ABSTRACT

The Internet of Things (IoT) is no longer a fanciful vision. The Internet of Things (IoT) has come of age in recent years, but not without some growing pains. It is very much with us, in everything from factory automation to on-demand entertainment. The Internet of Things is developing from being a concept just a few years ago to something far more tangible. Yet by most accounts, the full potential of interconnected systems and intelligent devices for changing the way we work and live has barely been tapped.

The whole idea of the IoT is dependent upon collecting masses of data from billions of so called edge devices, analysing it and deciding on actions. That data needs to be collected by sensors of all description – and those sensors need to be low cost if the aims of those creating products for the IoT are to be realised. Energy-efficient sensor nodes are crucial to the development of the industrial internet of things (IIoT). Although the IoT is still in its early days, applications developers are already looking to put more electronics into smaller packages.

The Internet of Things (IoT), Cloud-based solutions and Big Data represent major challenges for future system designs. IoT devices, which transmit and receive data and commands over the world's universal network, are exposed to a far greater variety and number of threats than earlier products that supported machine-to-machine (M2M) communication, typically over a closed, private network.

Today, it is a given that businesses are embracing the possibilities that the IoT can bring, whether that's collecting data, using data analytics or developing and providing new services or improving existing ones.

This report focuses on the above mentioned challenges that we need to meet in order to realize the Amazing potential of Internet of things (IOT) and overcoming its limitations.

CONTENTS

LIST OF ABBREVIATIONS

IOT	Internet of Things
IIOT	Industrial Internet of Things
M2M	Machine to Machine
2D-IC	Two Dimensional Integrated Circuit
3D-IC	Three Dimensional Integrated Circuit
SoC	System on a Chip
IC	Integrated Circuit
GaN	Gallium-Nitrite
Ga	Gallium
MCU	Micro Controller Unit
PCB	Printed Circuit Board
API's	Application Program Interface
NI	National Instruments
ISP	Internet Service Provider
STRIDE	Spoofing; Tampering; Repudiation; Information disclosure; Denial of service; and Elevation of privilege

LIST OF FIGURES

1. THE AMAZING POTENTIAL OF THE IOT

1.1. Introduction

As digital entities accumulate more and more data about their interactions with the real world, they become a new source for rich analytic information. This drives up the variety and amount of intelligence we can inject into them and the amount of value we can derive from them, creating a virtuous cycle. The explosion of connected entities between now and 2020 will create huge financial opportunities.

The Oxford English Dictionary added a definition for "Internet of Things" in September 2013: "***A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data.***"

So the big change is to connect all the things that have not been put online before. That means everything from toys to towns, houses to skyscrapers, shoes to shoe factories, cars to cows and packing crates to pack animals. The way you put an everyday object on the IoT is by first creating a digital entity to represent the real entity, which provides three important capabilities:

Identity: a way to define itself and capture its real world context in the digital world.

Visibility: a way to be digitally discovered and accessed by stakeholders, incl. other entities.

Intelligence: a way to become smart via digital processing, including the power to make decisions and take actions.

Next we need to connect the real entity to its digital entity counterpart using a mixture of devices.

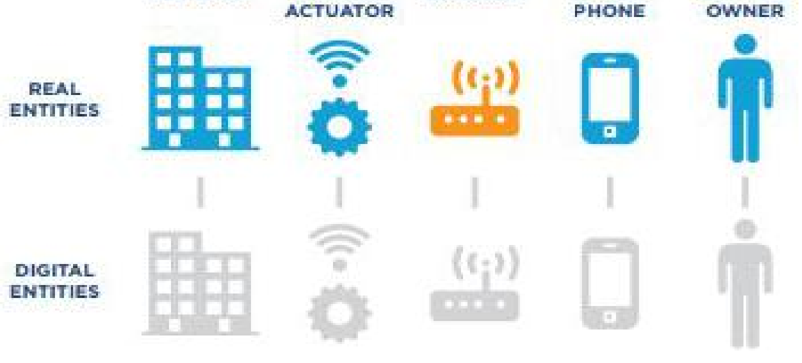


Figure 1: Real Entities and their digital entity counterparts.

Sensors: to provide analog-to-digital translation of data from the real world.
Actuators: to provide digital-to-analog translation of instructions to the real world.
Gateways: to connect the sensors and actuators to digital networks. These devices provide the foundation and scaffolding for building the IoT and are entities in their own right.

1.2 Human Vs. Machine

In his article ***"The Internet of Things and Humans"***, Tim O'Reilly describes "halfway houses" where IoT "applications in waiting" use humans to play roles that will eventually be played by machines. But a human with a smartphone is extremely capable in the role of sensor/actuator, adding two more useful entities to the IoT and giving us a way to realise the IoT right now.

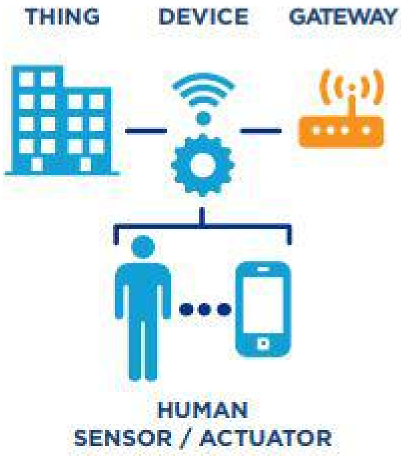


Figure 2: Human as sensor/actuator.

Even more importantly, the combination of human + smart-phone is a practical solution to two of the thorniest problems with autonomous devices: how to provide reliable power and connectivity. People keep their phone batteries charged and their connection plans topped up, with several billion device-carrying people ready to play the sensor/actuator role, either in perpetuity or at least until we get our machine act together.

1.3 Connect, Communicate & Share

Digital entities are concrete software objects hosted by a software service, which we refer to as a Hub. The Hub provides storage, processing and connectivity for digital entities, running locally or remotely – in the cloud. This enables digital entities to define and execute behavioral rules for e.g. performance, quality, compliance and security, and to store data for e.g. attributes, relationships, events and logs.

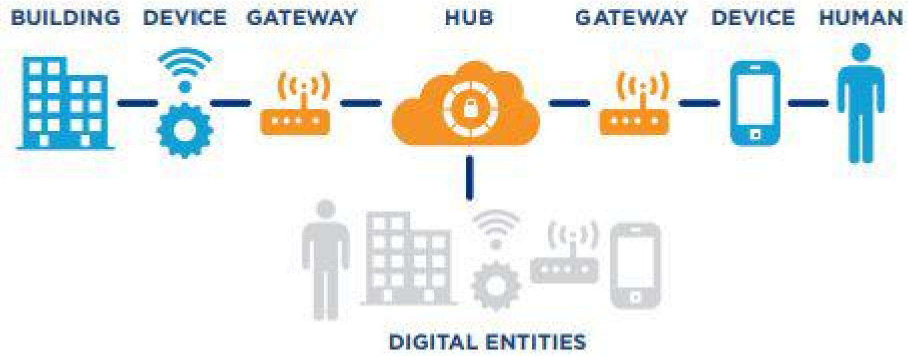


Figure 3: Hub as digital entity hosting service.

1.4 Smart Things Are Valuable Things

A connected digital entity enables stakeholders in the real entity to realize new value in the form of deficiencies, because a smart entity can perform tasks faster & cheaper than before, and opportunities, because a smart entity can interact with the world in new ways.

Tim O'Reilly's article "The Internet Of Things And Humans" also says that the IoT will make designers answer the question:

"How does a smart thing make it possible to change the entire experience and work flow of a job we do in the real world?"

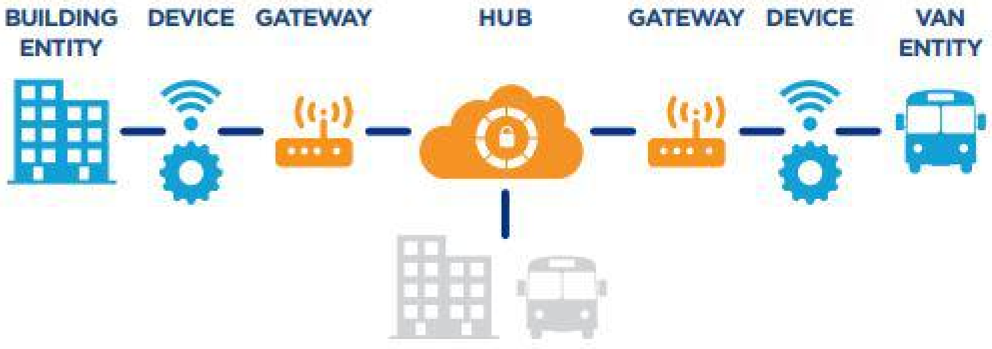


Figure 4: Smart building-vehicle communication

1.5 Smart Components

By connecting our real entities to the IoT we perform a kind of alchemy – where an entity that was previously dumb becomes smart by retrofitting it with IoT technology and providing it with digital processing capabilities. As these digital entities create ever-richer models of the real world, they can adopt a variety of roles based on their ability to monitor, measure, enforce and communicate. For example, we can take advantage of the processing power and capacity of Hubs to not only represent vehicle or building, but also all of their sub components as digital entities. These smart components will be policy-driven – monitoring their usage, scheduling preventive maintenance and providing access to supporting information, e.g. for use by a third-party mechanic to perform diagnostic checks or carry out repairs.

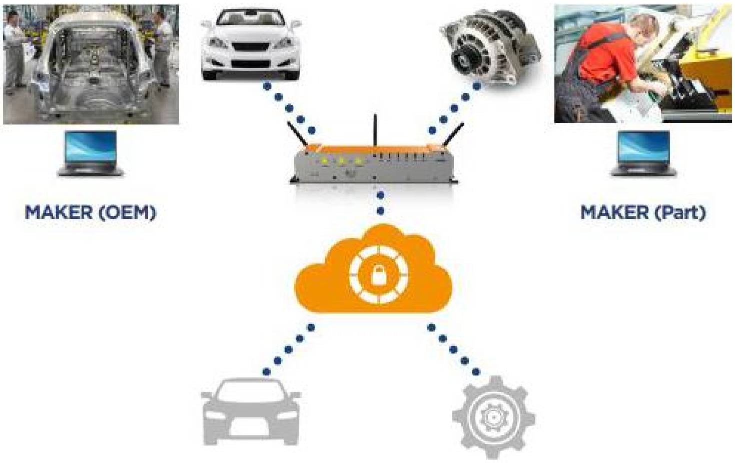


Figure 5: Smart vehicle components

At the same time the vehicle and component manufacturers can get access to rich information spanning across multiple vehicles in the field, which can be used to provide higher quality service and products to existing and future customers.

2. FUTURE VALUE OF THE IOT

As digital entities accumulate more and more data about their interactions with the real world, they ***become a new source for rich analytical information***. This drives up the variety and amount of intelligence we can inject into them and the amount of value we can derive from them, creating a virtuous cycle. The explosion of connected entities between now and 2020 will create huge financial opportunities.

Gartner estimates that the resulting global economic value add to industry as a result of increasing sales and decreasing inputs and costs will be ***$1.9 trillion***, split across a variety of industry sectors: manufacturing (15%), health care (15%), insurance (11%), banking &

securities (11%), retail & wholesale (8%),computing services (8%), government (8%), transportation (6%), utilities (5%), real estate (4%) and other (4%).

By 2020 Gartner estimate over $300 billion incremental revenue for IoT suppliers with $250 billion derived from services. This includes key service elements such as configuration & customization of IoT solutions, integration and data analytics.

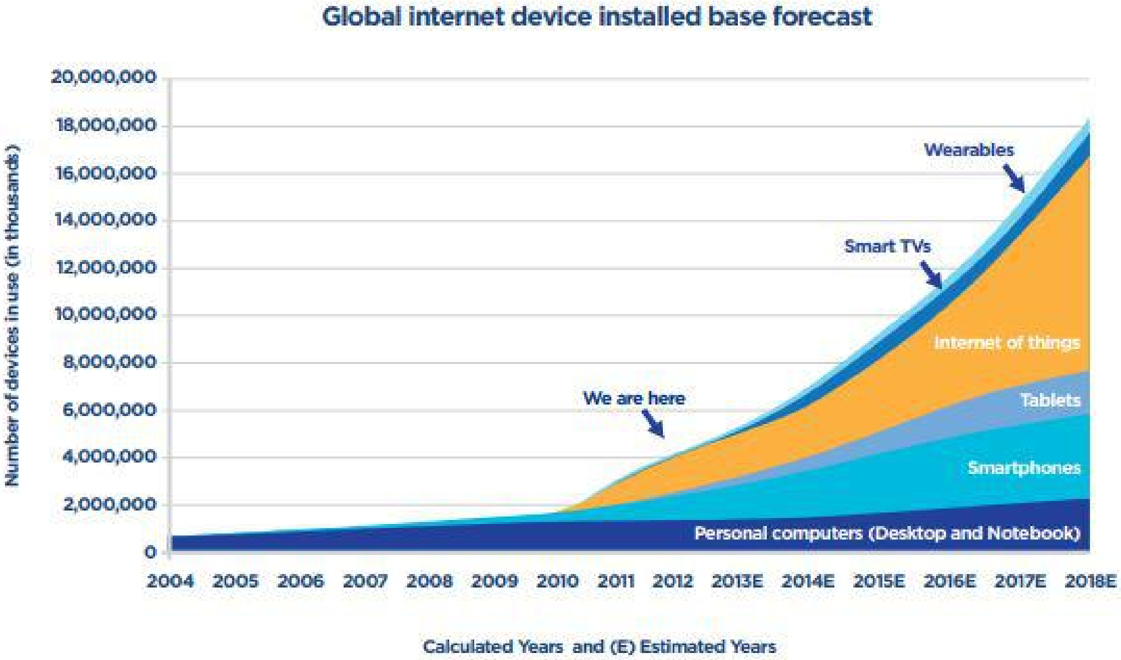


Figure 6: Projected growth of connected entities.

By 2020 the IoT will include an estimated 26 billion installed units. Others estimate that anywhere from 30 billion to 50 billion devices will be connected by then. Some analysts say even these estimates may be conservative.

3. RESEARCH CHALLENGES

The whole idea of the IoT is dependent upon collecting masses of data from billions of so called edge devices, analysing it and deciding on actions. That data needs to be collected by sensors of all description – and those sensors need to be low cost if the aims of those creating products for the IoT are to be realised. Energy-efficient sensor nodes are crucial to the development of the industrial internet of things (IIoT). Although the IoT is still in its early days, applications developers are already looking to put more electronics into smaller packages.

The Internet of Things (IoT), Cloud-based solutions and Big Data represent major challenges for future system designs. IoT devices, which transmit and receive data and commands over the world's universal network, are exposed to a far greater variety and number of threats than earlier products that supported machine-to-machine (M2M) communication, typically over a closed, private network.

The later section deal in detail about the future challenges of Internet of Things and how they can be achieved.

3.1 Design for energy-efficient IIoT sensor nodes

Energy-efficient sensor nodes are crucial to the development of the industrial internet of things (IIoT).

In many cases, these devices will have to perform for years on a single battery charge. That calls for an implementation that is as energy efficient as possible. Achieving this demands a holistic approach to energy optimization, one that reaches from the system level down to process and circuit-design choices.

The problem that faces the engineering team trying to optimise the energy consumption of an IIoT sensor node is that many of the design decisions interact with each other. And there are often hidden complexities of designs that lead to energy consumption being much higher than expected. Because of the long operational life of a typical IoT sensor node, the energy used even when subsystems are sleeping can be responsible for a heavy drain on the battery.

Despite the complex interaction between application design and implementation, there are some high-level choices that are likely to lead toward an optimal solution. One of these is the use of integration. Although it is entirely possible to use 2D-IC and 3D-IC multi chip packaging to assemble a compact IIoT sensor node from off-the-shelf components, integration into a single custom integrated circuit (IC) provides not just significant benefits in terms of cost and size but reductions in power consumption.

The other fundamental consideration for designing energy-efficient IIoT sensor nodes is an understanding of the duty cycle and its impact on lifetime energy consumption. Simply minimizing the power consumption of individual elements is not enough to guarantee that a remote or inaccessible sensor can operate on a single battery charge for a decade or more.

In such a situation, every microjoule the node requires from its battery is important. But that does not mean the system powered by a typical battery can consume no more than a few microwatts at any point in its life. Such a system would not be able to take measurements and communicate them wirelessly in any practical way.

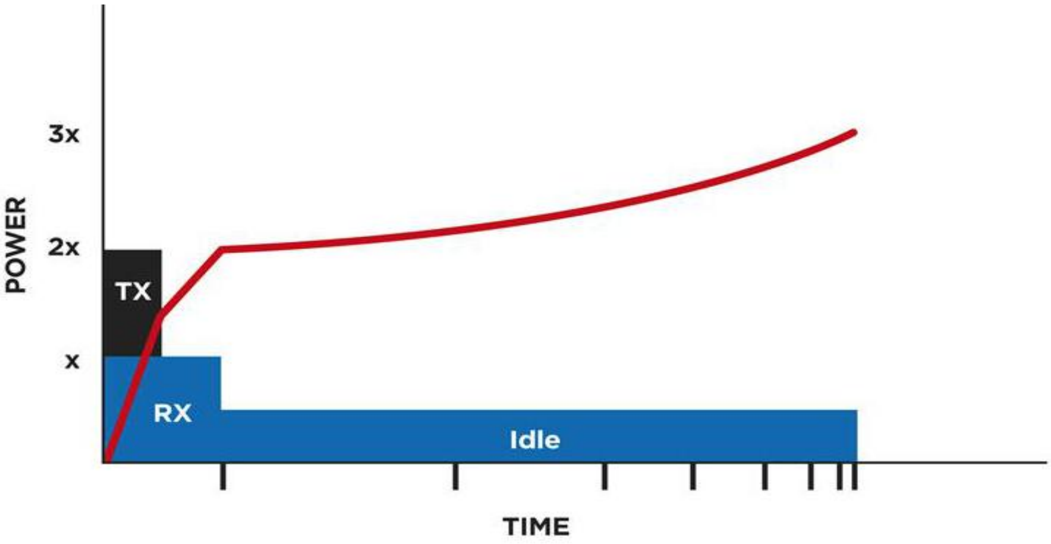


Figure 7: Relationship between time and power consumed

Many factors affect the optimum solution for a given IIoT sensor node application, although a custom SoC will frequently be the best target in terms of energy and overall cost. Therefore, the ability to call on the expertise of design teams with extensive experience in custom mixed-signal IC implementation is key to success.

3.2 Low cost sensors will help the IoT to be realised

The whole idea of the IoT is dependent upon collecting masses of data from billions of so called edge devices, analysing it and deciding on actions. That data needs to be collected by sensors of all description – and those sensors need to be low cost if the aims of those creating products for the IoT are to be realised.

One of the largest opportunities for IoT applications is environmental sensing. At the simplest, these could be measuring temperature, but more complex devices are being considered which can assess environmental quality. However, not only do such sensors need to be low cost, some may even be disposable. Enabling this vision will need new manufacturing approaches.

A team from Georgia Tech in the US believes it might have made significant progress in that direction.

According to the researchers, they have developed a technique by which GaN based gas sensors can be grown on sapphire substrates and then transferred to metallic or flexible polymer support materials. The technique, says the team, could enable the production of low-cost wearable, mobile and disposable sensing devices for a wide range of environmental applications. Transferring the GaN sensors to metallic foils and flexible polymers is said to doubles their sensitivity to nitrogen dioxide gas and to boost response time by a factor of six.

Sensors produced using the Ga Tech process are said to be capable of detecting ammonia at parts-per-billion levels and to differentiate between various nitrogen-containing gases.

Figure 8: Prof Abdullah Ougazzaden, left, and researcher Chris Bishop examine a sample sensor. Pic: Rob Felt, Georgia Tech.

According to the team, this approach for engineering GaN-based sensors is a key step towards economically viable, flexible sensors with improved performances that could be integrated into wearable applications.

So far, the researchers have transferred the sensors to copper and aluminium foil and to polymeric materials. In operation, the devices can differentiate between nitrogen oxide, nitrogen dioxide and ammonia. Because the devices are approximately 100 x 100µm, sensors for multiple gases can be produced on a single integrated device.

They can not only differentiate between these gases, but because the sensor is very small, can also be used to detect them all at the same time with an array of sensors. The engineers expects the devices could be modified to detect ozone, carbon dioxide and other gases too.

The GaN sensors could have a range of applications from industry to vehicle engines – and for wearable sensing devices. The devices are attractive because of their advantageous materials properties, which include high thermal and chemical stability.

In future work, the researchers hope to boost the quality of the devices and demonstrate other sensing applications.

3.3 Building security into IoT devices: the new potential for security integration

IoT devices, which transmit and receive data and commands over the world's universal network, are exposed to a far greater variety and number of threats than earlier products that supported machine-to-machine (M2M) communication, typically over a closed, private network.

The STRIDE threat classification model, originally developed by Microsoft, lists the potential security threats an IoT device or user of that device faces: Spoofing; Tampering; Repudiation; Information disclosure; Denial of service; and Elevation of privilege.

The security functions and resources required to protect an IoT device against these security threats are available in specialised discrete ICs such as:

A secure element: an SoC combining an MCU with on-board cryptographic capabilities, secure memory and interfaces.

A secure non-volatile memory ICs: which typically feature a cryptographic engine for pairing the memory securely to authorised devices.

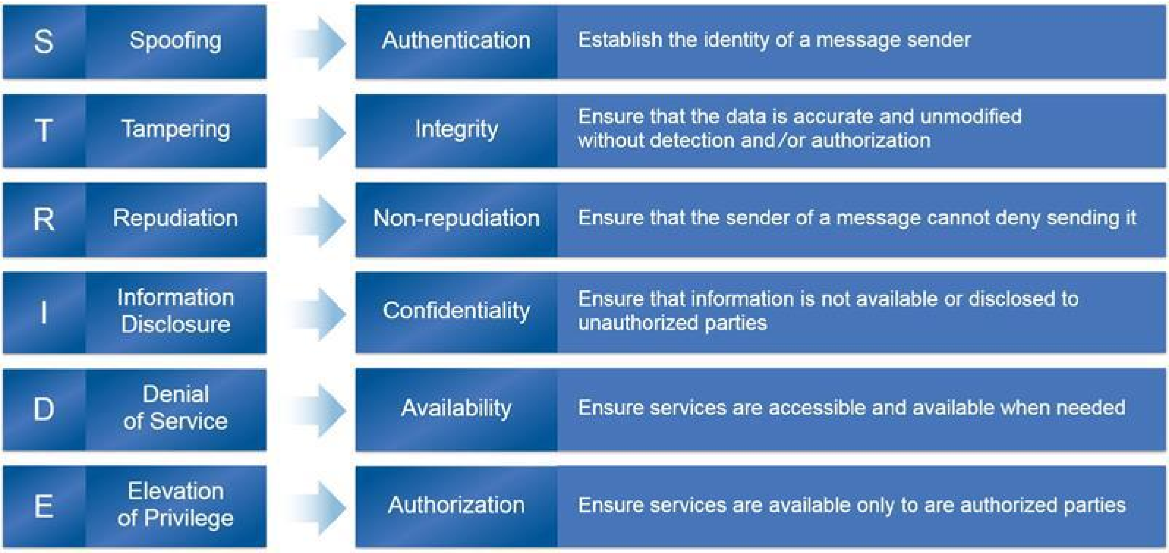
Requirement for core security capabilities

For each of the six STRIDE categories of threats, there are corresponding types of security requirements. Furthermore, an IoT device's security relies on three elements:

Security policies: These define which security requirements are used to provide system, network and/or data access.

Cryptography: Arithmetic algorithms used to implement different types of security requirements.

Tamper resistance: The ability of a system to perform cryptography and enforce its policies without leaking sensitive information or being altered.



S	Spoofing	➡	Authentication	Establish the identity of a message sender
T	Tampering	➡	Integrity	Ensure that the data is accurate and unmodified without detection and/or authorization
R	Repudiation	➡	Non-repudiation	Ensure that the sender of a message cannot deny sending it
I	Information Disclosure	➡	Confidentiality	Ensure that information is not available or disclosed to unauthorized parties
D	Denial of Service	➡	Availability	Ensure services are accessible and available when needed
E	Elevation of Privilege	➡	Authorization	Ensure services are available only to are authorized parties

Figure 9: Each STRIDE threat requires a protecting counter-measure

This ability to offer integrated hardware-based secure storage, cryptographic acceleration and tamper-detection functions has never before been available in an MCU for mainstream IoT applications. The new demands generated by the IoT call for new MCUs that are purpose-built for the IoT, with the security features, low-power attributes and processing capabilities that IoT devices need.

3.4 Establishing Control of the real world and digital entities:

While the tangible benefits predicted for the IoT are huge, there are several hurdles that need to be overcome before we can unlock its full potential. The most important of these is the trust problem, which stems from two sources:

1. The IoT has all the same security problems we have with information on the current Internet, except on a vastly increased scale.
2. The IoT introduces another security problem: a direct two-way connection from the digital world into the real world, which could be used to abuse real entities.

Solving The Trust Problem:

The solution to the trust problem of the IoT has the following elements:

Provisioning Things: a way to connect new entities easily and securely or else building the IoT will take too long, be too expensive and be vulnerable.

Capture Policies: a way to easily capture and manage the rules that govern our entities or else maintaining the IoT will be too expensive, and we will not have control. Enforcing **Policies:** a way to enforce our policies, esp. entitlements, compliance rules, quality measures and performance requirements or else the IoT will not be usable for our most important entities.

Points Of Control

As with information and services on the Web, access to entities and their data must not be open to just anybody. We want each of our digital entities to implement a micro-perimeter that enforces the policies and rules that govern each type of entity.

With the support of Hubs a digital entity can make control decisions for all input and output to and from both the digital and the real entity, at each of the key control points on the IoT connection diagram.

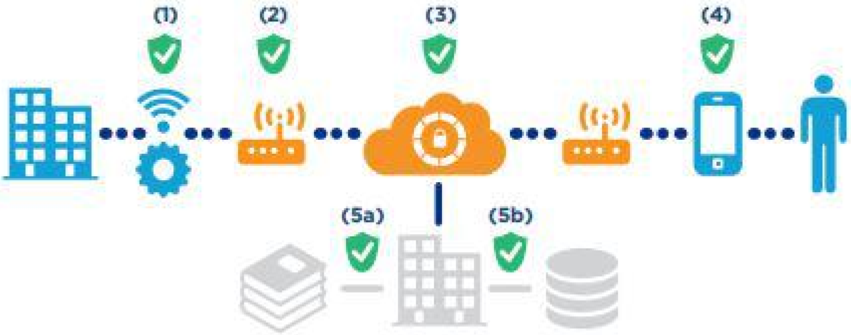


Figure 10: IoT entity access control points

The various control points in an IoT interaction where the entity perimeter can be checked include:

(1) Sensor/Actuator Device – physical security, certified installation & anti-tamper.

(2) Gateway Device – access to front-end & back-end connections.

（3）Hub Service – restricted inbound connection & service-scope permissions.

（4）Client Application Device – physical security & certified ownership.

（5）Digital Entity – read/write access to:

(5a) Rules – behavioral policies, constraints & operations.

(5b) Data – attributes, events, logs & analytic.

3.5 Meeting the PCB design challenge

Although the IoT is still in its early days, applications developers are already looking to put more electronics into smaller packages. Not only that, many products are being designed to fit into odd shapes or to fit into whatever space may be available in existing devices.

That's one challenge; designers are also trying to anticipate the expansion of features within existing hardware, as well as making their products capable of being upgraded when new technology becomes available.

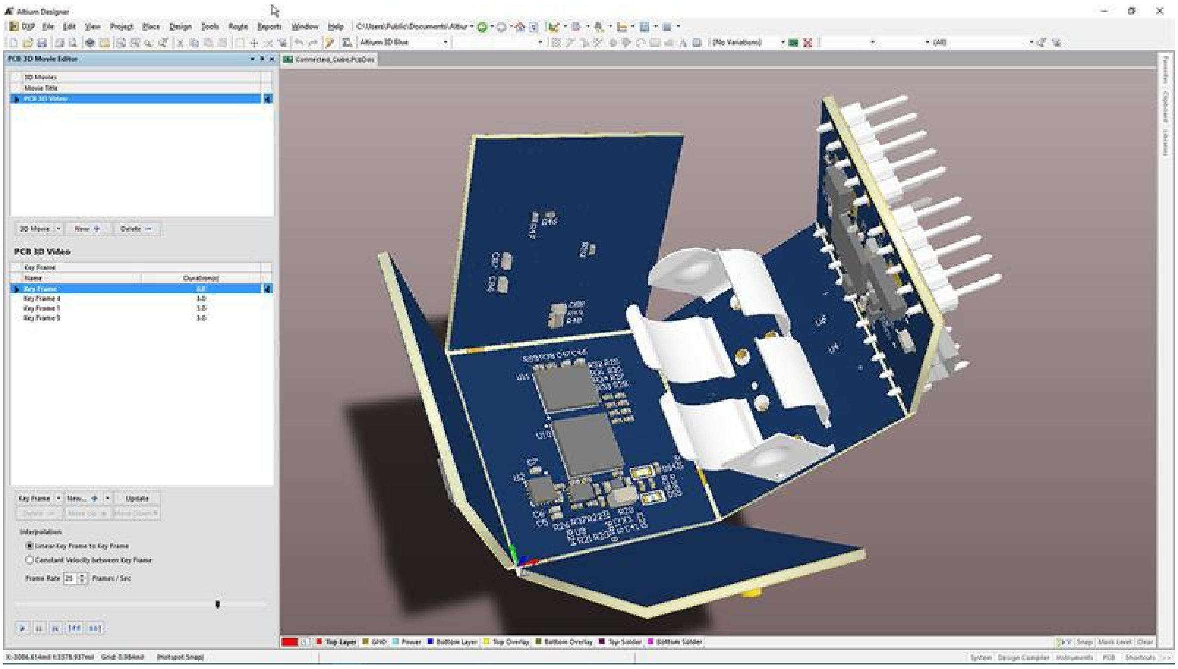
Multiple boards

Distributing the electronics among several PCBs is one solution to most of the challenges associated with IoT devices. From a mechanical perspective, multiple boards allow the electronics package to fit into 'unconventional' spaces. Products such as wearable devices, controls at manufacturing plants and safety and control devices deployed in a vehicle all may need to fit the available space. *Figure 11* shows a typical IoT device with its electronics distributed over several boards, which are then folded together for final assembly.

In other applications, the electronics must fit into an existing package that may not have been designed to house additional components, so integrating them, as well as finding power, can be a challenge.

In this case, rigid-flex PCB components is a potential solution, with designs looking to fit multiple boards into unusual spaces.

One area that relies heavily on rigid-flex technology is wearable IoT devices, which must not only be small and lightweight, but also have to adapt to go and cope with the user's movements. Designers can not only use flexible circuitry to conduct signals, but also to allow the entire package to flex while not breaking, shorting out or being uncomfortable to wear.



Name	Duration(s)
Key Frame	0.0
Key Frame 4	3.0
Key Frame 1	3.0
Key Frame 3	3.0

● Linear Key Frame to Key Frame
○ Constant Velocity between Key Frame

Frame Rate 25 Frames / Sec

X:-3086.614mil Y:3378.937mil Grid: 0.984mil (Hotspot Snap)

Figure 11: Typical multiple board design

In *Figure 12*, designers were challenged to add Bluetooth capability to a heart pump so that it could be connected to the Internet for remote monitoring. After searching for space to contain the circuitry, they found unused space in the connector. As a result, they designed small rigid boards connected by flex circuitry to make the necessary components fit, with a short flex segment fitting over the existing pins to tap into power.

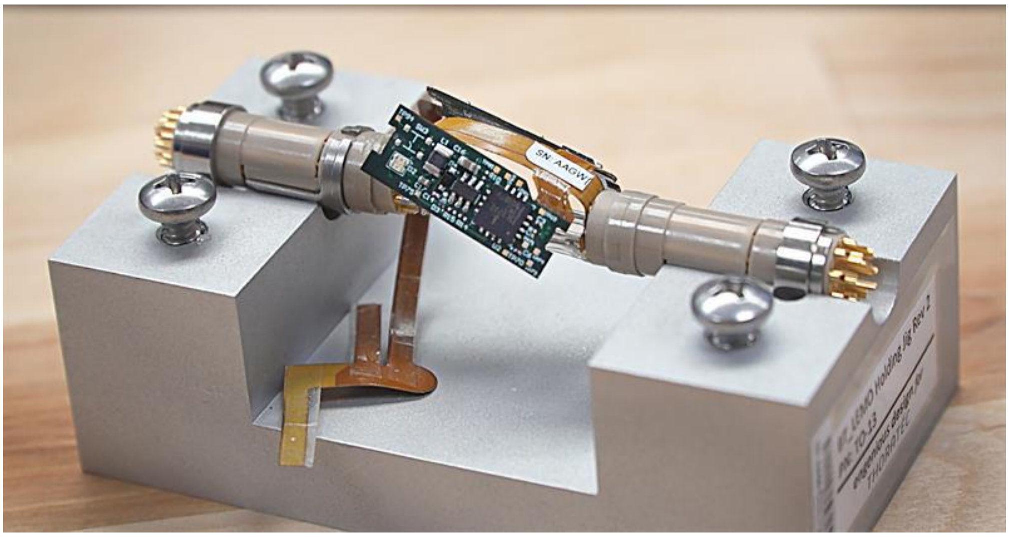


Figure 12: Clever solutions, like fitting Bluetooth communications inside a connector, will be necessary in future (Pic: Engenious)

Future expansion

Product evolution is inevitable if designs are to offer better functionality and to take advantage of better technology. Building on experience, designers are now incorporating ways to allow products to be updated without rendering legacy versions obsolete.

Expansion is twofold: expanded features and functions, and expanded technology.

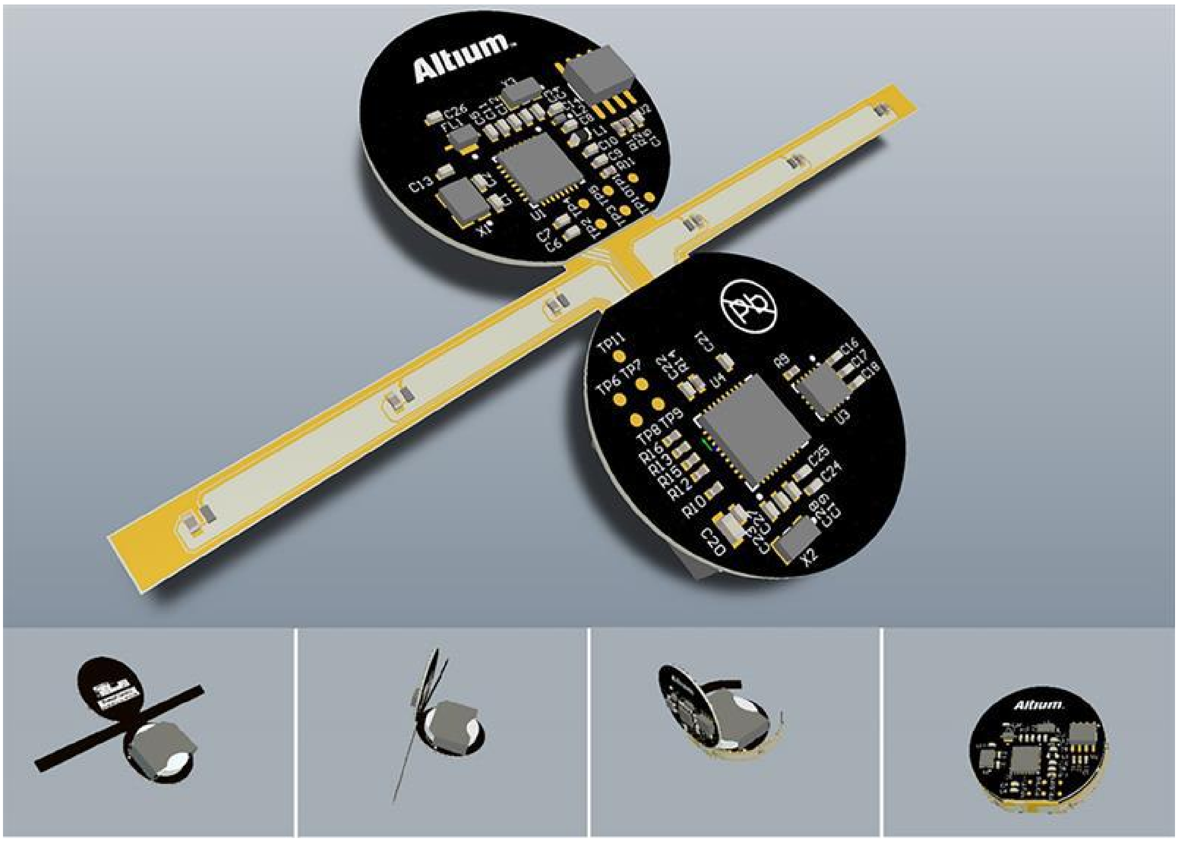


Figure 13: Full motion 3D visualisation allows designers to better communicate to manufacturing how products are assembled

Technology Updates: In the future, we are likely to become reliant upon many IoT devices and will expect them to evolve with technology and to be capable of being updated in a relatively convenient and inexpensive way.

The trivial solution – but also likely to be most expensive – would be to swap out the entire device. More palatable solutions would look at swapping out the updated components. To support this, designers must be ore conscious of development trends and component manufacturers more conscious of easy-to-perform upgrades.

With multiple-board solutions, the technology more likely to be updated could be isolated to a particular board and that could be made more accessible. For example, the processor and memory could be considered most likely to be upgraded and confined to one board. Considering how and what might be upgraded in the future will become a more common PCB design issue.

Many boards, little space:

The near future for IoT devices with respect to PCB design is clear: circuit complexity and speed will continue to increase, while the space available for the electronics diminishes. For most IoT devices, the solution is likely to include electronics distributed across multiple boards, often employing flex circuitry to make it all fit. Meanwhile, designer will need to take advantage of 3D visualisation tools in order to create imaginative solutions.
Fortunately, these tools and design methodologies are fast becoming part of the mainstream because, without them, IoT designs are likely to present insurmountable challenges.

3.6 Defining Systems With a Software Platform

The market is full of amazing tools that have proven their value over the years. From TwinCAT to MATLAB® to LabVIEW, these products have provided innovative functionality that has benefited engineers and scientists. But, the market is lacking a true software platform that enables the next wave of innovations at a pace that we simply just haven’t seen.
Instead of individual tools designed to solve a specific challenge, a software platform is a combination of unique capabilities, protocols, development approaches, and hardware interface APIs. The key to the platform is in the nature of this combination. The platform gives end users the collective power of these components, but is built in a way that the components are individually upgradeable and expandable and easily innovated upon. In other words, the platform has ultimate flexibility.

The undefined, constantly moving, and always evolving nature of the IIoT demands this flexibility. Any individual, vendor-defined tool that claims to be the answer is just plain wrong.

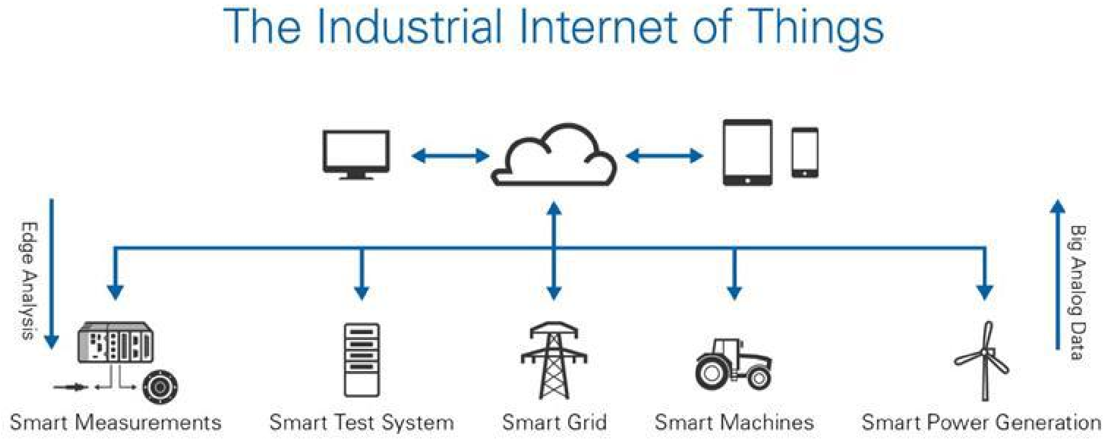


Figure 14: The most daunting IIoT challenges are latency, device synchronization, security, upgradeability, and end-to-end data analytics.

The flexibility of a software platform helps engineers tackle the most daunting aspects of the IIoT: latency, device synchronization, security, upgradeability, advanced control, and end-to-end data analytics. Similar to intelligent decision making, each of these challenges presents itself within every layer of a system of systems. Distributed networks of intelligent nodes, connected networks of smart machines, even the wholly connected factory floor must solve these challenges in a manner that can be changed, upgraded, and enhanced in six months, two years, or five years as new standards and requirements are defined.

Ultimately, the products built from a software platform will be the interface engineers use to solve these challenges. But the software platform itself—the foundational infrastructure—will be the building block that defines the products. A unique value of the platform is the ability to customize components of that delivered product to the specific needs of the problem. In Crossing the Chasm, Geoffrey Moore described this as “vendors must clothe their platforms in applications clothing”. Much like the Betamax, cassette tapes, and dial-up Internet, cassette tapes, and the ‘60s, general-purpose tools will become things of the past. The market demands the specificity of the tool to keep the challenges approachable, even solvable.

The Industry's Only Engineering Software Platform:

In the race to define the technologies that the IIoT will be built on, the company that thinks about the engineer doing the building and defining the next wave of products used to design, build, and test the connected machines will be the company that comes out ahead.

NI is building the industry's only true engineering software platform. Built off of 30 years of investment in LabVIEW software and other engineering-focused software products, NI's software platform will be the technology that connects engineers to the IIoT. Out of this software platform will emerge software products built to solve specific problems within the larger connected network of systems. The LabVIEW Communications System Design Suite, which provides representative productivity benefits to leading researchers such as Nokia and Samsung, is holistically built out of this platform and "clothed" in the application needs of wireless prototyping. And this is just the beginning. The question won't be "why use the NI software platform to solve the IIoT?" The question will be "how could you not?"

MATLAB is a registered trademarks of The MathWorks, Inc.

4. SUMMARY AND CONCLUSION

IT and control systems manufacturers are seizing the opportunity of having new novel hardware devices as the "Internet of Things" begins to scale up. As the number of devices continues to increase, more automation will be required for both the consumer (e.g. home and car) and industrial environments. As automation increases in IoT control systems, software and hardware vulnerabilities will also increase. In the near term, data from IoT hardware sensors and devices will be handled by proxy network servers (such as a cellphone) since current end devices and wearables have little or no built-in security. The security of that proxy device will be critical if sensor information needs to be safeguarded. The number of sensors per proxy will eventually become large enough so that it will be inconvenient for users to manage using one separate app per sensor. This implies single appls with control many "things," creating a data management (and vendor collaboration) problem that may be difficult to resolve. An exponentially larger volume of software will be needed to support the future IoT. The average number of software bugs per line of code has not changed, which means there will also be an exponentially larger volume of exploitable bugs for adversaries.

Until there are better standards for privacy protection of personal information and better security guidelines on communication methods and data/cloud storage, security of wearable and other mobility devices will remain poor. More work needs to be spent on designing IoT devices before too many devices are built with default (little or no) security.

Physical security will change as well. As self-healing materials and 3D printers gain use in industry, supply-chain attacks could introduce malicious effects, especially if new materials and parts are not inspected or tested before use. The main benefits of autonomous capabilities in the future IoT is to extend and complement human performance. Robotic manufacturing and medical nanobots may be useful; however, devices (including robots) run software created by human. The danger of the increased vulnerabilities is not being addressed by security workers at the same rate that vendors are devoting time to innovation. Consider how one might perform security monitoring of thousands of medical nanobots in a human body.

The ability to create secure IoT devices and services depends upon the definition of security standards and agreements between vendors. ISPs and telecommunication companies will control access to sensor data "in the cloud" and they cannot provide 100% protection against unauthorized access. IoT user data will be at risk. Diversity of the hardware and software in the future IoT provides strong market competition, but this diversity is also a security issue in that there is no single security architect overseeing the entire "system" of the IoT. The "mission" of the entire IoT "system" was not pre-defined; it is dynamically defined by the demand of the consumer and the response of vendors. Little or no governance exists and current standards are weak. Cooperation and collaboration between vendors is essential for a secure future IoT, and there is no guarantee of success.

5. BIBLOGRAPHY

[1.] whitepapers/new-life-for-embedded-systems-and-the-internet-of-things

[2.] http://www.newelectronics.co.uk

[3.] electronics-technology/the-digital-industrial-revolution-is-here

[4.] electronics-technology/meeting-the-pcb-design-challenge

[5.] electronics-technology/design-for-energy-efficient-iiot-sensor-nodes

[6.] Converging technologies for smart environment and integrated ecosystems.pdf

[7.] Designing the Internet of things -Adrian McEwen & Hakim cassimally