brand image, success and very existence.



Why security is needed

For policy makers, the principal concerns related to IoT risk mitigation are the protection of public safety and privacy. It is critical that networked systems controlling industrial and public infrastructure are protected from both accidental and malicious attacks. Personal information about individuals that are monitored by IoT devices while going about their daily lives or using such devices to monitor their own property also must be protected both from accidental exposure or deliberate theft with intent to misuse.

With its potential to improve traffic flow and thus both manage emissions and save fuel costs, automation of traffic management systems is a common initial project for IoT deployment in municipalities. Early implementations, however, have failed to exercise basic principles of system security and have been shown to be open to attack. In 2014, a white hat team of students at the University of Michigan took control of real, networked traffic signals and found that they could change the status of the lights (red, green, yellow) remotely. It was found that factory default settings were left unchanged and network commands were unencrypted. [9]

In December 2014, the German Federal Office for Information Security reported a cyberattack on a steel mill. Beginning with a penetration of the mill's office computer network, the unidentified attackers were able to cause "massive damage" by compromising the industrial control network and preventing a blast furnace from being shut down properly. [10] While many details of this successful attack are unknown, it is likely that companies with similar automation systems are now closely examining security guidance and actual practice.

A first of its kind attack that caused a loss of electrical power to customers was reported by utility companies in the Ukraine at the end of December 2015. More than 80,000 customers of at least one Ukrainian power distribution company lost service for several hours. While the cause of the outages is still being investigated, it appears that three different strategies were used to gain control of internal systems at the utility, indicating a high degree of planning involved in the attack. [11]

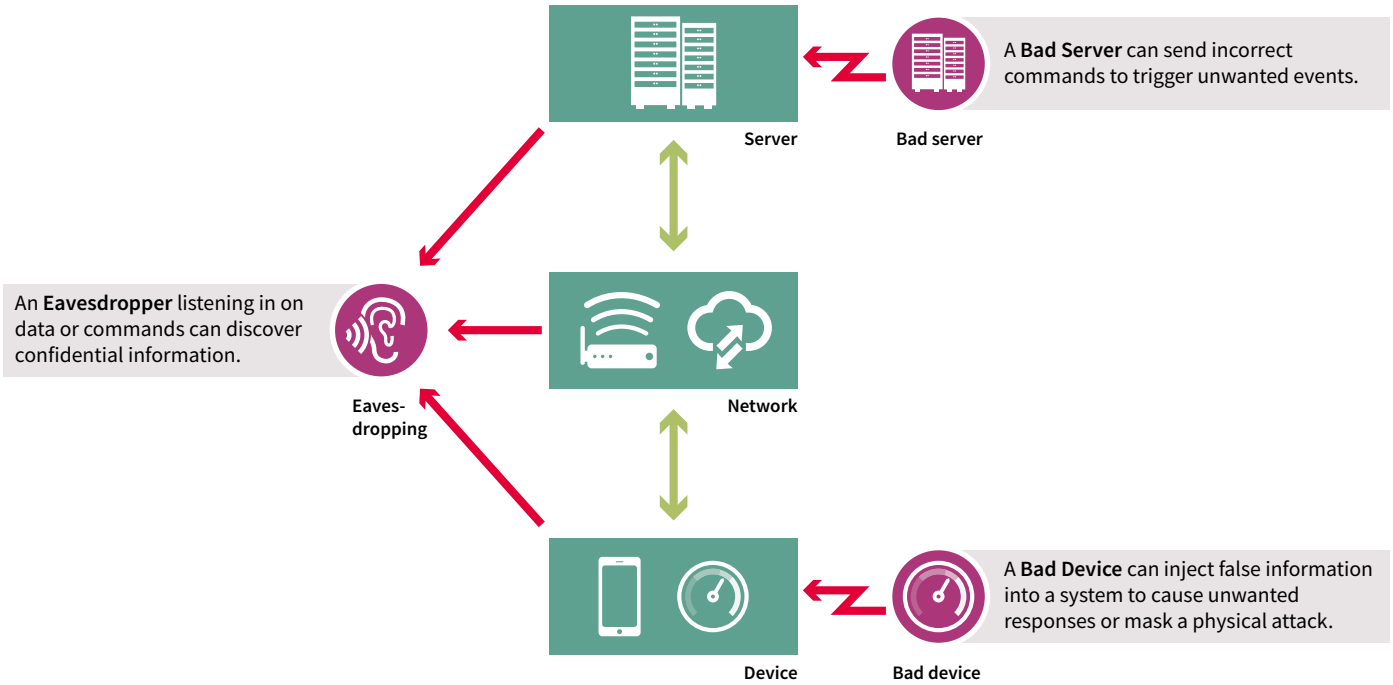
The rush to the IoT for home monitoring and security also appears to have outpaced principles of design for security. A vulnerability study conducted by security researchers in the summer of 2015 [12] found serious security flaws in every one of nine Internet-connected baby monitors it tested. The researchers noted that every camera had a backdoor that would allow intruder access. Additional security flaws included the use of default passwords, easily accessed Internet portals and lack of encryption. Hackers have created web sites featuring thousands of discovered insecure webcams for curious peepers.

One final example of the risks that arise when everyday devices are connected to the Internet was reported in early 2014 by researchers in Silicon Valley. In a one month study of spam messages, the researchers were able to trace spam email to smart appliances, including a refrigerator that had been hacked and used to send spam. [13] Consumers cannot, and should not, be expected to know about and maintain the security status of net-connected home appliances. Appliances, and other devices on the IoT, must be designed with provisions for security that lasts for the lifetime of the product.

4. Managing and reducing risks

The types of risk associated with the IoT vary depending on the application (i.e., smart home, Industry 4.0, Connected Car, Information & Communication Technology, etc.). However, the methods of attacks are common across the range of systems. Eavesdropping attacks are aimed at discovering information (which may then be used in future attacks). Other attacks involve subverting or impersonating the server to send bad commands, or injecting false information from devices with the intent to cause an unwanted response or hide a physical attack.

Security threats for IoT



Clearly, the consequences of eavesdropping vary depending on the IoT application. For an individual, invasion of privacy could escalate to personally catastrophic consequences. If the attack is industrial spying, it may lead to theft of intellectual property or be a precursor to an attack on a plant or other operations. Injection of fake commands can be an annoyance to a home dweller, cause commercial loss to a company, or seriously damage critical infrastructure. Conversely, causing a device to inject false information into the network can easily have negative consequences.

Just as the risks of the IoT mirror other networked technologies, appropriate security responses to protect digital systems have been demonstrated and are relatively well understood. And while there is no single solution to IoT security, there are commonalities in the approach across the many different application scenarios. In every case, the goal of security is to prevent unauthorized reading, copying and analysis of digital information, and to avoid direct manipulation of the protected system. This can be accomplished with a spectrum of techniques that range from a software only approach to the use of robust hardware-based security that is specifically designed to resist even determined attacks by bad actors with access to sophisticated resources.

Assessing risk

IoT security should be evaluated using a risk-based approach, in which increasing levels of protection are applied as overall risk to the system or the information contained in the system increases. A scalable security implementation can be designed to protect each device in a way that isolates simpler, lower cost devices on the edge of the network and builds higher level security at critical points.

Risk analysis also considers the security both of the entire networked system and the many devices that will or could be connected to that system. When devices are linked in a communication network, every linked device represents an attack surface. Even a simple smart lightbulb that is controlled via a wired or wireless link can be an entry point for either a nuisance or more serious attack on an IoT system. [14]

With nearly 30 years of experience in the field of security for embedded systems, Infineon and its customers have learned that a software only approach to protecting systems from malicious attacks leaves both the individual device and larger networked system at risk. Hardware security provides a critical layer of protection appropriate to the risk level of the many different devices that make up the IoT. This critical layer revolves around the concept of a “Root of Trust,” which is a secured area that resides on a computer chip and provides a memory and processing environment that is isolated from the rest of the system. The Root of Trust is shielded from malicious attacks and thus provides security for the other operating layers of the computing system that it protects.

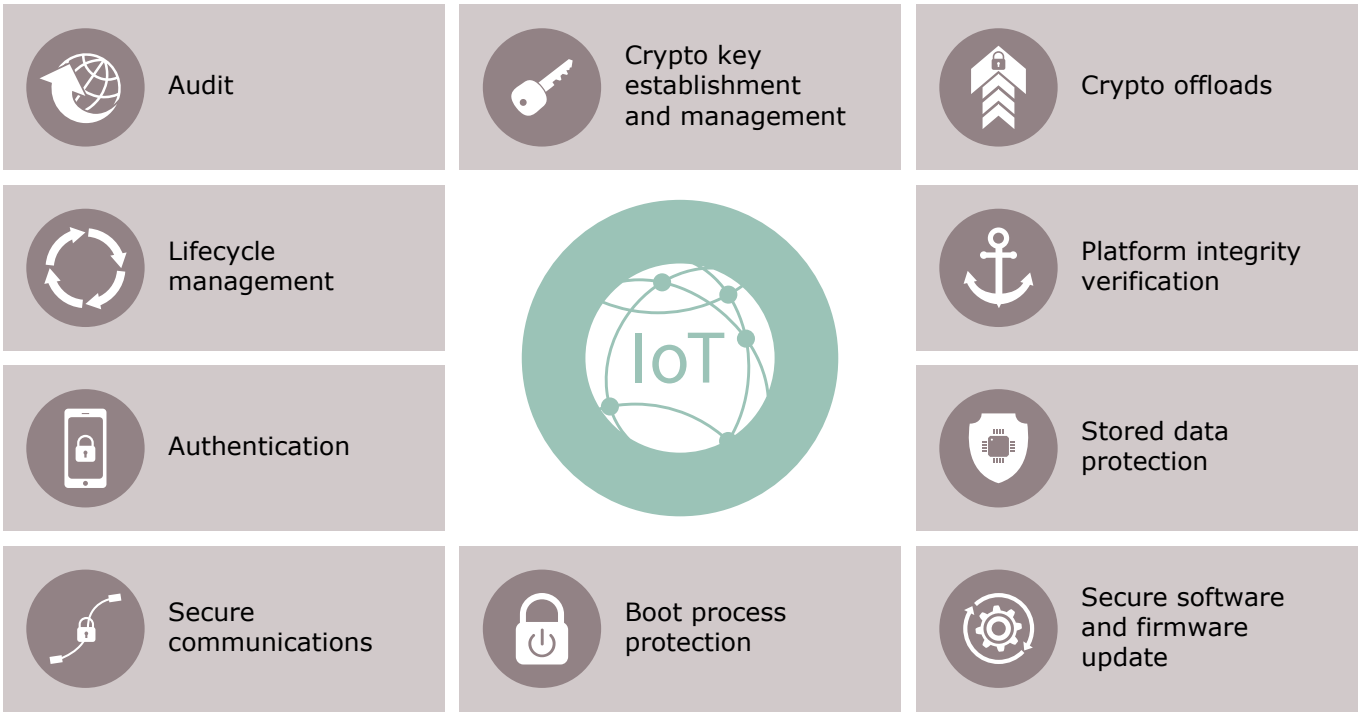
5. Best practices for IoT security

Security for the IoT revolves around three main concepts: Confidentiality, Identity and Integrity. These concepts can be expressed as questions.

- Is the transfer and storage of sensitive data protected?
- Are the components of the IoT system (device, server, etc.) what they claim to be or are they digitally disguised?
- Have the components been compromised or infected?

A Root of Trust is the best way that these questions can be positively answered. The Root of Trust is a security chip hardened against attacks and integrated into the IoT device, network, or server. Depending on the intended application, the chip used can provide different levels of protection that fulfill some or all of the roles for hardware security illustrated here.

Role for chip-based, hardware security



The lowest level of risk in an IoT system may be a non-programmable end node that simply relays sensor data to some type of gateway or local server which verifies the source and includes the input in its operating data. Even at this level, a low-cost authentication chip with a single pre-programmed identity provides a way to confirm identity throughout the device lifecycle. This also helps to prevent the proliferation of cloned devices at the edge of the network. If there is a requirement that the transmitted data be encrypted or that the device be resold or reconfigured, additional protected storage of keys and certificates should be considered.

The data and commands that flow between devices and servers should be encrypted sufficiently to resist attempts at eavesdropping and false command injection. This requires cryptographic computation capability at both ends, which can be scaled to suit the level of risk.

Even at the lowest level of functionality, hardware-based security uses cryptographic mechanisms to protect secret data. The cryptographic algorithm can be implemented running on a general purpose MCU, but it is advisable for the devices themselves to have at least basic tamper-resistant capability and cryptographic functionality. Such protections are already widely implemented in chips such as those used in credit cards. These chips protect themselves and can even automatically erase their memory if tampering is detected.

IoT security benefits from a holistic approach that provides for security throughout the lifecycle of every device used in the system. In systems that use large numbers of low-cost devices, secure hardware supply chains support shipping chips directly from the chip manufacturer to the point of assembly. With a preprogrammed identity, the chips then can register themselves “over the air” when turned on. It is easier to defend against intrusion and subversion if each device is fitted with a security key at a central point of control.

IoT Security Solutions are available

All these techniques (tamper-resistant circuits, authentication, and encryption) have been used previously in other systems but are not yet routinely considered for IoT. Infineon believes the benefits of hardware-based security – including better performance, improved security (including tamper resistance), and security partitioning (protection against bugs in operating system and application code) – make a strong case for using this technology in the IoT.

Infineon is a leader in providing security for the connected world. The company has shipped more than 20 billion secure security chips ICs worldwide in the last 25 years and is ranked by market researchers at IHS as number one in embedded security [15]. The company has a broad portfolio with different product families established to match different system requirements.

Security for embedded systems can be provided by the OPTIGA™ product family, comprising the OPTIGA™ TPM (Trusted Platform Module) as a standardized, feature-rich security solution and the OPTIGA™ Trust family with turnkey or programmable solutions. For secured M2M communication via cellular wireless, Infineon offers the SLM 76 and SLM 97 SOLID FLASH™ products for industrial applications and the SLI 76 and SLI 97 for automotive applications such as eCall (emergency call) services, software updates over the air and Car-to-Car communications. These security ICs are very robust, have extended temperature range specifications and are qualified for industrial and automotive standards.

In the emerging segment of smart wearable devices, Infineon provides embedded Secure Element (eSE) and Boosted NFC Secure Element ICs. Additionally, selected security ICs from Infineon support the latest FIDO 1.0 specifications for secured online authentication.

Security solutions for embedded systems
(OPTIGA™ TPM and OPTIGA™ Trust family)

Security controllers (SLM 76, SLM 97
SOLID FLASH™ families for industrial and SLI 76,
SLI 97 SOLID FLASH™ families for automotive)

Innovative devices for embedded secure elements,
boosted NFC, FIDO, USB token and RFID

More information on the many uses of security ICs and Infineon's product portfolio is available at www.infineon.com/IoT-Security

6. References

[1] "The Internet of Things: Sizing up the opportunity," http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_sizing_up_the_opportunity

[2] "Internet of Things By The Numbers: Market Estimates and Forecasts," http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/

[3] "Los Angeles to upgrade street lights with GPS," http://www.fiercewireless.com/tech/story/los-angeles-upgrade-street-lights-gps/2015-05-14

[4] "LA's Street Lights Can Now Be Wirelessly Controlled," http://gizmodo.com/las-street-lighting-will-be-controlled-by-a-wireless-ne-1696359821?utm_expid=66866090-62._DVNDEZYQh2S4K00ZSnKcw.0&utm_referrer=https%3A%2F%2Fwww.google.com%2F

[5] "New system lets buildings learn from energy use," http://www.capitalnewyork.com/article/city-hall/2014/12/8558111/new-system-lets-buildings-learn-energy-use

[6] "IoT and Big Data Analytics Pilot Bring Big Cost Savings to Intel Manufacturing," https://blogs.intel.com/iot/2014/09/28/iot-big-data-analytics-pilot-bring-big-cost-savings-intel-manufacturing/

[7] "IoT Innovations Offer Essential Benefits for People with Disabilities," http://www.aapd.com/resources/power-grid-blog/iot-innovations.html?referrer=https://www.google.com/

[8] "Driverless Cars: The Car Hack Security Challenge," http://destinhaus.com/driverless-cars-the-car-hack-security-challenge/

[9] Network World, August 20, 2014; http://www.networkworld.com/article/2466551/microsoft-subnet/hacking-traffic-lights-with-a-laptop-is-easy.html

[10] SecurityIntelligence.com; January 14, 2015; https://securityintelligence.com/german-steel-mill-meltdown-rising-stakes-in-the-internet-of-things/

[11] "Everything We Know About Ukraine's Power Plant Hack," Wired, January 20, 2016, http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack /

[12] "Watch out, new parents – internet connected baby monitors are easy to hack,"http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/

[13] "What Do You Do If Your Refrigerator Begins Sending Malicious Emails?," http://www.npr.org/sections/alltechconsidered/2014/01/16/263111193/refrigerator-hacked-reveals-internet-of-things-security-gaps

[14] "Why Lightbulbs Will be Hacked," http://www.eetimes.com/author.asp?section_id=36&doc_id=1327843

[15] IHS TECHNOLOGY Insight Report
Embedded Digital Security Report – 2016
December 2015 ihs.com
Contacts
Sam Lucero, Sr. Principal Analyst
Sam.Lucero@ihs.com

Infineon Technologies AG

81726 Munich
Germany

www.infineon.com