European Semiconductor Industry Association

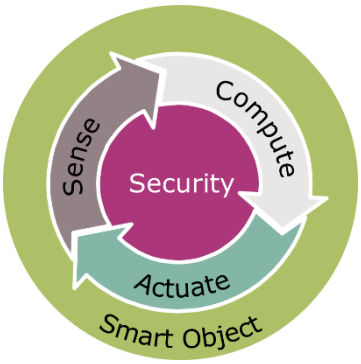
POSITION PAPER

The Semiconductor Industry in Europe: A Key Enabler for Trusted IoT Solutions

Brussels, 28 April 2016

I. Introduction

The "Internet of Things" (IoT) is a network of objects that exchange data with each other and/or the internet. It is "*an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react*"[1].



IoT is one of the most important technology trends of our time – with the potential to radically impact the way businesses and consumers interact among themselves and with their surrounding infrastructure. From a technical perspective, many IoT business models across industries rely on the smart aggregation and interpretation of data. Individual smart objects equipped with semiconductors, such as security controllers, sensors, processors and actuators, deliver the desired data and react to it.

Market trends such as Smart Mobility up to Autonomous Driving, Wearables, Smart Manufacturing, Smart Cities or Smart Healthcare, promise new added value to our society and the economy. By 2025, researchers and industry experts envision the IoT to connect 7 billion people and 50 billion IoT devices, generating annual economic value of several trillion Euros. But the impact of the IoT reaches beyond economic growth and new jobs. It can also help address pressing social and global challenges.

It is now crucial for Europe's success to define a broadly applicable global framework for IoT. The semiconductor industry in Europe is the key enabler to provide the fundament for any secure, smart and power-efficient system architecture. To build trust in the IoT, hardware-based security is vital: sensitive data must be protected, user authentication must be secured and device/equipment integrity must be monitored in order to prevent data theft and fraud. Furthermore, the value chain must be interoperable across sectors and countries and rooted in common standards so that IoT can reach its full potential in the Digital Single Market.

[1] ISO/IEC JTC 1 Information Technology, *Internet of Things (IoT). Preliminary Report 2014*, p. 3. URL: http://www.iso.org/iso/internet_of_things_report-jtc1.pdf (retrieved on 26/04/2016)

ESIA is an Industry Association of:
EECA : European Electronic Component manufacturers' Association
Rue de la Duchesse 11/13 · B-1150 Brussels
Tel: +32 2 290 36 60 · Fax: +32 2 290 36 65 · E-mail: secretariat@eusemiconductors.eu · Web: www.eusemiconductors.eu

II. From Security to Trust

In the hyper-connected world every networked device must be sufficiently secured in order to not become a potential target for hackers. The vulnerabilities are twofold: applied software and installed hardware are two sides of the same coin. It is evident that machine-to-machine communication without direct human interface and control of processes will put a new dimension to the currently existing understanding of the terms “trust” and “security”. Moreover, a balance between high security standards, energy consumption and cost-effectiveness must be ensured in the manufacturing and designing of high-end semiconductor solutions. Any new regulation needs to be “smart regulation” in the true sense of the word. It needs to allow being adapted to new technical and scientific developments and findings.

In order to strengthen the trust in our networked day-to-day and commercial lives, it must be ensured that data is protected and the security of networked devices is guaranteed. To that end, regulatory precautions that are technology-neutral and remain open to innovation, are called for to minimise risks. They need to relate to all sectors and cover all components of the networked devices as well as the overall system architecture. The purpose is to ensure the following minimum requirements:

1. **Security- and Privacy-by-Design:** Manufacturers of connected devices and service providers must ensure that their products are secure and will remain so until the end of their lifecycle. Security must be firmly rooted in the devices, and its implementation at product level must be tested and confirmed in existing and proven state-of-the-art certification procedures like CCRA[2] or SOG-IS MRA[3]. A uniform minimum degree of security features for classes of devices must be ensured.

2. **Integrity is vitally important** in the connected world. Data, device and information integrity – across the entirety of the architecture – needs to be protected at all times. Communication with other IoT devices and data processing should be standardised and use integrity-secured or, where necessary, encrypted channels. Reciprocal authentication of the communication partners is required.

3. The same goes for the **confidentiality of information**: individuals’ identities must be decoupled from the identities of the connected devices to protect users’ rights. To that end, it is necessary to put EU data protection and privacy rules under permanent scrutiny.

Secure semiconductor solutions are able to encrypt sensitive data and capture secure communication. They enable secure identification of connected components, objects, systems and individuals. For the generation of data, the combination of sensor and secure hardware-based anchor function as root of trust will be necessary.

[2] Participating parties of CCRA, the Common Criteria Recognition Arrangement, mutually recognise intermediate levels of evaluation against the Common Criteria (CC) standard. CC is the predominant ISO-standard for IT security, and the certificates are accepted both for commercial and public domain applications, as well as for essential services.

[3] The Mutual Recognition Agreement of the Senior Officials Group – Information Systems Security (SOG-IS MRA) seeks mutual recognition of highest security levels for IT products.

III. Secure & Interoperable IoT

The following, non-exhaustive list of examples is meant to describe particular security requirements for selected IoT use cases.

Smart Mobility

Secure Connected Cars and Intelligent Transport Systems (ITS) are both based on key technologies like Vehicle-2-Vehicle (V2V) and Vehicle-2-Infrastructure Technology (V2X). They are essential parts of Smart Mobility. Connected Vehicles create an intelligent road network that is safer, greener and more efficient.

V2X or modern radar[4] systems allow vehicles to interact with each other and the surrounding infrastructure (like traffic lights and road signs) within a 2,000-metre range, providing critical information to the driver. V2X-equipped vehicles need to follow both the safety criteria of the automotive industry as well as the security and privacy issues of connected systems in general.

As the infrastructure becomes part of ITS, all stakeholders need to define secure and interoperable communication based on trust anchors, almost always based on use of cryptographic protocols in combination with secure hardware. Additional security standards, including solutions for V2V and V2X communication, are necessary. Security in system integrity, such as protections put in place to prevent tempering with safety-critical systems, is equally important for automotive platforms.

A stocktaking exercise about the regulatory context in other regions could be beneficial to identify the best approach.

Wearables

Smart Wearable devices must be designed to understand the user's needs, protect the user's privacy and deliver relevant information when required from Smart Homes and Smart Cities, Connected Cars, etc. Security needs to be implemented throughout the wearable device and the system architecture – with the full data flow being secured from node to application. Moreover, the security protocols may not violate the privacy of the end-user.

IoT environments, and the use of Wearables in particular, are special in that they typically serve and affect multiple stakeholders (e.g. user, service provider), needing to operate for longer timespans in a way that is perceived as reliable by all stakeholders.

Smart Manufacturing

Smart Manufacturing allows for real-time connectivity of value chains and provides significant benefits such as shorter development cycles, reduced time-to-market as well as faster adaption to demand changes. Furthermore, it enables higher productivity through optimal capacity utilisation and an improved quality and reliability of the products.

[4] Advanced Driver Assistance Systems (ADAS)

In order to protect the investments, including Intellectual Property, and the effective operation of a Smart Manufacturing site, dedicated security solutions for different levels of the industrial automation architecture are required. System performance and security specifications vary from field level to control level to supervisor level.

IV. Recommendations

In the wake of the publication of the "Digitising European Industry" package on 19 April 2016, ESIA would like to recommend the following concrete actions:

Regulatory initiatives

- Minimum requirements for security and privacy are needed for different classes of IoT[5] devices. In order to guarantee protection for users and their data, these requirements need to be applied along the value chain and in various layers of these devices and the system architecture. These should be so comprehensive that they apply to all connected devices – whether a Connected Car or an energy management system in a Smart Building.
- In order to achieve a large-scale uptake of IoT by customers, interoperable solutions and common standards must ensure that no obstacles remain, and a Digital Single Market for IoT is achieved. ESIA welcomes the European Commission's call for an open standards environment and supports the objective of international consensus-building on standardisation with other regions.
- European semiconductor companies are global leaders for hardware-based security solutions. In this context, ESIA advocates for a common certification framework with minimum security requirements based on Common Criteria (CC).
- The EU should take the lead on international alignment of the regulatory context. A stocktaking exercise between governments that will enable the assessment of existing regulations in other jurisdiction, in particular the US, China and Japan should be carried out.
- Recently agreed on or adopted legislation, predominately the Network & Information Security Directive (NIS Directive) and the General Data Protection Regulation (GDPR) should be put under permanent scrutiny as for their adequacy to address specific challenges as well as to take into account new questions and phenomena arising from increased uptake and cross-sectorial penetration of IoT applications.
- The regulatory framework needs to strike the balance between energy performance of devices and security patterns. Both issues need to be addressed jointly and must not lead to contradictory or mutually exclusive regulation and/or standardisation.

[5] Such minimum requirements for security and privacy for IoT should be developed by the European Union Agency for Network and Information Security (ENISA), in co-operation with all stakeholders, based on good practices currently deployed and in line with the NIS Directive provisions.

Trusted IoT Label

- Security is complex, and the fast-evolving capabilities of both technologies and hackers create uncertainties about the level of security of aging hardware and infrequently updated software. An additional service to certification, compliant with the requirements of the NIS Directive, must be established to uniquely identify if a product can be trusted or when it should be improved or replaced. A Security Label, along the lines of the European Commission's Trusted IoT Label, with information about the lifecycle of a security solution would create further clarity. The semiconductor industry in Europe strongly supports the implementation of the Trusted IoT Label.

Research & Innovation

- The European Research & Innovation Roadmap should, among other things, focus on security and privacy in the IoT and aim at creating a level playing field for trusted platforms, products and services in the hyper-connected world. ESIA believes that all activities, projects and contributions regarding IoT and its uptake should strive for results that:
    - are technology-neutral, interoperable and transparent;
    - are built on, and use, proven certification schemes;
    - combine measurable security & privacy improvements that elaborate and indicate addressed minimum levels of security, and provide evidence on how to enhance trust and acceptance among customers

V. Conclusion

IoT is expected to connect the physical with the virtual world as none has ever before. With billions of devices communicating almost non-stop, the key word is hyper-connectivity. Data, sometimes sensitive in nature, will flow in unprecedented amounts. To facilitate this vast exchange, the entire network architecture from cloud to end-user device must be able to communicate with integrity, it must be secure, and the data must be protected; but above all: consumers have to trust these devices to ensure all of that.

The semiconductor industry in Europe is a key enabler for this new, hyper-connected world and has a long tradition in offering innovative and secure hardware solutions, required for rendering digitisation possible and building trust and confidence both in the Digital Single Market, and around the world. ESIA represents global leaders for hardware-based security solutions that apply the principles of Security- and Privacy-by-Design, and provide the fundament for any secure, smart and power-efficient system architecture.

However, there won't be any IoT revolution without addressing concerns related to interoperability, security and privacy. Disruptive innovations such as IoT will require out-of-the-box thinking from programmers, manufacturers and policymakers. In this context, ESIA welcomes the European Commission's initiative to establish a Trusted IoT Label and offers its know-how to contribute to a secure Internet of Things which is fully trusted by all stakeholders.

For further information:

Hendrik Abma
Director General
European Semiconductor Industry Association (ESIA)
Tel: + 32 2 290 36 60 Web: http://www.eusemiconductors.eu

ABOUT ESIA

The European Semiconductor Industry Association (ESIA) is the voice of the Semiconductor Industry in Europe. Its mission is to represent and promote the common interests of the Europe based semiconductor industry towards the European Institutions and stakeholders in order to ensure a sustainable business environment and foster its global competitiveness. As a provider of key enabling technologies the industry creates innovative solutions for industrial development, contributing to economic growth and responding to major societal challenges. Being ranked as the most R&D intensive sector by the European Commission, the European Semi-conductor ecosystem supports approx. 200.000 jobs directly and up to 1.000.000 induced jobs in systems, applications and services in Europe. Overall, micro- and nano-electronics enable the generation of at least 10% of GDP in Europe and the world.