An Ecosystem Vision of Security and Data Protection for the Internet of Things

Antonio Kung (Trialog), Ahmed Amokrane (CoESSI), Hocine Ameur (CoESSI),
Hervé Daussin (CoESSI), Olivier Genest (Trialog)

antonio.kung@trialog.com, ahmed.amokrane@coessi.fr,
hocine.ameur@coessi.fr,herve.daussin@coessi.fr,
olivier.genest@trialog.com

Abstract. This paper takes an ecosystem perspective in approaching security and data protection for the internet of things. It first provides a rationale on the need to consider ecosystems. It then explains the impact of security and privacy at the lifecycle level. It then elaborates on the need to take an integration approach taking into account all non-functional requirements such as safety, availability and so forth. It highlights in particular the need for stakeholders specialised for assurance and testing, covering one use case on smart grids and another use case on transport. It concludes with recommendation to investigate a number of issues.

Keywords: Ecosystem, Internet of things, Lifecycle, Suppliers, Integration of non-functional requirements, Interoperability, Privacy Impact assessment, Privacy-by-design.

1 Introduction

The Internet of Things (IoT) refers to smart devices, sensors, and actuators that are embedded in the physical world, connected to each other and to further computing resources, allowing applications and intelligent services through standard communication networks. An IoT system can include a wide variety of hardware and software elements, ranging from simple temperature sensors to complex systems such as robots, autonomous vehicles or drones. An IoT system can also be part of infrastructures providing essential services such as smart grids, or transport, which means it has to meet stringent operational requirements such as safety. Consequently it is important to take into account the ecosystem in which such IoT systems are designed, developed, deployed and operated. The term ecosystem, initially used in biology to designate an ecological community together with its environment is now widely used in the information and communication technology (ICT) community to designate a complex network of stakeholders. This paper takes an ecosystem perspective in approaching security and privacy for IoT systems, reflecting similar coordination orientations:

- Research is structured around ecosystems. For instance, at the European level, coordination on IoT research is led by the AIOTI (alliance for IoT initiative) public privacy partnership [1]. Likewise, research on big data is led by the BDVA (big data value association) public privacy partnership [2]. Finally research cooperation on smart cities is carried out within the EIP-SCC (European Innovation Platform on Smart Cities and Communities) platform [3].
- Standardisation is also structured around such ecosystems. For instance ISO has established in recent years three working groups dedicated to big data (ISO/IEC JTC1/WG9), smart cities (ISO/IEC JTC1/WG11), and IoT (ISO/IEC JTC1/SC41) respectively. Further, standardisation topics on security and privacy are also defined around such ecosystems. A proposal is currently discussed for the creation of a standardisation project to provide security and privacy guidelines for the IoT. An on-going project is already in place for big data (ISO/IEC 20547-4 – big data reference architecture – security and privacy fabric). A proposal is currently discussed for the creation of a standardisation project on privacy for smart cities. An overview on such activities is provided in [4].

The paper first provides a rationale on the need to consider ecosystems. It then explains the impact of security and privacy at the lifecycle level. It then elaborates on the need to take an integration approach taking into account all non-functional requirements such as safety, availability and so forth. It highlights in particular the need for stakeholders specialised for assurance and testing, providing two examples on smart grids and transports. It concludes with a list of four issues.

2 The need for an Ecosystem Viewpoint

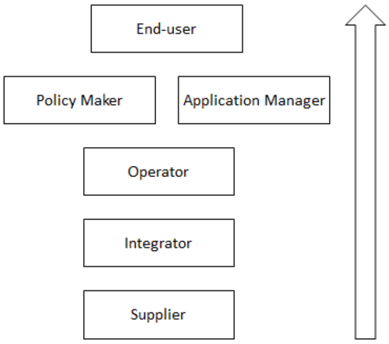


Fig. 1. Ecosystem stakeholders

Fig. 1 lists important stakeholders in an ICT ecosystem:

- Suppliers provide the components of an IoT system: a sensor, a (smart device), a cloud system, electronic components, security components, operating systems, middleware, tools, methods and so forth.
- Integrators build the IoT system, integrating the various components provided by suppliers.
- Operators deploy, operate and maintain the IoT system.
- Application managers are the interface with end-users.
- Policy makers provide rules concerning the application.
- End users are the beneficiary of the IoT system.

ICT systems in the past involved less complex ecosystems. Before the advent of smart phones, a mobile phone offer would typically consist of a mobile operator and a mobile phone supplier. The same stakeholder would play the role of application manager, operator and integrator. The number of suppliers would be limited. This is no longer the case in IoT systems. Many stakeholders of different types (e.g. research organisations, SMEs, large companies, public organisations) might be involved. Here is an example for a smart transport application providing real-time traffic advice to citizens. End users are the inhabitants of a city. The application manager and the policy maker is the city. The operator can be a local SME associated with a major international cloud operator. The integrator can be a very large company with experience in building complex systems. The suppliers can be local producers of devices (e.g. a display system), an external start-up providing features for real-time advice, and a big operating system provider.

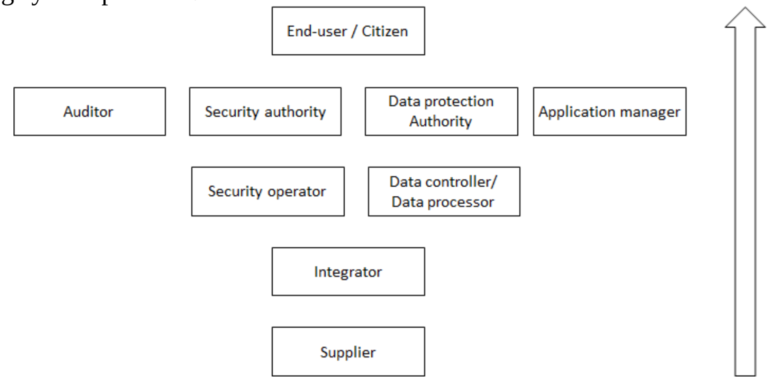


Fig. 2. Ecosystem from a security and privacy viewpoint

The resulting complexity of IoT ecosystems also has a profound impact on the way security and privacy can be integrated. **Fig. 2** shows the specific roles and stakeholders that need to be taken into account when focusing on security and privacy. From the security viewpoint:

- suppliers provide components that may contain security capabilities (e.g. dedicated security hardware, or security mechanisms integrated in a larger component);
- integrators have to provide the overall security capabilities integrating those provided by suppliers;

- security operators have to carry out the specific security operation duties (e.g. security supervision, security incident management);
- security authorities provide operation rules to the security operators (e.g. guidelines upon security incident):
- auditors verify that operation rules are well followed (e.g. security management conformance);
- application managers get the operation rules from the security authority;
- end users or the beneficiary of the IoT system are protected at the security level.

Likewise, from the privacy viewpoint:

- suppliers provide components that may contain data protection capabilities (e.g. de-identification mechanisms);
- integrators have to provide the overall data protection capabilities integrating those provided by suppliers;
- data controllers and data processors carry out data protection related operations (e.g. consent management, privacy breach management);
- data protection authorities provide operation rules to the data controllers and data processors (e.g. privacy impact analysis guidelines);
- auditors verify that operation rules concerning privacy management are well followed;
- application managers get the operation rules from the data protection authorities;
- end-users or citizens using the IoT system are protected at the privacy level.

Table 1 and **Table 2** provide an example of the security ecosystem and privacy ecosystem in a hospital health monitoring system of patients living in their home.

Table 1. Example of smart city security ecosystem

Stakeholder	Example of stakeholders	Example of security related activity
End-user	User of health monitoring system	Relies on a 24x7 system
Auditor	Security conformance auditor	Verifies that hospital information system and health sensor communication systems conform with security requirements
Security authority	National security center	Carries out audit of security related activities
Application manager	City security officer	Manages security breach
Security operator	Hospital	Monitors systems against cyberattacks
Integrator	Integrator of hospital information system	Carries out security risk analysis Implement security capabilities
Supplier	Health sensor communicating with information system	Provides a secure channel capability.

Table 2. Example of smart city privacy ecosystem

Stakeholder	Example of stakeholder	Example of privacy related activity
End-user	User of health monitoring system	Provides consent Complains to the city data protection officer in case of privacy breach
Auditor	Privacy conformance auditor	Verifies that hospital information system, health sensor communication systems and associated operating procedures comply with GDPR [6]
Data protection authority	National data protection authority	Provides recommendations to city data protection officer and hospital manager. Carries out audit of privacy related activities. Interacts with city data protection officer in case of privacy breach
Application manager	City data protection officer	Manages citizen requests for privacy information. Manages privacy breach
Data controller/ Data processor	Hospital	Maintains a registry of personal data processing, and a secure log of access
Integrator	Integrator of hospital information system	Carries out privacy impact assessment Implement data protection capabilities
Supplier	Health sensor communicating with information system	Provides a user control capability

IoT ecosystems can be profoundly impacted by global concerns such as security or privacy. These concerns are addressed by policy makers who define rules and provide recommendations that will influence the way IoT systems are built and operated. Since the building and operation of IoT systems involve a complex set of stakeholders, it will be important to understand how recommendations are taken into account and how it impacts on the contractual relationships between these stakeholders.

3 The Impact of Security and Privacy on the Lifecycle of an IoT System

The recognition by policy makers that cybersecurity incidents or privacy breaches are bound to happen has profoundly changed the regulation landscape. Upcoming regulations and recommendations on security and privacy is therefore changing the mindset of the ICT community from avoidance (i.e. the priority is to build a system that is protected so that incidents cannot happen) to a resilience mindset (i.e. the priority is to build a system that is protected throughout its lifecycle).

This change of mindset is well exemplified in the area of security by the NIST recommendations [5] which advocates a new security framework. **Fig. 3** shows on the left the former security framework, focusing on a design oriented vision with two processes: identify risks, design and deploy controls. In the new framework on the right, the focus is a life cycle perspective with the following set of processes: identify risks, protect, detect, respond and recover.

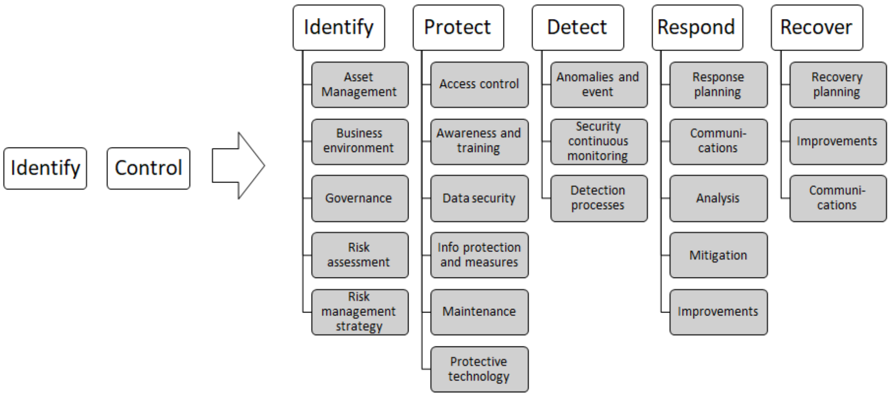


Fig. 3. Moving towards a Cybersecurity Lifecycle Practice

Table 3. Privacy engineering lifecycle processes

Types of processes	**Selected system life cycle processes** [7]	**Privacy engineering processes** [8]
Agreement processes	Acquisition process Supply process	Supply chain involving personal information
Organizational project-enabling processes	Human resources management process	Privacy engineering human resource management
	Knowledge management process	Privacy engineering knowledge management
Technical management process	Risk management process	Privacy risk management
Technical processes	Stakeholder needs and requirements process	Stakeholders' privacy expectations
	System requirements definition process	Privacy principles operationalisation
	Architecture definition process	Impact of privacy concerns on architecture
	Design definition	Impact of privacy concerns on design

This change of mindset is also visible in the area of privacy. While there has been significant focus on design in so-called privacy-by-design approaches [9,10,11,12], a recent focus on lifecycle has taken place, in the PRIPARE initiative on privacy engineering [13,14], followed the current work at ISO level. The ISO/IEC 27550 report [8] is structured according to sevon system lifecycle processes following ISO/IEC 12588 [7] as showed in **Table 3**.

4 The Challenge of Integration

There are at least two important integration challenges associated with security and privacy in the IoT.

The first challenge is on the integration of the different concerns: security, privacy and other concerns such as safety. For instance it is important to have an integrated view of security, privacy and safety risk analysis. **Fig. 4** shows a typical integrated risk analysis model: the central point is the event one wishes to avoid; cybersecurity feared event, privacy breach, dependability failure. The left part focuses on sources: threats/vulnerabilities, problematic data action (using [15] terminology), and faults/errors. The right part focuses on consequences: impact on the protection of digital assets, impact on the privacy on individuals, and on the safety of operations. The result of an integrated risk analysis process should be a set of organisational and technical measures covering the three types of concerns: security, privacy, and safety.

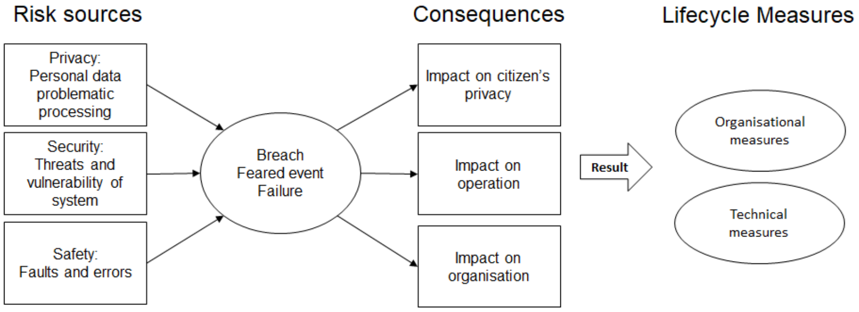


Fig. 4. Risk analysis process integrating security, privacy, safety

The second challenge is on the integration of suppliers contributions. Let us first assume that there are no suppliers, i.e. the integrator develops the whole system. **Fig. 5** shows describes a simplified model of what it takes to integrate security and privacy in a system:

- a developer develops a system;
- the system includes security and privacy capabilities;
- the security and privacy capabilities are documented by a system security and privacy risk analysis;
- the security and privacy capabilities are demonstrated by system assurance capabilities.

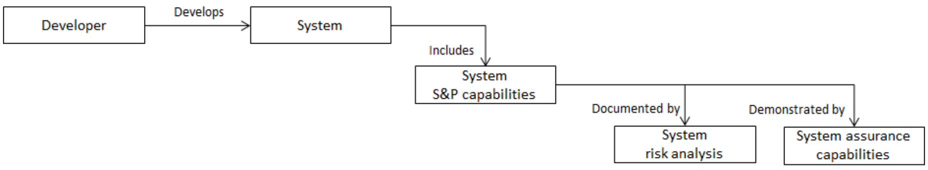


Fig. 5. Developing a system including security and privacy capabilities

Fig. 6 shows an example: the system is a smart meter, providing a secure communication channel capabilities. The smart meter is provided with a smart meter risk analysis report and with a penetration test system demonstrating protection concerning communication.

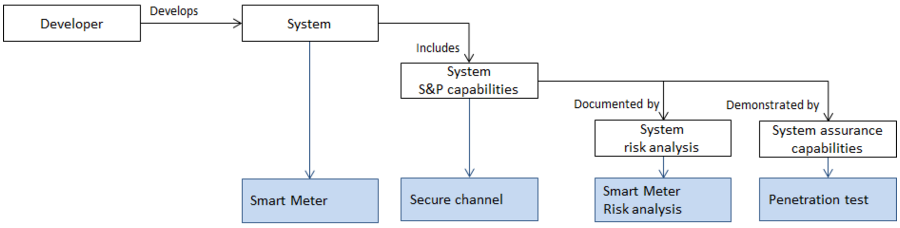


Fig. 6. Example of a system including security and privacy capabilities

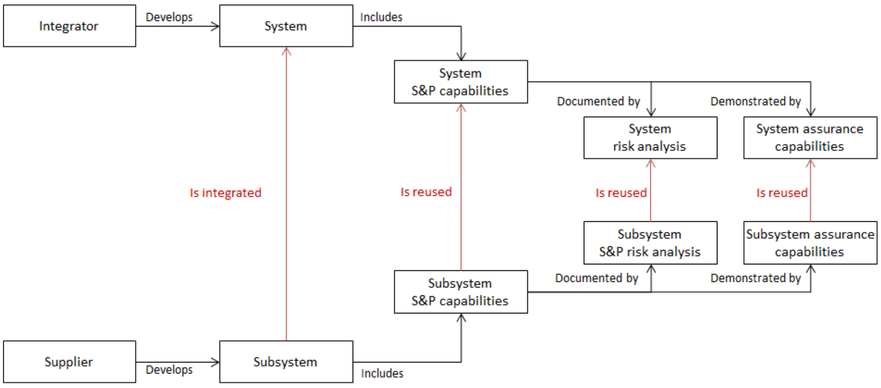


Fig. 7. Integrating a subsystem which itself includes security and privacy capabilities

Let us now assume more complex IoT systems where several stakeholders are involved in the development of the system. **Fig. 7** shows the case of an integrator which develops a system that includes a subsystem which is provided by a supplier:

- the integrator is responsible for the overall development of security and privacy capabilities, part of which can be provided by the subsystem,
- he carries out a system security and privacy risk analysis of the entire system, taking into account the security and privacy analysis associated with the subsystem,

- he develops system assurance capabilities (e.g. penetration test) for the entire system, integrating the subsystem assurance capabilities.

5 The Impact on Assurance and the Need for Penetration Tests

Throughout the whole process of running the ecosystem, the chain of dependability from the supplier all the way to the end user needs to rely on an agreed level of assurance. One important type of assurance is penetration testing. While risk assessment (safety and security) and privacy impact assessment are the means by which one can have insights on the risks and impacts that can result from using an IoT system, penetration tests provide the means to measure the impact of an attack. The measurement can be in terms of properties (such as confidentiality, integrity, availability for security, or unlinkability, transparency and intervenability for privacy [16]). A penetration test will provide some level of evidence that the system is properly protected.

In fact, risk assessments and penetration testing need to be performed at different levels: at a component level as well as at the fully integrated level. In the latter case, the system is viewed as a whole and risks caused by lack of security controls for instance can have top management level business impacts. The security tests need to be carried out on the whole attack surface of the IoT solution. This attack surface mapped on the IoT architecture as presented in **Fig. 8** includes [17]:

- Internet facing services
- Web and administrative interfaces
- Cloud infrastructures
- Mobile Applications
- Communication networks and wireless communication media
- Communication APIs and web services
- Hardware
- Device firmware and software updates

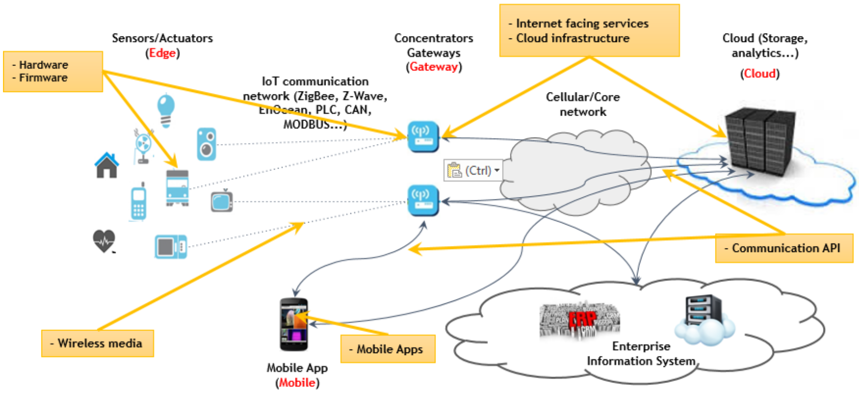


Fig. 8. IoT Architecture [17]

Security tests will confirm and further look for vulnerabilities that can lead to system or data compromise if exploited by an attacker. These tests are conducted using generic existing tools or specific tools developed to fit the purpose of the target system. This process which might lead or not to a certification procedure results in clear identified responsibilities and design criteria to be integrated by the suppliers as required by the users/integrators. Moreover, the self-reinforcing lifecycle is run over and over from the user all the way to the supplier to span the entire supply chain ecosystem. Note that the aim is to guarantee a target level of security of the components and/or the fully integrated system.

To illustrate the needs for an ecosystem including the lifecycle, we provide, in what follows, some examples from industrial projects of securing IoT infrastructures.

5.1 A large scale Smart Grid project

In this context, security was addressed first through a large scale thorough risk assessment. The risk assessment both at the system and component levels identified the threat scenarios and feared events. Moreover, privacy risk assessment, as required by the regulation, was conducted on the personal identifiable information of parts of the system. The risk assessment with regard to data protection of the personal identifiable information resulted in a set of recommendations and data anonymization to guarantee users' privacy. These controls were integrated into the design phase of the different devices and data storage platforms throughout the system and enabled by default to assure privacy-by-design of the whole system.

The threat scenarios identified during the risk assessment were then put to practice through penetration testing spanning the whole attack surface. The results of the penetration testing identified weaknesses that confirm the feared events of the risk assessment. Moreover, the penetration testing confirmed or helped to adjust the likelihood of the attack scenarios to reflect the real-life attack cases. Consequently, a set of additional security controls and design rules were identified and pushed up to be included in the next iteration of the components and the integrated system. These rules and controls further improve the security-by-design and privacy-by-design of the system as they are being integrated throughout the development lifecycle regarding the different stakeholders of the supply chain. For instance, integrating Hardware Security Modules (HSM) into concentrators were identified to be integrated in the security-by-design of the devices. These HSM ensure confidentiality of the encryption keys as well as a secure way for performing the data encryption. Moreover, these penetration tests were conducted in the certification process of components to guarantee a certain level of security. It's worth noting that a set of other interoperability and functional tests were run to homologate the whole system.

Fig. 9 provides a bird's eye view of the security process from the supplier to the integrator. The security policies are checked in this case within the smart meter (subsystem level) as well as the smart grid (global system level). During the integration phase, the security and the privacy analysis performed on the smart meter are considered and reinforced by another security study at the global system level.

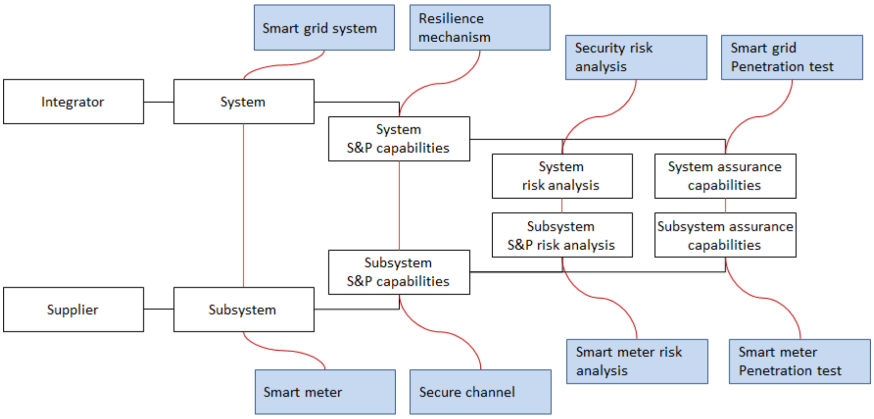

Smart grid system
Resilience mechanism
Security risk analysis
Smart grid Penetration test
Integrator
System
System S&P capabilities
System risk analysis
System assurance capabilities
Subsystem S&P risk analysis
Subsystem assurance capabilities
Subsystem S&P capabilities
Supplier
Subsystem
Smart meter risk analysis
Smart meter Penetration test
Smart meter
Secure channel

Fig. 9. Integrating a smart meter with security and privacy capabilities to the smart grid

Smart grid systems are exposed to a large attack vectors and attackers' profiles, this is due to their distributed nature, large scale deployments and multiplicity of technologies. Furthermore, each part of the infrastructure could represent an entry point into the system, if one of these parts is compromised, the whole system can be exposed. Attacking a smart grid system can affect the power utility network as well as the end users (homes/businesses), including their personal data. Furthermore, the security of the smart grid and protection of the communicated data must be insured for the final customers, in compliance with the CNIL regulation at the French level few years ago and currently the European data protection and privacy legislation [6].

To show how the risk assessment can be done through multiple stages, we restrict our study to The AMI (Advanced Meter Infrastructure). The AMI is integrated within the smart grid system and it includes, home network systems, smart meters and communication network. The AMI and its network provide an important pillar for the smart Grid. Their interactions involve some important functions like customer information systems, billing systems, meter data management systems as well as distribution management systems. In **Fig. 10**, we provide a simplified AMI, divided into 3 layers: the consumer layer, the metering layer and the communication layer and then we highlight how the main entities interface with the system. By dividing the AMI into multiple layers, each part can be considered as a subsystem. The attack surface and the vulnerabilities of each layer are identified and studied separately. At the consumer layer, the study will focus on the HAN (Home Area Network) by identifying the vulnerabilities related to the used wireless technologies, the gateways as well as the different interfaces. The security of the metering layer relates to the smart meters and their design, the study can be conducted on the serial ports and the used firmware. The network connecting the different equipment and the managements services is considered in the communication layer.

Based on the different layers, and the risk assessment associated with each one, the whole system security is checked during integration process as shown in Fig**. 11**.

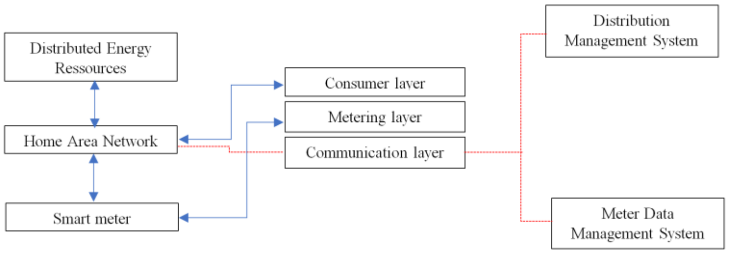

Distributed Energy Ressources
Home Area Network
Smart meter
Consumer layer
Metering layer
Communication layer
Distribution Management System
Meter Data Management System

Fig. 10. Simplified AMI

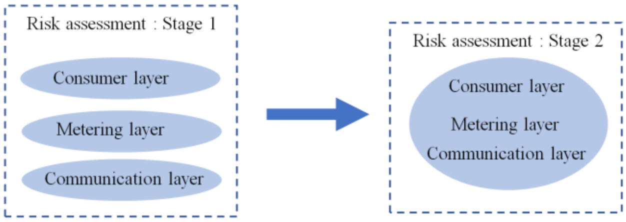


Fig. 11. A step by step risk assessment approach for the AMI

From a technical point of view, the security of the communication depends on the used technologies in the deployed nodes, the access networks, the used services as well as the field of use of the communicated data (**Table 4.).** This adds more complexity to the study and thus a need of a self-reinforcing lifecycle from the user all the way to the supplier at the operational phase as well as the design phase (Fig. 13).

Table 4. IoT architecture layers

Nodes technology	Access network	Services	Applications
ZigBee			Transport
6 LoWPAN	LAN	PaaS	Production
NFC	WLAN	SaaS	Smart buildings
RFID	Cellular network	IaaS	Electric vehicle charging
Bluetooth			

The risk assessment as discussed focuses on the security issues as well as privacy issues. The security is considered from attackers' perspective. The feared events are related to attack scenario where attackers get unauthorized access to the system and impact the data and system. The however is regarded both from an attack perspective as well as the regulatory stand point. In fact, privacy is regarded through the type, scale and content of the collected data. For instance, the collection, storage and sharing of user identifiable information is clearly studied and data collection is limited to the required information. Furthermore, the absolute necessity of anonymization of some data is identified and integrated into the design of the system.

We summarize in **Table 5** some classified security issues and vulnerabilities inspired from the NIST study which are worth considering in the different stages of the smart grid risk assessment [18]. These vulnerabilities allow an attacker to access the whole or part of the smart grid. By way of example, accessing a smart meter can have a huge impact on users' data privacy. The data collected from a smart meter can be used to discern the behaviour of the end users. By performing a data analysis, the attacker can tell whether a residence is occupied, how many people lives and if it uses an alarm system or not. These information, can be used for burglary, targeted advertisements or to spy companies' activity.

Table 5. Classified smart grid vulnerabilities

Security issues	Vulnerabilities
Public Information Availability	Non-restricted access to the smart meter Inadequate policy for logs management within the smart meters
Policy and Procedure Vulnerabilities	Large attack vector (smart meters, SCADA, PLC) Hard coded credentials within the smart meters Unlimited connection attempts to the smart meter Remote control of the smart me-ters through the AMI Low storage capacity of the smart meters
Platform Configuration Vulnerabilities	Simplified access to the smart meter (using the same password) Lack of integrity, allowing sniff-ing and injecting data Non-mutual authentication be-tween the nodes
Hardware vulnerabilities	Accessible physical ports Ease of physical access to the equipment
Platform Software Vulnerabilities	Weak security protection of the used services (ex: HTTP, FTP), due to the low storage capacity of the smart meters The use of simplified protocol stacks (vulnerable to denial of service attacks)
Network Communication Vulnerabilities	Exposure to Jamming attacks Weak authentication protocols Weak cryptography algorithms

5.2 A connected Yacht project (Smart-boat)

In the smart vehicle industry (Cars, boats, bikes…), vehicles are released with a certain degree of autonomy and remote access from manufacturers. In a specific case of smart boats tackled in one of our projects, risk assessments were conducted to identify the impacts of security attacks and data breaches of the end-users' data. The risk assessment is followed by penetration testing of the whole attack surface (Cloud, communication networks and APIs, mobile apps, hardware and firmware) to illustrate the feasibility of identified threat scenarios and impacts (**Fig. 13**). These tests were conducted using specific developed tools to address the context of smart-boats (e.g. communication protocols). The two resulted in a set of security controls and design rules that were integrated into the system throughout the development lifecycle. The set of security controls were checked over again in the following iteration of the product in the self-reinforcing development lifecycle.

Security and privacy capabilities are checked within each component of the yacht. After integrating the components to the yacht, another security process is performed as shown in **Fig. 12**.

On the one hand, the security analysis and testing of each component aims to identify the absolute vulnerabilities of the components. In this case, penetration tests are conducted on the entire attack surface of the single component (hardware, software, OS, application, network protocols, communication API, code…).

On the other hand, the security analysis and testing during the integration phase aims to reinforce of the study performed previously within the subsystems at the scale of the whole integrated system. This process allows one to handle the complexity and the interoperability of the several integrated components as well the security issues that might result. For instance, some identified vulnerabilities on the components are covered after the integration by other components. This the case of components that use cleartext protocols which are put in separate networks with enough security filtering of ingress traffic after the integration of the whole system. However, some security controls can be identified and should be added at the components level after the integration of the whole system. For instance, after connecting the local servers to the CAN network on the boat, additional controls for traffic filtering and access control were identified as needed at these different nodes of the network that are connected to the CAN network.

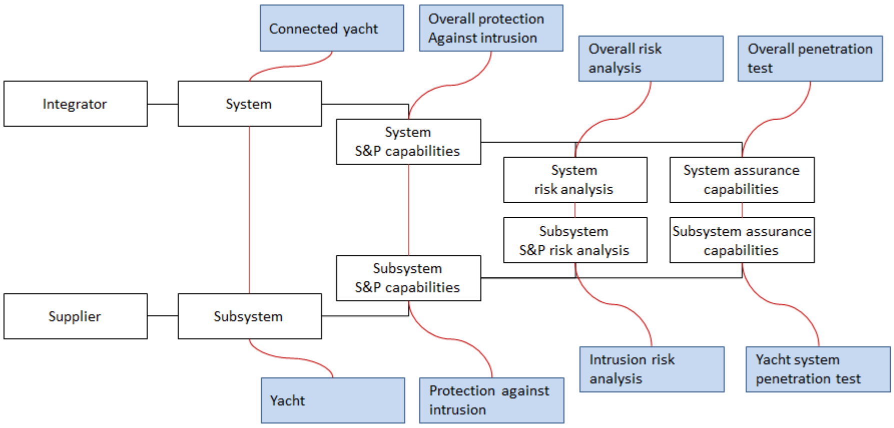

Connected yacht
Overall protection Against intrusion
Overall risk analysis
Overall penetration test
Integrator
System
System S&P capabilities
System risk analysis
System assurance capabilities
Subsystem S&P risk analysis
Subsystem assurance capabilities
Subsystem S&P capabilities
Supplier
Subsystem
Intrusion risk analysis
Yacht system penetration test
Yacht
Protection against intrusion

Fig. 12. Integrating yacht components with security and privacy capabilities to a yacht

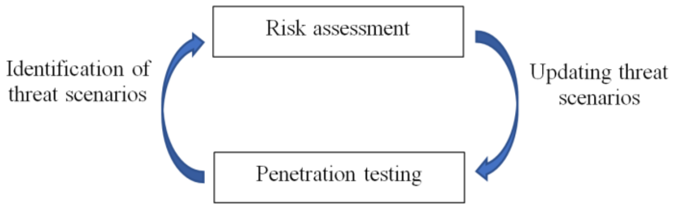


Fig. 13. Threat identification process

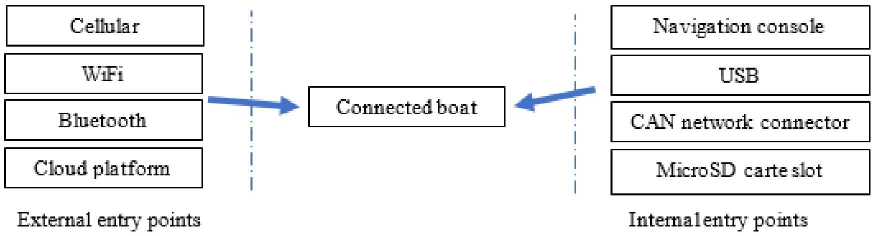
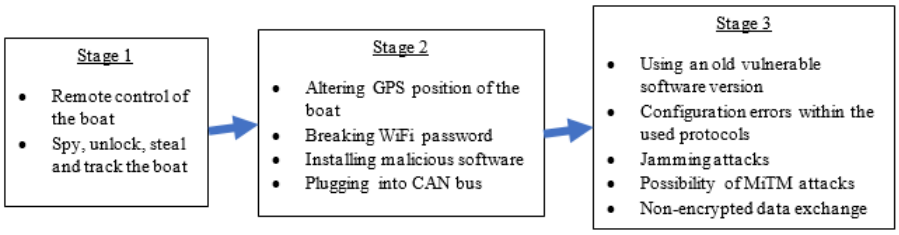


Fig. 14. Connected boat threats

We give in Fig.15 a general view of the technologies used in the boat while identifying the internal and the external entry points of the attack surface and then we show in Fig.7 an example of how the risk assessment evolves in the different stages of the study. The different scenarios are sometimes interconnected to form an attack tree. By integrating an equipment, the vulnerabilities can be identified through multiple stages, from a global to a more precise view, which allows to update continuously the model as the product moves through the lifecycle.



Stage 1

- Remote control of the boat
- Spy, unlock, steal and track the boat

Stage 2

- Altering GPS position of the boat
- Breaking WiFi password
- Installing malicious software
- Plugging into CAN bus

Stage 3

- Using an old vulnerable software version
- Configuration errors within the used protocols
- Jamming attacks
- Possibility of MiTM attacks
- Non-encrypted data exchange

Fig. 15. Risks identification at different stages

From the privacy perspective, the different types of collected data are reviewed. In fact, data related to the boat are stored locally and in cloud platforms and sent to manufacturer for predictive maintenance as well as remote access from users. The collected data can be seen as belonging to one of two classes: data related to the boat (engine statistics, location) and data related to the user (bookmarked locations, shared locations with other users…). The first class of data, even though not directly related to the user, can be tied to the user as ownership is clearly specified at the manufacturers level. The second class of data is clearly personal as each user is identified in the platform. In both cases, recommendation for data anonymization are introduced. For instance, the data collected by the manufacturers is only related to the boats and no ownership relationship is kept. The users are left in control of their data by explicitly asking for that data if needed or instructing the manufacturer to the predictive maintenance security control to ensure data privacy.

6 Conclusion

This paper has provided an analysis on how security and privacy should be taken into account by taking an ecosystem viewpoint. We have identified the following issues concerning a practice for the building and operation of IoT systems:

- it should integrate multiple concerns (security, privacy, safety);
- it should support assurance capabilities, in particular the use of penetration testing at different levels of integration;
- it should provide descriptions of interoperable security and privacy capabilities. **Fig. 9**, shows a possible approach based on a separation between applications and things: a security and privacy-by-design process is applied to the development of things; a description of interoperable security and privacy capabilities is then provided; these descriptions are used in a global security and privacy-by-design process applied to the development of applications.
- the relationships between stakeholders of an IoT ecosystem should be clarified, notably at the contractual level.

We recommend that further investigation takes place on those issues so that sufficient insight is gained on future practice for the building and operation of IoT systems.

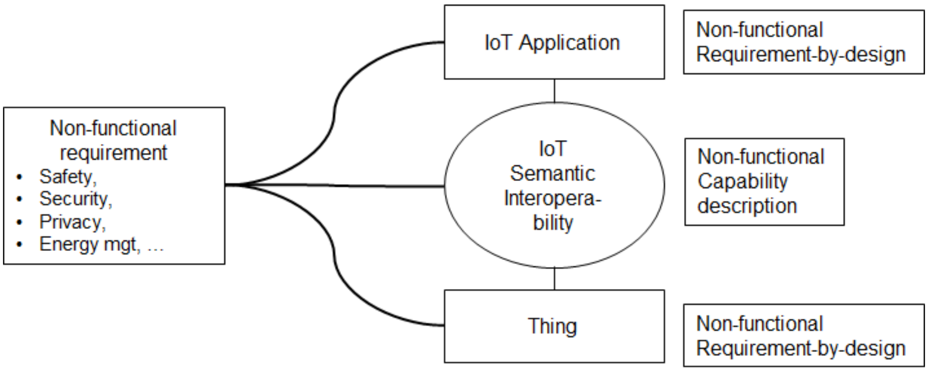

IoT Application
Non-functional Requirement-by-design
Non-functional requirement
• Safety,
• Security,
• Privacy,
• Energy mgt, …
IoT Semantic Interopera-bility
Non-functional Capability description
Thing
Non-functional Requirement-by-design

Fig. 16. Integration of Interoperability in the IoT

This paper is the result of a joint research work between Trialog and Coessi. The work from Trialog has also benefitted from contributions made in the FP7 PRIPARE [19], and H2020 Create-IoT support action [20] on security and privacy.

7 References

1. AIOTI public private partnership. https://www.aioti.eu/, last visited on 28.09.2017
2. Big data value association public private partnership. http://www.bdva.eu/, last visited on 28.09.2017
3. European Innovation Platform on Smart Cities and Communities. https://eu-smartcities.eu/content/citizen-centric-approach-data-privacy-design, last visited on 28.09.2017
4. IPEN wiki on privacy standards ipen.trialog.com, last visited on 28.09.2017
5. NIST Cybersecurity framework (2014). https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. last visited on 28.09.2017
6. General Data Protection Regulation: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf, last visited on 28.09.2017.
7. ISO/IEC 15288 - Systems and software engineering - System life cycle processes. https://www.iso.org/standard/63711.html, last visited on 28.09.2017.
8. ISO/IEC 27550 - security techniques - privacy engineering (under development). https://www.iso.org/standard/72024.html, last visited on 28.09.2017.
9. Privacy-by-Design. http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD, last visited on 28.09.2017.
10. Antonio Kung, PEARs: Privacy Enhancing Architectures. Annual Privacy Forum, May 21-22, 2014, Athens, Greece. Proceedings APF14 "Privacy Technologies and Policy". Lecture Notes in Computer Science Volume 8450, 2014, pp 18-29
11. Japp Henk Hoepman, Privacy design strategies. ICT Systems Security and Privacy Protection - 29th IFIP TC 11 Int.Conf, SEC 2014, Marrakech, Morocco
12. Antonio Kung, Johan-Christoph Freytag, and Frank Kargl, "Privacy-by-design in ITS applications. 2nd IEEE International Workshop on Data Security and Privacy in wireless Networks, June 20, 2011, Lucca, Italy.
13. Nicolás Notario, Alberto Crespo, Yod-Samuel Martín, Jose M. del Alamo, Daniel Le Métayer, Thibaud Antignac, Antonio Kung, Inga Kroener, David Wright. PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology. IEEE International Workshop on Privacy Engineering, May 21st, 2015, San Jose. http://ieee-security.org/TC/SPW2015/IWPEKung A. et al. (2017)
14. Antonio Kung, Frank Kargl, Santiago Suppan, Jorge Cuellar, Henrich C. Pöhls, Adam Kapovits, Nicolas Notario, Yod Samuel Martin. A Privacy Engineering Framework for the Internet of Things. In: Leenes R., van Brakel R., Gutwirth S., De Hert P. (eds) Data Protection and Privacy: (In)visibilities and Infrastructures. Law, Governance and Technology Series, vol 36. Springer.
15. NISTIR 8062 (Draft). Privacy Risk Management for Federal Information Systems. May 2015. http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf, last visited on 28.09.2017.

16. Marit Hansen, Meiko Jensen, Martin Rost. Protection Goals for Engineering Privacy. In 2015 International Workshop on Privacy Engineering (IWPE). http://ieee-security.org/TC/SPW2015/IWPE/2.pdf, last visited on 28.09.2017.
17. Ahmed Amokrane. Internet of Things: Security Issues, Challenges and Directions. C&ESAR 2016
18. V. Y. Pillitteri and T. L. Brewer/ Guidelines for Smart Grid Cybersecurity. IST Interagency/Internal Report (NISTIR) - 7628 Rev 1, Sep. 2014.
19. PRIPARE support action. http://pripareproject.eu/, last visited on 28.09.2017.
20. Create-IoT support action. https://european-iot-pilots.eu/project/create-iot/, last visited on 28.09.2017.