H2020 Work Programme 2014-2015

ICT-30-2015: Internet of Things and Platforms for Connected Smart Objects

Duration: 24 months

Supporting Internet of Things Activities on Innovation Ecosystems

H2020 – UNIFY-IoT Project

Deliverable 04.01

Report on the factors of user's acceptance framework and societal and education stakeholders

Revision :	**1.0**
Due date :	**30-06-2016 (m06)**
Actual submission date :	**12-07-2016**
Lead partner :	**INNO**

Dissemination level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Summary	
No and name	**D04.01 Report on the factors of user's acceptance framework and societal and education stakeholders**
Status	Released **Due** m06 **Date** 30-06-2016
Author(s)	S. Vallet Chevillard (inno), G. Guri (HIT), Ondine Freté (inno TSD), Fabrice Clari (inno TSD), Alex Gluhak (Digicat), Ovidiu Vermesan (SINTEF), Roy Bahr (SINTEF), Philippe Moretto (ETSI)
Editor	S. Vallet Chevillard (inno), G. Guri (HIT), O. Vermesan (SINTEF)
DoW	This deliverable is an outcome of task T4.1 (Framework for Users' Acceptance and Awareness): This task aimed at preparing the design and content of the educational platform by identifying the nature and type of content to be included as "framework of dimensions" relevant to promote IoT towards end-users and futures developers, adopters and promoters. That include the double aspects related to users' acceptance and education. The task are based on preliminary desk research and will be intensively and iteratively extended through interaction with IoT communities through dedicated working groups, as described in WP6. The main objectives of these tasks are to prepare a breeding ground to document education materials of various forms on the educational platform.
Comments	

Document history

V	Date	Author	Description
0.00	18-04-2016	Inno, HIT	Template/Initial version, outline
0.01	17-05-2016	Inno, Sophie Vallet-Chevillard, Ondine Freté	Section 3.4 Barriers for IoT adoption by the consumers
0.02	31-05-2016	HIT, Gert Guri	Section 4 State-of-the-Art of educational material
0.03	15-06-2016	DIGICAT, Alex Gluhak	Section 3.2 Barriers of adoption seen by EPI projects and Section 3.3 Barriers for a developer to adopt platform ecosystem
0.04	17-06-2016	HIT, Gert Guri	Conclusion and next steps / education
0.05	28-06-2016	HIT, Gert Guri	Section 5.2
0.06	28-06-2016	SINTEF, Ovidiu Vermesan	Section 3.5, 3.6
0.07	30-06-2016	SINTEF, Ovidiu Vermesan, Roy Bahr	Sections 3.5, 3.6 updates and review
0.08	30-6-2016	ETSI, Philippe Moretto, DIGICAT, Alex Gluhak, HIT, Gert Guri	Section 3.6, updates and revision, section 5.2
0.09	30-6-2016	Inno, Sophie Vallet Chevillard, Ondine Freté, Fabrice Clari	Final modifications
0.10	11-7-2016	ISMB Claudio Pastrone	Review
1.0	12-7-2016	Inno, Ondine Freté, HIT, Gert Guri, SINTEF, Ovidiu Vermesan, Roy Bahr	Final validation and release

Disclaimer

The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

The document reflects only the author's views and the EC is not liable for any use that may be made of the information contained therein.

Table of contents

1. Executive summary

1.1 Publishable summary

The UNIFY-IoT objectives are to stimulate the collaboration between IoT projects, between the different IoT platforms and support these in sustaining the IoT ecosystems developed by focusing on complementary actions, e.g., fostering and stimulating acceptance of IoT technology as well as the means to understand and overcome obstacles for deployment and value creation. In this respect, this document aims to report on the factors of user's IoT acceptance and on the offer of IoT education by highlighting the matrix between the barriers and needs for education and to pave the way to set up an IoT Open Education Platform. The work presented in this report is based on various sources: desk research undertaken by the project team with regards to the existing working groups in the European IoT community – the Alliance for Internet of Things Innovation (AIOTI) community, the IERC (WG01 of AIOTI) community and the IoT-European Platforms Initiative (IoT-EPI) – and feedbacks from the 7 Research and Innovation Action (RIA) projects and the IoT-EPI Task Force on education.

The section 3 of the document is entitled "Analysis of the factors of IoT acceptance" and starts with a summary of the key barriers of eco-system adoption identified by the 7 IoT-EPI RIA projects (3.2). According to them, common barriers perceived by the majority of the projects deal with the issues of trust in IoT ecosystems. The analysed barriers of IoT acceptance have been classified in three categories: Barriers for a developer to adopt platform ecosystem (3.3); Barriers for IoT adoption by the consumers (3.4); Barriers of a business for adoption of IoT solutions (3.5). As synthesis of these elements, a matrix of barriers identified has been set up (3.6) showing how the different kinds of stakeholders are impacted by the lack of trust, the need for adapted regulation, the market barriers and the interoperability issues. Some measures (already existing or in development) to jump over these barriers are presented at the end of the section, such as the creation of a trusted IoT label, the General Data Protection Regulation that will ensure stricter condition for giving a (informed) consent.

The following section (section 4) proposes an overview of specific education programmes and activities dedicated to various end users (consumers, developers, business) to support the deployment of IoT application and services. Higher Education Institutions (HEIs) are called to tailor their academic programmes to address new challenges and make the academic offer more attractive for students, since in the next 10 years there will globally be two million unfilled jobs related to IoT. The courses proposed by HEIs are very different from one institution to the other and depend also on the academic level (undergraduate, graduate, post-graduate…) Furthermore, beyond traditional IoT education programme offered by the Universities, a new alternative on IoT education is provided by commercial companies. Both HEI and commercial companies provide always more courses offered either on free online or on commercial platforms to answer the increasing demand for IoT courses. Considering the end users' needs (level of students, kind of professionals), course structure varies in terms of content, length and topics. This state-of-the-art of the education offer in IoT shows that the introduction of education courses for end-users offers a common positive development to HEIs, researchers/experts and companies as it support innovative solutions in the IoT but still lacks of coherence.

The aim of UNIFY-IoT is here to take stock of the good existing practices to address the barriers for IoT adoption and to support the community to address those challenges. In this respect, two perspectives are taken into account: supporting the RIA's in their development and the dissemination of their results to the IoT ecosystem. In order to achieve these goals, UNIFY-IoT will develop two complementary tools presented in section 5 and part of the IoT-EPI web

landscape: Bibl-IoT, shaped on the previous experience of the open-platforms, and the Open Education Platform (OEP). The first one will make good practices, reusable assets, use-cases available to IoT ecosystems for further use and development; it will provide the possibility to test online web-services and a virtual space where stakeholders (soft-developers, platform developers, architects) will be able to interact. The aim of the second platform is dedicated to IoT (future) end-users and linked to the need to increase the factors of acceptance of the IoT. The OEP is presented as an answer to the lack of comprehensive, coherent and standardized education offer on IoT by making available to all kinds of stakeholders courses, training material, as well as a match-making area. The OEP will not duplicate existing contents (e.g. HEI online courses) but act as both content repository and links directory. Both platforms will be developed and constantly improved during the project life based on the coordination with the RIAs and the recommendations that will be highlighted and drafted until the end of the project.

1.2 Non-publishable information

None.

2. INTRODUCTION

This document establishes a first analysis of the educational needs in IoT on both technical and non-technical aspects in order to build the grounds of the IoT Open Education Platform. More generally, the document aims at highlighting the matrix between the barriers and needs for education identified in the document and the “spaces” (to be understood as virtual space such as existing or under construction web portals or physical space such as existing working groups in the European IoT community including the IERC community, the AIOTI community and the IoT-EPI initiatives) where these issues are addressed and that can support the community in tackling them.

This document consists in a first step to structure an IoT education offer addressing the various kinds of stakeholders involved in IoT and to support IoT development beyond the barriers, impediments and constraints regularly emphasized by the community. The analyses provided have to be considered as the beginning of a process of coordination and animation of the communities in order to involve them in working and spreading their progresses, knowledge and good practices in tackling the barriers identified. It is thus not an end in itself and the framework proposed is supposed to evolve constantly and dynamically by the engagement of the IoT community.
The document is composed on three main parts:

- The first section reviews the factors of acceptance of IoT in order to emphasize the barriers for IoT adoption split by category of stakeholders. The current measures to address those barriers are quickly presented. Finally, a synthetic matrix summarising the identified barriers and the spaces where they are addressed is provided.
- The second section consists in a state-of-the-art of the current situation regarding the education offer in IoT. It provides the current trends and challenges to build a comprehensive IoT offer addressing the needs of the various stakeholders.
- Based on the two previous sections, the third section provides a proposition of the structure of the content for the open education platform. It has been intensively discussed in the community through the Education Task Force of the IoT-EPI that has been taken into account in the proposition.
- Finally, the last section provides some conclusions and recommendations to continue the work and presents the next steps.

In terms of methodology, the analyses presented in the document are based on a collective work and several interactions within the project and the community including desk research undertaken by the project team, analyses of a web questionnaire circulated among the partners of the IoT-EPI projects. The 7 RIAs projects participated in that survey and shared their view on their needs to adopt IoT platforms, their vision on the factors and barriers for IoT adoption and acceptance, and their perception of the needs for an IoT education offer. Moreover, the preparation of this document benefited from the support of the IoT-EPI Task Force on education where issues, challenges and the proposition for the structure and the content of the open education platform have been intensively discussed in several conference calls and in a workshop that took place in Valencia on the 22nd of June 2016.

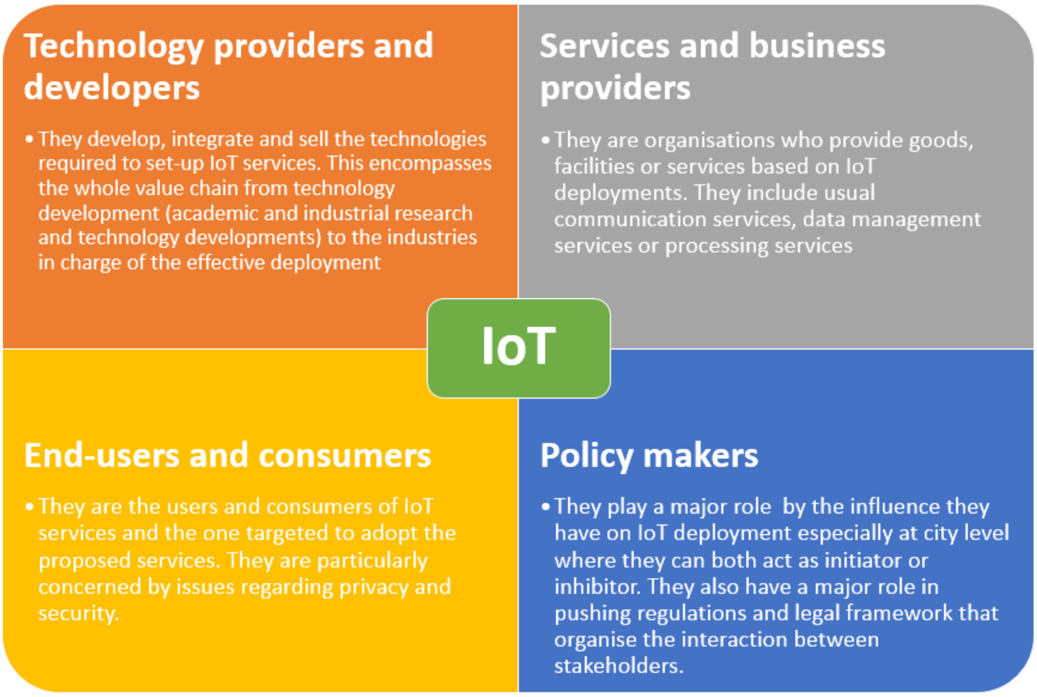
3. Analysis of the factors of IoT acceptance

3.1 Introduction

The purpose of this section is to identify the main concerns **that influence adoption and users' acceptance of IoT applications and services** in order to provide support to IoT stakeholders – such as manufacturers, developers, services providers, promoters, etc. – to address these barriers.

Data protection and privacy appear to be ones of the **main critical issues for the acceptance of IoT applications by the users**. A Eurobarometer on Data Protection published in June 2015 showed that only a minority (15%) feel they have a complete control over the information they provide online; 31% think they have no control over it at all. Furthermore, two-third of respondents are concerned about not having complete control over the information they provide online[1]. These results concern all ICT applications but are especially applicable in the field of IoT and are often further complicated due to:

- The **technical specificities of the IoT**: size of data set, complexity of data operation.
- The high **complexity of the IoT ecosystem**: physical objects, software, Internet infrastructure, behaviour of the final user, etc.
- The **variety of stakeholders involved**: product manufacturers, sensor manufacturers, software producers, infrastructure providers, data analytics companies and other actors involved in the supply of different services, final users.



Technology providers and developers

- They develop, integrate and sell the technologies required to set-up IoT services. This encompasses the whole value chain from technology development (academic and industrial research and technology developments) to the industries in charge of the effective deployment

Services and business providers

- They are organisations who provide goods, facilities or services based on IoT deployments. They include usual communication services, data management services or processing services

End-users and consumers

- They are the users and consumers of IoT services and the one targeted to adopt the proposed services. They are particularly concerned by issues regarding privacy and security.

Policy makers

- They play a major role by the influence they have on IoT deployment especially at city level where they can both act as initiator or inhibitor. They also have a major role in pushing regulations and legal framework that organise the interaction between stakeholders.

Figure 1: IoT stakeholders

Setting the right framework for the deployment and exploitation of the IoT potential in order to become a global leader in the field of IoT and to **increase the users' acceptance in Europe has become one the key priorities of the European Commission** these last years.

[1] Eurobarometer on Data protection, European Commission, 2015 http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf

In this respect and from a regulatory point of view, the Council and the Parliament have recently adopted, in April 2016, a new legislation called the **General Data Protection Regulation** (GDPR) which should **increase the trust of users in digital services and IoT by ensuring a higher protection of personal data** and introducing key changes for IoT users[2].

Any stakeholder participating in the IoT ecosystem could potentially have a share of liability. We propose to classify IoT stakeholders in 4 groups, as depicted in the Figure 1.

In the rest of the document, we present a synthetic view of those barriers with respect to each stakeholder, as the meaning and means to tackle them is different throughout the value chain. We also emphasise the barriers seen specifically by the IoT-EPI projects as they are the main target of the support of UNIFY-IoT (section 3.2). In the previous taxonomy, they are covering mainly the technology providers and developers.

3.2 Barriers of adoption seen by IoT-EPI projects

As part of the Innovation Task Force, UNIFY-IoT has conducted a survey to understand the major barriers for successful eco-system adoption that the IoT-EPI projects anticipate for the development of their project. The responses were diverse as the projects approach the IoT market from different angles; nevertheless, various common threads can be identified.

Table 1 captures a summary of seven IoT-EPI projects who provided responses. The detailed project responses can be found in the Appendix - Section 8.

Table 1: Key barriers of eco-system adoption seen by IoT-EPI projects

Project	Key barriers of eco-system adoption
AGILE	• Timing / speed to market • Lack of community traction • Lack of market confidence in EU project outcomes • Comms (informal communications) of value proposition to a diverse stakeholder audience & volatile market
BIG-IoT	• Legislation on sensor deployment in public, security and privacy, national differences • Lack of common semantic and inter-operability standards • Lack of investments to standardise BIG IoT model • Stimulating demand and supply on the IoT platform/marketplace • Availability of big volumes of open data
Inter-IoT	• Privacy, security and trust in cross-platform data sharing • Reliability of integrated systems of systems • Trust among integrated/federated platforms • Data sharing across heterogeneous systems and boundaries
SymbIoTe	• Lack of effective collaboration btw academia/research and commercial industry • Lack of willingness to federate platforms/services • Jungle of IoT standards • Closeness of IoT platforms (silos) • Privacy / trust concerns of end users

[2] General Data Protection Regulation, 2016 : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

TagITSmart	• Open comms between multiple project partners • Invention of new use cases on the platform • Engagement of consumers • Lack of accessibility of platform information
VICINITY	• Lack of cooperation between IoT end users • Reluctance of commercial players and vendors to support interoperability efforts • Regulatory barriers • Trust issues around provenance and authenticity of IoT data across different IoT platform boundaries
bIoTope	• Non maturity of Security/Privacy/Trust solutions in the IoT • Reluctance of industrial IoT players to support interoperability efforts • Lack (or slow evolution) of EU regulation about the data ownership from an end-user perspective • Lack of market confidence in EU project outcomes

According to the IoT-EPI project common barriers perceived by several projects are concerned with the **issues of trust in IoT ecosystems**. This includes both end user trust, in how potentially personal data may be handled to respect peoples' privacy, but also trust related to the provenance and authenticity of IoT data, if exchanged across different IoT platform ecosystems.

A further common barrier identified across IoT-EPI projects is the **heterogeneity and diversity of IoT standards and lack of alignment and interoperability** between them. Tackling this barrier is challenging as vendors may exploit the situation to force lock-in of the customer into their solutions and may resist effort co-operating towards more interoperability.

Inadequate legislative and regulatory environment is another common barrier highlighted by several projects. As the IoT is still an immature market that is rapidly growing, regulators currently lag behind the developments. Regulation is often addressed at the level of an individual country or within an economic region and the realisation may differ from each other. This makes it more difficult to develop solutions at scale that can be sold on a global market.

The current **immaturity of the IoT market** also poses challenges beyond regulatory aspects. In particular market development is a major issue, generating the demand and matching demand and supply side stakeholders and building out adequate value chain constellations between IoT vendors, developers and service providers to match the needs of the end users. Several projects are concerned with getting the right community traction and are concerned with how the value propositions of the platforms are adequately communicated to the right eco-system stakeholders without the causing more confusion on the crowded market.

3.3 Barriers for a developer to adopt platform ecosystem

IoT platforms are only as good as the service propositions they enable on top of them. Successful IoT platform ecosystems must attract sufficient developers, in order to ensure continuous service innovation around their platforms and to keep an advantage on the marketplace by using collective intelligence of an active developer community. The same applies even to IoT products such as smart watches, home gateways etc. In order to ensure product evolution and extensible functionalities, developer ecosystems are essential.

According to Vision Mobile [24], developers can enrich a IoT platform eco-system in different ways: 1) they can act as customers; 2) extend the own product offering; 3) enable more valuable end user data to be captured inside of IoT platforms; 4) help distributing the platform offering to new markets; 5) act as resellers by opening up new sales channels for an IoT platform ecosystems. Developers are important decision makers when it comes to fostering adoption of an IoT platform eco-system on the wider market.

Developers turn to an IoT platform to be able to deliver quicker and effortlessly products and services to market. However, there are various barriers that they face which ultimately impact the selection of a particular platform.

Market diversity: The current situation on the IoT platform market is likened to a wild west with new platforms appearing nearly on a daily basis and little structured information available about them. IoT Analytics has surveyed more than 360 IoT platform offerings on the market, one for each day of the year IoT Analytics[3]. There is unfortunately little information out there that adequately guides developers with the selection of a platform to make an informed decision about which platform to choose. Comparing existing offerings, even when only considering their features, takes a considerable amount of time. There is a lack of reliable platform benchmarking evidence or comparative studies, leaving developers with a dilemma of making an extensive upfront investment for a market analysis or to gamble on some IoT platforms after a superficial review of various IoT platform choices.

Market uncertainty: A developer is likely to spend a considerable amount of time and investment in developing a service/product offering on top of an IoT platform. Furthermore, once the service / product offering is operational and serves its client base it is expected to be operational for a significant amount of time. On the current IoT platform market there is a significant risk that some of these IoT platforms may not get enough traction and disappear very quickly from the market. This reliance on a third party platform can put a developer or service provider into a difficult position in case the third party disappears from the market or discontinues the support for the IoT platform. A developer may be forced to move to a different IoT platform and possibly migrate existing applications and services to the new platform, demanding considerable time and investments. This risk represents significant barrier for IoT developers, in particular those who rely on IoT platforms for commercial projects. As such IoT developers are more likely to consider platforms on the market provided by bigger players where there is enough confidence that their platform offering will exist for some time on the market or on open source solutions that are maintained by a larger developer community.

Market outreach: Another important element for IoT developers are the opportunities that an IoT platform eco-system may offer to reach a market for their developed service offerings. A major barrier is to find (paying) customers for the developed services and applications. Market development and sales is a major activity for most companies in the IoT space due to the immaturity of the market. Successful ecosystems in the mobile world such as app-stores (iTunes, Google Play) have proven to provide a platform to match the supply with a demand-side in an eco-system and provide monetisation capabilities to developers to extract revenue streams for their customers. Most IoT platforms are a far cry from offering such eco-system reach. Both Apple and Google are starting to push their existing mobile platform eco-system to become IoT eco-system in the consumer space in areas such as smart home and smart car. A successful IoT platform will not only provide useful technical features to developers but help solving some of the barriers in establishing market outreach and distribution of the developed IoT products and services.

[3] https://iot-analytics.com/product/list-of-360-iot-platform-companies/

Learning curve and development complexity: Once developers have identified a platform of choice that satisfies their requirements, a second barrier relates to the learning curve of becoming productive on top of the selected platform. This can be roughly broken down into how quickly developers can familiarise themselves with the development process and the ease and effectiveness of development process itself.

The learning curve usually is strongly influenced by the familiarity of the developer with the development language, the development environments and how intuitive the development tools are. It also depends on the level of support provided during the development process in terms of learning and training material etc. Tutorials, code examples and adequate API documentation can significantly lower the burden on the developers and remove friction in the IoT platform environment. The ease of development also depends on how well modularised functionalities are already available to developers and can be reused without the need of reinventing the wheel or developing modules from scratch.

In order to attract developers, it is important that IoT platforms actively help overcoming the above mentioned barriers and minimise friction for developers to become productive on top of them. A survey conducted by Vision Mobile [24] found that the three most important factors for developers for choosing an IoT platform are:

- Ease of use and development speed,
- Value for money and
- Technology familiarity.

These three factors appear more important than the features of an IoT platforms and more detailed technical characteristics. This is an important insight as many IoT platform providers try to differentiate in terms of novel features and technical capabilities instead minimising friction for developers.

3.4 Barriers for IoT adoption by the consumers

End-users are defined as the final users who ultimately use or are intended to ultimately use an IoT based application or service. They can thus be considered as the consumers of those applications and services, even if the business relationships are not necessarily based on a financial relationship and the term “consumers” is preferred to “customers”. Furthermore, they can also be companies, when IoT services and applications apply in a B-to-B context.

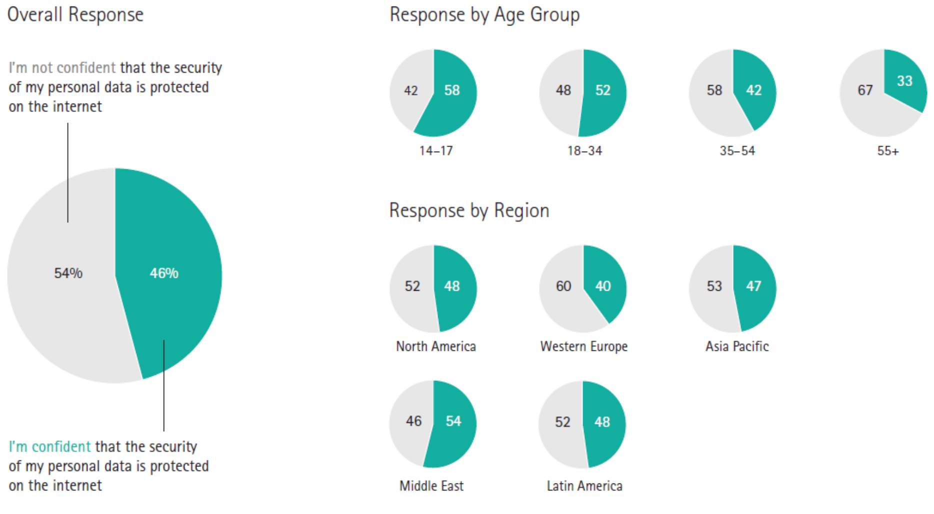
They represent a key success factor for the use of IoT applications and services and are at the heart of the issues related to:

- Lack of trust,
- Need for adapted regulation and legislation,
- Digital skills and competencies
- Market immaturity (from the beginning of the deployment process to the elaboration of the business model).

1/ Lack of trust: From the consumer’s side, the lack of trust towards developers and services providers in the IoT is due to the lack of control: “*What is happening with my data and who is controlling them?*” A survey related to digital trust in the IoT area highlighted the fact that the majority of the population worldwide (54%) is not confident that the security of his/her personal data is protected on the internet. This amount is even more important in Western Europe, as shown in Figure 2.

For the institutional stakeholders working in field of IoT, such as the European Commission or at a more technical level the AIOTI, the main challenge for the acceptance of IoT remains user’s trust. According to a recent Eurobarometer (IP/11/742), 70% of Europeans are concerned that their personal data may be misused[4].

In its Staff Working Document accompanying the Communication "Digitising European Industry[5], the Commission's services consider that "security, liability, privacy and data liability are critical challenges for the IoT" and that "ultimately trust will emerge as a derived characteristic".



Source: 2015 Accenture Digital Consumer Survey

Figure 2: Evaluation of the digital trust in the IoT are[6]

The main obstacles related to data protection are the following:

- There is insufficient usage of pseudonymised and anonymised data by those designing and developing IoT applications.
- Collected Data shall be adequate, relevant and not excessive: "Data Minimization". The principle also helps to setup the user contract, to fulfil the data storage regulation and enhance the "Trust" paradigm.
- Collector shall use data for explicit purpose: Data shall be collected for legitimate reasons and shall be deleted (or anonymized) as soon as data is no longer relevant.
- Collector shall protect data at communication level and protect collected data at data storage.
- Collector shall allow user to access / remove Personal Data: Personal Data may be considered as a property of the user.

Regarding issues in terms of privacy, the AIOTI alliance has identified 10 existing or potential privacy barriers that may constitute threats to the take-up of IoT across Europe, and which must be addressed. They are focused mainly on: "privacy engineering" and "privacy impact assessments". The main treats highlighted by the alliance[7] are:

- "Privacy Engineering", an integral component of a Privacy by design approach, is not yet embedded within the engineering community;

[4] Ibid.

[5] EU Commission, Staff Working Document accompanying the Communication "Digitising European Industry – Reaping the full benefits of a Digital Single Market" https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe

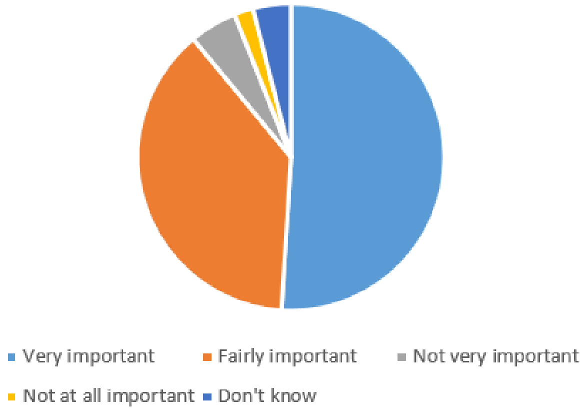
[6] Source : Accenture Digital Consumer Survey, 2015: https://www.accenture.com/t20160318T035041__w__/us-en/_acnmedia/Accenture/Conversion-Assets/LandingPage/Documents/3/Accenture-3-LT-3-Digital-Trust-IoT-Era.pdf

[7]https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

- There is no commonly applied framework for privacy risk that can be translated into engineering objectives to help companies implement their own privacy impact assessments;
- There is a lack of widely acknowledged and endorsed privacy engineering approach.

Moreover, the fragmentation of regulation and rights among countries is also perceived as a major threat. According to the EU Barometer, nine out of ten Europeans think that it is important for them to have the same rights and protection over their personal information, regardless of the country in which the public authority or private company offering the service is based.

To address the privacy and overcome this issue, the EU Commission has set up new initiatives on soft law and regulation (further details are reported in section 3.6).



How important or not is it for you to have the same rights and protections over your personal information regardless of the country in which the authority or private company offering the service is established?

Figure 3: Data protection at EU level[8]

The increase of acceptance of IoT by the end users is thus strongly linked with the privacy and data protection including communication and storage of personal data. Their expectation regarding data minimization, control and protection of personal data shall be ensured by adequate legislation.

2/ Need for adapted legislation and regulation: the regulation appears to be an essential step to strengthen the adoption of new technologies by end-users and facilitate business by simplifying rules for companies in the Digital Single Market. Currently the data protection is ensured at the EU level by the Directive 95/45/EC which is no longer adapted to the current needs and challenges of the digital age in terms of privacy and security of personal data.

Furthermore, the legislation doesn't ensure the transparency of the terms of contract. From the consumer's side, a gap appears between what a service is providing and the terms of contract he should agree with to use it. In particular, there is a lack of transparency regarding how to exercise a real consent for using the service.

The European Union is aware of the limitation of this directive and the Council and the Parliament have recently adopted, in April 2016, a new legislation called the **General Data Protection Regulation** (GDPR) which should **increase the trust of users in digital services and IoT by ensuring a higher protection of personal data** and introducing key changes for IoT users. The key principles of this regulation that is supposed to come into force in 2018 are briefly presented in the section 3.6. Even if such an initiative is definitively a good step in reinforcing users' rights and protection, the way the stakeholders will comply concretely is unclear for the moment and it will require supporting the developers and services providers.

[8] Ibid.

3/ Weakness of digital skills: In general, the IT industry is suffering from a skills gap in Europe which is even bigger in the field of IoT. This is linked to the normal time gap for adoption of new products/solutions due to user resistance towards new technologies. This is largely dependent on users' digital skills (disparities among different ages, countries, etc.) but there is clearly a need for more education and training of students, professionals, as well as citizens to harness the adoption of IoT application and services. End users typically do not possess the technical understanding or skill of the product designers: this is a fact that it is easy for designers to forget or overlook, leading to features with which the customer is dissatisfied.

4/ Immaturity of the market: The lack of value or benefits gained by using / experiencing a new IoT technology is relatively strong on this still "immature" market. The developers are not always fully aware of the disconnection between the service providers and the end-users. The IoT developers and providers have then a strong interest in the increase of users' trust. It is important to note that all IoT applications and services do not always answer the users' needs (answer a need vs. creating a need). The resistance to change is a natural reaction that can be overcome by using the concept of functional/experimental dimension. Within the innovation process of an IoT application, different kinds of values could be integrated in the business model and act as drivers of acceptance.

Drivers of acceptance rely on five main pillars where the "**functional value**" (i.e. the usefulness of a service) is only one of the pillars, as shown in the figure below:

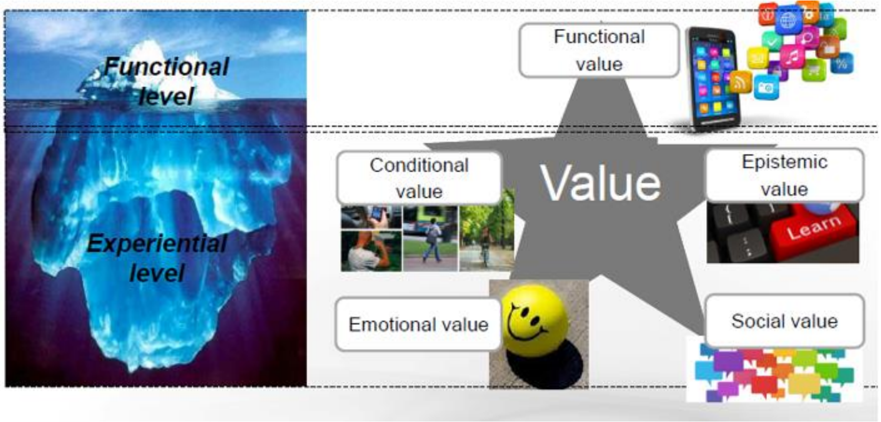


Figure 4: Drivers of acceptance – Source FP7 BUTLER project[9]

The experimental dimension of acceptance seems to be more and more relevant compared to the functional one.

It appears also that the functional value (i.e. composed by usefulness, ease of use and price of the technological innovation) is not the main variable to explain the acceptance or adoption of a technological innovation by consumers and users.

Other "drivers of acceptance" should be taken into account by IoT businesses, such as:

- **Social value**: is the influence of relevant others on the single user. The influence can come from family, friends, co-workers etc.
- **Epistemic value**: derives from the capability of the product to spur learning or curiosity in the user.
- **Emotional value**: is constituted by the emotions the tech product transmits to the user, such as happiness, pleasure etc.
- **Conditional value**: is the context in which the product is actually used, so the time, the place and the people with whom the user interact while using the product.

[9] BUTLER Project, "Users' feedbacks in Butler trials"

3.5 Barriers of a business for adoption of IoT solutions

In order to analyse the barriers for adoption of IoT solutions we have to consider that the stakeholders involved in IoT ecosystems and IoT use cases and applications have different roles, different business models and various positions in the value chain.

A stakeholder in an IoT value chain is any entity, group or organisation that has an interest in an IoT development activity, project or programme. This includes both intended beneficiaries and intermediaries, winners and losers, and those involved or excluded from decision-making processes in the value chain. IoT stakeholders include in the different IoT activities either primary stakeholders (i.e., stakeholders that are directly affected, and who expect to benefit from or be adversely affected by the IoT technology and applications deployments) or secondary stakeholders (stakeholders with intermediary role, i.e., citizens, trades unions, banks, local government, agencies, business service providers, etc.). Key stakeholders are those who can significantly influence the IoT technology and applications development and deployment.

When considering the barriers for adoption of IoT solutions it is important to identify/define the characteristics of key stakeholders, assess the manner in which they are affected by the IoT development/deployment outcome and understand the relations between them. This includes an assessment of the real or potential conflicts of interest and expectation for developing/deploying various IoT solutions in different industrial sectors and application domains.

In the context of IoT ecosystems including various stakeholders, the mapping of the stakeholders and the interactions among them will play an important role in addressing the potential barriers for adoption IoT solutions. The IoT stakeholder map can incorporate diverse set of stakeholders and uses IoT technology developments to indicate the direction of interactions between the organization and each of the stakeholders. These interactions are all direct transactions involving the organization and one other stakeholder involved in providing an IoT solution. The IoT deployments include as well indirect transactions that consider a network of stakeholders.

The IoT ecosystem' strategies detailing how networks are used in a positive and proactive fashion to address and remove the barriers for adoption of IoT solutions are not well developed as too few real large scale IoT deployments are available today.

To realize the expected impact and potential market for IoT, stakeholders will have to work together within the IoT ecosystem of infrastructure, hardware, software, and other vendors to develop solutions that have greater potential to drive significant business value for enterprises. Collaboration across the IoT ecosystem brings together a range of expertise and abilities required to create the IoT value chain and implement and deploy the technology and the IoT applications.

The potential value from IoT technology comes from moving beyond the proprietary technology silos that largely exist today. This is one of the potential barriers since new revenue may come from product and service innovations that enable growth beyond current products and market segments.

The IoT ecosystem design and development elements combined can help to coordinate, attract and mobilize a critical mass of participants. This is the first step required to unleash the network effects expected as the IoT evolves.

A requirement for the deployment of effective IoT solutions is sharing of data between large numbers of devices by using/adapting common standards for the interchange. The IoT business platforms need to provide solutions to assimilate data from multiple vendors and support open APIs across platforms. Building the IoT environment of the future requires taking into consideration issues such as openness, participation, accountability, effectiveness, coherence and offering innovative solutions for business platforms that enable self-governance, self-management, and context aware scalability.

Scoping out vulnerabilities and mitigating security risk is on the critical path of IoT. The privacy-aware consumer base opens up technology innovation in areas such as personalized privacy settings and context aware privacy and security.

The traditional value chain of the technology sector, where technology companies primarily sold to each other, is not a valid way to look at IoT deployment opportunities. New dynamic networks of connected products and people to drive the new information values are expected from intelligent device networking in IoT applications. One expects creation of IoT ecosystems that search for barriers to adoption and innovate on eliminating them rather than search for use cases in the white spaces. Solutions within the IoT ecosystem has to be created by addressing the challenges related to technology and deployment of IoT applications.

Significant barriers to deployment of IoT solutions are the relatively high costs, the regulatory barriers in different countries, market (economic) barriers, developer business model barriers, cross-cutting barriers and technology barriers. The European research community working together in the IERC activity chains classifies the barriers for adoption of IoT solutions into two main categories that comprises of technological and business/organisational factors.

Technological and business/organisational factors affecting the adoption of IoT solutions are given in Table 2 and Table 3.

Table 2: Technological factors affecting the adoption of IoT solutions

Barrier Factor	Description
Energy and power supply	In order for the IoT to reach its full potential, the edge devices included on the network need to become self-sustaining in terms of communication and supplying power. Reliable electricity to power the billions of IoT devices is a challenge as IoT is becoming a dominant market consideration, and these two functions internet connectivity and power are very important for autonomic edge devices. Battery density and battery life are important features and research advancements on lithium-air batteries and fuel cells can offer solutions in the future. Changing batteries regularly on billions of devices is challenging for future permanent IoT solutions and can be a barrier for large-scale IoT deployments. Wireless power including technologies that can transmit power at distance (up to meters) and energy harvesting technologies (vibrations, mechanical, light, airflow, etc.) can reduce the barriers for adoption.
Accuracy and Unambiguity	Accuracy and unambiguity of data considering the amount of data received is an important element in the adoption of IoT. It expected to have tools that can process the data at the edge (gateway devices designed for collecting and analysing data physically close to IoT edge devices) and in the Cloud, provide analytics and differentiate between the useful signal and the noise. One challenge is how to make real-time decisions and automate the real-time decisions in complex IoT applications.
Connectivity	The network bandwidth needed for connecting tens of billions of devices to the internet the need to be “always” connected is another IoT barrier to the large-scale deployments in many places. However, connectivity

	can be solved by investing to add more network capacity. One challenge however is how to get billions of different types of devices to communicate with each other seamlessly. This problem is related to interoperability challenges that are discussed in another section. At the device level, there are varieties of communication protocols that must be included within any IoT device to communicate with the maximum number of other devices. There are many protocols including Wi-Fi, Bluetooth low energy, ANT, ZigBee, RF4CE, LoRa, Sigfox and tens other smaller standards on the market. One challenge is how to select the protocols, which will influence how the device can communicate with other objects and could ultimately limit its adoption within the IoT. Highly specialised functions may only be available via proprietary solutions, immediately limiting the options open to the designer. In addition the various protocols have to be secure, robust, low-power, use worldwide available frequency spectrum, have optimum data rate, range and function in different environments. The connectivity challenge must be addressed and overcome in order to have widespread adoption of the IoT technology.
Interoperability	Today there are a lot of siloes of connectivity and it is difficult to get devices to work together without common standards. However, IoT stakeholders in the industrial sector do not replace their equipment to accommodate the IoT and want to combine the new IoT solutions with the legacy systems. In this context, the stakeholders are in stable and flexible connectivity stack that lets them combine and match the legacy sensors/actuators and back ends with the new IoT implementations depending on their requirements and specifications. In addition, for IoT, the number of platforms available is very large, which makes it difficult for stakeholders to find a common layer for connectivity. The same challenge comes when selecting among different operating systems.
Real-time data analytics technologies	For IoT applications the flow of data will vary both in volume and velocity from the edge devices to edge/fog/cloud infrastructure and then into the organization data systems. In this context, the stakeholders' lack of stream processing capabilities that are important for the collection, integration, analysis and visualization of data in real time is a major barrier to the IoT applications deployment and adoption.
IoT Platforms	An IoT Platform is an intelligent layer that connects the things to the network and abstract applications from the things in order to enable the development of services. The IoT platforms achieve a number of main objectives such as flexibility (being able to deploy things in different contexts), usability (being able to make the user experience easy) and productivity (enabling service creation in order to improve efficiency, but also enabling new service development). In the landscape of hundreds of IoT platforms available one barrier to large-scale adoption of IoT is the lack of an open technology platform to host, commercially manage, and securely deploy new IoT solutions. IoT is a combination of multiple technologies, heterogeneous communication solutions and devices, which requires a federation of platforms or a unifying platform for multiple products and protocols. This in turn requires an open platform to host and manage multiple devices from a multi-vendor perspective. From the interoperability prospective, it is required solutions for a universal developer interface to accommodate multiple platforms and to unify data into a single interface in order to lower the

	barriers for adopting the IoT technology. The concept of platform-as-a-service (PaaS) provides a platform that lets app developers create, deploy, and manage their web and IoT apps including a drag-and-drop developer interface to add common features and functions, which is used in some IoT applications. PaaS incorporates a development platform, a deployment platform, the back-end infrastructure and can have an app-building mechanism to easily connect devices. Such open multi-vendor and multi-platforms could lower the barriers for IoT adoption.
Privacy	In IoT applications, the edge devices are collecting/harvest enormous amounts of data, and exchange to analyse and inform the other devices and the humans involved about certain events and provide new services. In this context, the ownership of the data and what control various stakeholders in the IoT value chain have on how that data is shared and stored are relevant for the widespread adoption of IoT technologies, and for addressing data ownership, privacy and control of data. Privacy is interlinked with security and trust. Security breaches can be especially dangerous in many IoT applications. Security is considered one of the barrier elements to mass IoT adoption because a hacked/compromised device could put at risk personal data and once happened will compromise the reputation of the IoT deployment and reduce the trust in the IoT technology. The IoT technology end users, consumers and developers consider that IoT devices managing their personal data are not secure enough, there is a need for privacy assurances, privacy-by-design techniques, and IoT trusted label measures for accelerating the wide scale consumer adoption. The privacy assurances measures include providing information in a transparent manner on the nature of the data-collected by IoT devices, the controls and security measures that guard it. Providing global guidance on the design and operation of connected objects and recommendations for IoT devices design to be resilient to attack, use authenticated data, end-to-end encryption, token-based authentication, implement sensible access controls on the data collected, and offer a strong degree of user privacy will lower the barriers for IoT technologies and applications adoption.
Security	Privacy and control include disputes over legal ownership, storage and sharing of data, while security represents protection of that data outside the data paths. Hackers in the future can be physical persons, organizations or other intelligent devices that are part of the IoT applications and try to exploit critical vulnerabilities of an IoT application or platform. Today in the IoT development field there is a trade-off between cost and security features, with many IoT product pushed to market before adequate security is implemented. Stakeholders involved in designing and deploying industrial IoT applications are entering a new phase of development when industrial devices cannot be designed to be secured by isolation since these systems need to securely communicate to external networks. End-to-end security frameworks, security-by-design techniques that consider software security, embedded security and hardware-encrypted security are essential for the IoT deployment and adoption.
Trust	For IoT products, services, applications, solutions infrastructure and ecosystems, it is crucial that the society, its citizens and other (potential) customers and users have trust in what they use, buy, wish to enjoy or otherwise are connected to. In order to create a workable level of such

	trust and therewith-durable adoption, one will need to have comfort, the offer will need to be credible and usable. In that scope, concepts such as ethics, safety, accountability, security and privacy-by-design have to be widely spread from the early stages of development for IoT products, services, applications, solutions infrastructure and ecosystems. To enable large-scale deployments of IoT systems ensuring massive and durable user adoption, it will be essential that IoT and related IoT ecosystems be based on complementary architectures based on similar principles, enabling to leverage across multiple use cases and to catch the extra value arising from information exchange across multiple sectors / domains.
Standardisation and regulatory landscape	Regulatory compliance is an important driving factor behind IoT adoption. There is a lot of effort in the area of IoT standardisation but the landscape is still fragmented and more is needed in terms of security, privacy and IoT architecture. The competition between technology and telecoms groups for market domination of IoT is driving the development and ant the same time is increasingly fragmenting the market in many cases due to the prevalence of proprietary standards. One challenge for the IoT adoption is that there are very few IoT universal standards. Today, the IoT technology sector still is based on ad-hoc governance by the large companies. The IoT solutions include multiple standards, multiple solutions that are based on silo built platforms. To connect devices from multiple vendors, it is necessary to have a federation of IoT open platforms and unified open platforms to supports different protocols and standards. Many standards are already deployed for IoT applications such as Wi-Fi, Bluetooth, and ZigBee, LoRa, Sigfox, etc. However, the lack of coordination and the emergence of many new standards initiatives can create confusion and continue the fragmentation the IoT industry. The IoT technology adoption will be fuelled by the decreasing cost of hardware/sensors/actuators combined with the right integration of hardware, communication channels, the proper edge/fog/cloud computing, storage, big data analytics and right decision-making. Fragmented landscape of technology that is not interoperable delays IoT technology adoption since requires the stakeholders and end-users to make the right choice very early and make sure that is the winning technology. In this context, the may choices at different levels such as device architecture (ARM or x86), device OS (FreeRTOS, Linux, Android or Windows), programming languages, connectivity and discoverability framework (Zigbee, Z-wave, LoRa, Sigfox or AllJoyn), communication (Ethernet, Wi-Fi, LoRa, Sigfox EDGE or 3G), carrier (based on the communication selected), storage, IoT and analytics (ThingWorx, AWS, Azure, etc.) could be a barrier to the IoT adoption.
Customization of apps	The complexity of IoT solutions, the limited capabilities of different stakeholders to implement them, and the need for interoperability and customization, require from hardware, software, and service providers (technology providers, systems integrators, IoT platforms providers, etc.) to provide end-to-end IoT solutions to meet the various requirements and specifications for different use cases and applications. Open horizontal platforms, with federation capabilities that offer customization of apps for ensuring interoperability could be a solution. In this context, the stakeholders in the IoT value chains provide

	distinctive technology, distinctive data, software platforms, and complete solutions. At different levels of technology (technology stack), there is a division of value among various stakeholders.

Table 3: Business/organisational factors affecting the adoption of IoT solutions

Barrier Factor	Description
Multi-disciplinary approach	IoT is an enabling framework of technologies that connects devices, business tools, medical technology, robotics, manufacturing equipment, via the internet that requires a multi-disciplinary, multi-vendor approach. The adoption of IoT applications incorporate a multi-disciplinary, multi-vendor, open approach to facilitate development on the scale and scope needed to create a unified and practical approach to using multiple IoT devices. These requirements, at least in the first phase of IoT development requires close cooperation among the stakeholders in the ecosystems and IoT value chains and creates delays in the adoption of IoT technology.
IoT Business cases	On barrier for IoT adoption is the lack of clear stakeholders' commitment to up-front investment based on clear IoT business cases. An indicator of companies' financial commitment to IoT is their willingness to invest in acquisitions that could provide a shortcut in IoT-adoption, when internal capabilities do not allow it.
IoT Business models	IoT is facilitating new business models based on the real-time data acquired by billions of sensor nodes. These new trends push for development of advances sensor, nanoelectronics, computing, and network and cloud technologies and lead to value creation in utilities, energy, smart building technology, transportation and agriculture. Building and deployment of public IoT infrastructure with open APIs and underlying business models is an important element for reducing the barriers of IoT adoption. IoT business models no longer involve just one stakeholder, but comprises on highly dynamic networks of stakeholders and completely new value chains. In IoT applications data is generated and transmitted autonomously by smart devices/machines and the data is crossing company boundaries. New instruments are required if companies wish to pursue the conventional strategy of keeping the knowledge secret in order to protect their competitive advantage. New, regulated business models are necessary - the raw data that are generated may contain information that is valuable to third parties and companies may therefore wish to make a charge for sharing them. Innovative IoT business models require legal safeguards (predominantly in the shape of contracts) in order to ensure that the value added created is shared out fairly, e.g. through the use of dynamic real-time pricing models.
Risks associated with change	IoT start-ups change the dynamics of entire industrial sectors by redefining how to deliver the products, services and end-user experience. In this context, the main barrier to IoT adoption is the power to disrupt the companies' current business models and the risk avoidance associated with change. IoT is at the early stages of adoption, and companies experience that traditional governance structures that are effective for prioritizing mature business areas are preferred instead of new IoT business models.
Qualified IoT personnel and skills	A lack of IoT skills and knowledge among employees and management is one of the biggest obstacles to using the IoT more extensively. The adoption of IoT systems requires new skills and support for workers

	through new tasks, teach new skills, while monitoring performance. This has implications for companies (i.e. substantial gains in productivity), employees (new jobs, new tools, skills, more creative tasks, etc.), and regulators (i.e. need to be involved in establishing rules for use of personal data generated by IoT technologies in the workplace).
Employee resistance	Augmented-reality devices (i.e. electronic glasses) where employers can place computer-generated graphics in a worker's field of vision to provide real-time assistance in performing a task, such as making a machine adjustment can support the adoption of IoT technology and reduce the employees' resistance. Implementation can be more successful if there are clear and transparent benefits for workers as well as institutional trust in employers. Employees could trade off privacy if they can acquire new skills and find ways to perform their jobs better. To take advantage of the capabilities that augmented-reality devices provide in the workplace, companies will have to redesign business processes.
IoT Educational programs	The IoT technology has introduced the need for educational programs (i.e. hardware/software, IoT architectures, embedded and cyber-physical technologies, security, applications, etc.) that will prepare the new generation of users, developers and practitioners. In addition, the educational institutions need to actively incorporate IoT technology into learning, supporting the massive adoption of IoT technology in education so that the power of IoT can be realized and learning can become authentic and relevant through engagement of the participants in the learning process. IoT can support professional development for stakeholders who may adopt new learning models, as data about their practice is collected through participants' feedback, achievements, and video recordings.
Maturity of IoT Solutions	IoT technology is still not market ready and the immaturity of IoT technologies and services is a recurring discussion among the IoT stakeholders, which need to design considering this immaturity, while managing the risk for organizations exploiting the IoT.
Monetise the IoT solutions and expected benefits	Making money and achieving real benefits are still difficult to evaluate since only a relatively small number of stakeholders have deployed IoT technology in large-scale deployments. The integration of IoT system comprises heterogeneous tools, edge devices, security, database management system, middleware, APIs, analytics, visualization tools, etc. and involves many stakeholders in the IoT value chain and IoT ecosystem. In this context, sharing and monetising the benefits among various actors in the IoT value chain is still a challenge.
IoT Ecosystems	The quality of IoT data, the numerous IoT data sources provisioning, and the inherent need to generate semantic-driven business platforms, require enabling business-driven IoT ecosystems and the generation of functionalities for operating across multiple IoT architectures, platforms and business contexts. IoT ecosystems offer solutions comprising a large system beyond a platform and solve important technical challenges in the different verticals and across verticals. These IoT technology ecosystems are instrumental for the deployment of large-pilots and can easily be connected to or build upon the core IoT solutions for different applications in order to expand the system of use and allow new and even unanticipated IoT end uses. Stimulating the creation of IoT ecosystems comprising of stakeholders representing the IoT application

	value chain (i.e. components, chips, sensors, actuators, embedded processing and communication, system integration, middleware, architecture design, software, security, service provision, usage, test, etc.) by integrating the future generations of applications, devices, embedded systems and network technologies based on open platforms and standardised identifiers, protocols and architectures is of paramount importance for lowering the barriers for IoT adoption.
Cost of implementation and deploying	Another barrier for deployment of IoT applications is the cost. IoT solutions comprise different approaches such as designing IoT devices with a centralized cloud-based business model that can lead to a long period of expense without revenue. Edge computing can help IoT stakeholders to reduce the costs and make money. Using distributing data based on edge computing techniques allows the stakeholders to protect the date and pay only when is needed it, while the stakeholders can keep and control their own data.
Knowledge about IoT solutions	There are many experimental solutions in the IoT field, and companies are offering promote IoT-related products and services. For the end-user there is a lack of knowledge about IoT solutions and their and since the IoT technologies are so new implementing them can be challenging, time-consuming and risky. In this context many stakeholders are waiting to see best cases and best practices before taking decisions.
Infrastructure	Building IoT infrastructure is part of the business model of cloud providers like Amazon and Microsoft, mobile network providers like AT&T and Verizon, microprocessor companies like ARM and Intel. The IoT landscape is fragmented, and large companies are creating their own IoT ecosystem of partners. There is a risk of creating a world of Intranets of Things and anti-interoperability between the systems that form the architecture for this technology. This is a world of Platformia.
IoT workflows	IoT market is an emerging, which has not yet defined workflows for product, service and experience development. Today, there are few IoT reference implementations, which is challenging considering the variability of the data that is coming from heterogeneous edge devices or other sources. This is even more challenging in the industrial IoT where is needed to connect things that have not been connected before secure, at scale, and align with the legacy devices and the workflow at the manufacturing floor. The IoT landscape is fragmented with a multitude of IoT connectivity and solutions and more than 300 end-to-end IoT platforms available, which make the workflows ambiguous by not having a clear view on how data flows and how can integrate that data into the company workflow. IoT technology and data integration is a challenge since the IoT applications are based on connected devices where data is flowing continuously.
Government and public authorities, strategy, involvement and public policy.	Governments and public authorities play an important role in adoption of technology, like IoT. By creating legislation, clarifies issues such as ownership of data, privacy and security. A national and European policy that would address the adoption of IoT and the barriers for deployment can help accelerate the deployment of a disruptive technology such as IoT. Governments and public authorities own IoT adoption is a driver for IoT technology and creates a large demand for IoT applications. Governments run some of the largest organizations that can directly consume or benefit from IoT. Governments and public authorities adoption is important from an IoT adoption perspective.

Business adoption cycle	New disruptive IoT technology adoption follows the technology adoption life cycle, with the early majority of adopters coming only after the innovators and early adopters. IoT disruptive nature will affect the traditional business models of many businesses. In order to find the reference IoT implementations there is a need for IoT stakeholders to implement and test IoT solutions in prototypes and large-scale pilots.

3.6 Synthesis of barriers identified and current measures

This section proposes a framework of barriers as they have been identified in the previous sections. Most of them are already being addressed by the IoT community and we briefly summarise the current trends and development undertaken.

Based on the barriers identified previously, we retain 5 main categories of barriers:

1. Trust
2. Regulation and legislation
3. Skills and competencies
4. Market barriers
5. Interoperability.

(1) Trust is an important topic of the European IoT community. Several working groups are addressing this issue to support the community and in particular the cluster IERC and the alliance AIOTI through the WG3 "IoT Standardisation" and WG4 "Policy issues".

Among the current trends to address the issue of trust, an interesting idea brought by the European Commission consists in the development of **a trusted IoT Label**. As explained in the Staff Working Document[10], on 7 December 2015, the European Parliament and the EU Council of Ministers reached informal agreement on the Network and Information Security Directive ("NIS Directive") calling for cyber secure solutions in critical sectors. For emerging requirements, **operators using the IoT may wish to adopt the Trusted IoT label as a demonstration of compliance**, where relevant, to the NIS Directive's requirements.

More generally, the EC's services would be in favour of the development of this kind of label for consumer's products, providing transparency about different levels of privacy and security (such as the energy efficiency label).

(2) Regulation and Legislation are also addressed long since by the community and especially within the WG3 and 4 of the alliance AIOTI. The Alliance publishes regularly reports and papers that include policy recommendations[11] in order to assist the European Commission in the preparation of future IoT research agenda as well as innovation and standardisation policies.

The major recent advance in that topic is the adoption in April 2016 by the Council and the Parliament of a new legislation called the GDPR which shall apply from 25 May 2018[12]. It will replace the EU Data Protection Directive currently in force[13]. This regulation should **increase the trust of users in digital services and IoT by ensuring a higher protection of personal data** and introducing key changes for IoT end-users, such as:

- Right to be forgotten;
- Easier access to its own personal data;

[10] https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe

[11] Report available here: https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

[12] General Data Protection Regulation, 2016 : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[13] Directive 95/45/EC: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0045

- Right to transfer personal data from one service provider to another;
- Information about data breaches;
- Improved administrative and judicial remedies in cases of violations.

The GDPR should also incentivize businesses to innovate and develop new ideas, methods, and technologies for security and protection of personal data. Furthermore, the future regulation enacts the principle of "**data protection by design and by default**" which is strongly linked with the need for more privacy engineering.

The **privacy by design** approach could guarantee the privacy rights and therefore contribute to increase the user's trust, as well as the **privacy impact assessment**, the **informed consent**. The three topics are addressed in the GDPR as described below:

In this respect, the GDPR enacts the principle of "**data protection by design and by default**" in its Article 25:

Article 25, §1 : Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

For the Commission, another way to address the lack of privacy in the IoT is to further develop and elaborate a new Data Protection Impact assessment framework and guidance. The AIOTI considers this lack of transparency of usage of the data as one of the main obstacles for the end-users' acceptance of IoT applications and devices.

A good example of the principles of Privacy by Design put in practice in the field of the Internet of Things can be found in the **Privacy and Data Protection Impact Assessment Framework** for RFID Applications[14] created under the impulse of the European Commission[15].

Furthermore, the future GDPR the article 35 of the new GDPR[16] is dedicated to the Data protection impact assessment:

*Article 35, §1: Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, **the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data**. A single assessment may address a set of similar processing operations that present similar high risks.*

The regulation requires that the assessment shall contain at least:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes;

[14] http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf

[15] http://ec.europa.eu/digital-agenda/en/blog/the-privacy-and-data-protection-impact-assessment-framework-for-rfid-applications-a-defining-moment-in-the-modern-epic-of-co-regulation-in-ict#more-17

[16] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

- An assessment of the risks to the rights and freedoms of data subjects referred to in paragraph1;
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Another way to increase the users' acceptance towards IoT applications is to provide the "data subjects" and end users with the possibility to fully exercise their rights and to be "in control" of their personal data. But users are often not able to give adequate consent where this is required. Informing the user and keeping information available on the way private data are handled is a key component of the "informed consent" process. However, the actual legislation related to the informed consent and to the information that should be given to the users on privacy is weak.

In the GDPR the consent should be given by a **clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data** relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

Article 7, §1: Condition for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

(3) Skills and competencies are addressed through different working groups, mainly on behalf of the IERC via the activity chains AC01 and AC03. The issues addressed are mainly targeting the research community with a focus on open platforms and propose the repository and the working methods and structure to collect and maintain the results (open source software, documents, etc.).

The IERC activity chains AC01 on IoT Architecture approaches and open platforms and AC03 on IoT Results Exploitation are working on an inventory of components and results of the previous projects. The work is identifying and collecting information on the applications and pilots developed by different FP7 projects.

In this context, the purpose of the IoT Open Platform initiative[17] is to encourage development and industrial communities to leverage on existing achievements considering that no single solution / platform will answer all the needs and requirements of a fully deployed IoT. The aim is to provide a single place to document tangible assets without restriction depending on the license policies (i.e. GPL and AGPL licences are not compatible with the Eclipse Public Licence), establish liaisons/interactions with other projects and allow continuity from project to project in time. The

[17] www.open-platforms.eu

IoT Open Platform initiative will have links with IoT-EPI tools and apply IoT-EPI branding (see section 5.1).

The work aims to reduce the barriers of adoption of IoT technologies by evaluating, advising and supporting different scenarios for rapid deployment of research results around IoT.

This topic is at the heart of the IoT-EPI projects and supported by two Task Forces: the Task Force 05 (TF05) on education which aims at developing on open education platform (see section 5) and the Task Force 01 (TF01) on innovation. While the former focuses more broadly on skilling up an IoT workforce, the latter looks specifically at removing friction for innovation around the emerging IoT-EPI platforms. It aims to establish guidelines and best practice to minimize the learning curve for IoT developers and to recommend measures that IoT platform ecosystems should put in place in order to create a successful developer community.

More detailed information about the current situation of IoT education is presented in section 4.

(4) Market barriers are also considered as a burning issue and it address importantly the IoT-EPI projects through different Task Forces namely TF01, Task Force 03 on IoT accelerators (TF03) and Task Force 04 on IoT Business Models (TF04).

The users' acceptance of IoT products will strongly depend on the business' capacity to take into account the privacy issues. According to the AIOTI, these issues should be better integrated in the businesses. In this respect, the concept of "Privacy as Business Model" could clearly help to face the challenges listed below:

- Raising interest in privacy and trust issues within the companies' side;
- Not all companies place sufficient importance on privacy;
- Ignoring altogether the privacy requirements of end users and treating privacy only as legal burden can only be a losing strategy in the long run.

The Concept of Privacy as Business Model has been – for example – used in the FP7 BUTLER project[18], a large IP project focused on enabling the development of secure and smart life assistant IoT applications studied in depth the potential and ethical privacy implications of the Internet of Things[19].

Privacy as business models constitutes an interesting way to increase the consumers' adoption of IoT by using the privacy engineering.

But other aspects have to be taken into account from the companies' side. The benefits of IoT technologies are distributed on how much IoT value is created in business-to-business vs. consumer markets, and which stakeholders in the value chain capture the most value from IoT applications. IoT ecosystems communicating with each other increase the value of IoT applications. IoT policy measures encourage increased development and deployment of IoT technologies and practices in the various sectors by providing best practice implementation examples and launching large-scale projects to demonstrate the benefits of the various solutions. The figure 5 gives an example of a possible win-win scenario in creating value at ecosystem level.

Creating different **value chain/network scenarios** and defining the most relevant segments for **value creation**

Analysing Revenue models and revenue streams between different actors

Identifying stakeholders and **potential cooperation partners** along the value chain (esp. to meet the needs of SMEs)

Figure 5: Reliable revenue streams between all relevant actors of the value network (win-win situation)

(5) Interoperability

The interconnection of smart devices, sensors, and actuators exposing data services, control functions and analytics presents opportunities for novel applications and new ways of thinking about the links between the physical and virtual worlds. Realization of these possibilities requires new levels of interoperability.

In today’s world, interoperability often refers to scenarios in which devices and subsystems from different vendors implement the same set of use-cases within the confines of a bounded domain (a silo). In these cases, services, service options, data models, security models and often technologies are mostly statically defined.

In an IoT world (as it is envisioned) there are no silos and significant emphasis is put on creating new value through cross-domain interactions. For example, your car navigation system could talk to the local city information system to locate the nearest parking possibility.

These simple interactions between devices and services commonly used in daily life yield intuitive and immediate benefits. However, an ability to successfully execute such ad-hoc, cross-domain interactions raises significant interoperability challenges: How does your car navigation system discover the city information services, understand how to invoke them, and correctly interpret the responses?

In 2008, the Gridwise Architecture Council published an Interoperability Context-Setting Framework, as depicted in figure 6[20].

According to Gridwise, interoperability incorporates the following characteristics:

- Exchange of meaningful, actionable information between two or more systems across organizational boundaries
- A shared understanding of the exchanged information
- An agreed expectation for the response to the information exchange
- A requisite quality of service: reliability, fidelity, and security.

Technical Interoperability has been the focus of standards organizations, alliances and consortia for many years and consequently strategies, standards and implementations supporting this level of interoperability are generally available. Strategies for Informational Interoperability, however,

[20] http://www.gridwiseac.org/pdfs/interopframework_v1_1.pdf

which includes the whole area of semantic interoperability, are less mature. One of the next steps required in unlocking the value of IoT is to address key challenges in these areas.

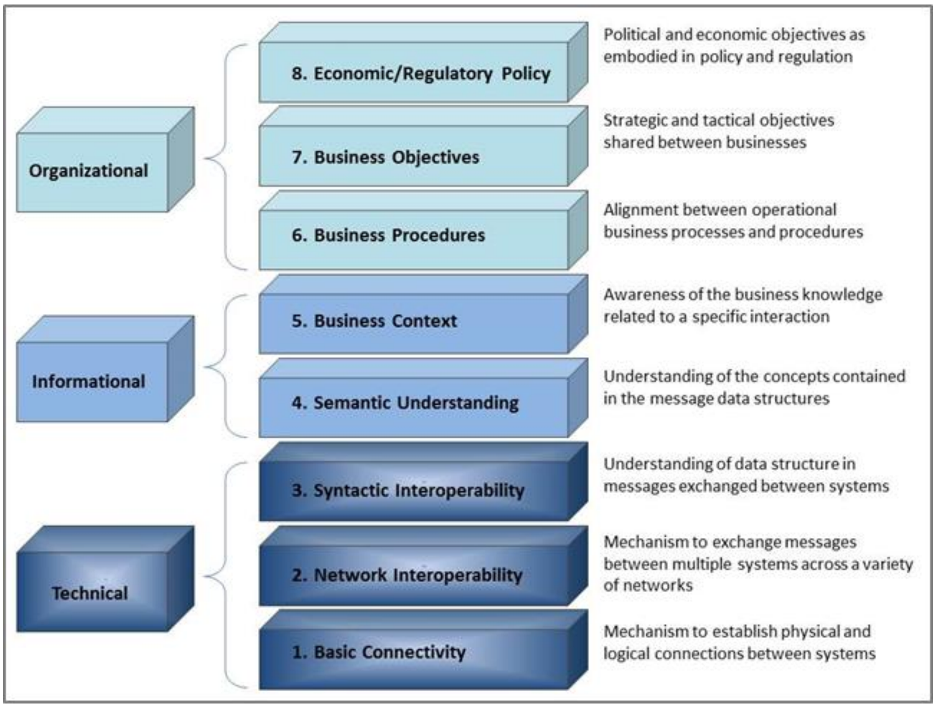

Organizational
Informational
Technical
8. Economic/Regulatory Policy
7. Business Objectives
6. Business Procedures
5. Business Context
4. Semantic Understanding
3. Syntactic Interoperability
2. Network Interoperability
1. Basic Connectivity
Political and economic objectives as embodied in policy and regulation
Strategic and tactical objectives shared between businesses
Alignment between operational business processes and procedures
Awareness of the business knowledge related to a specific interaction
Understanding of the concepts contained in the message data structures
Understanding of data structure in messages exchanged between systems
Mechanism to exchange messages between multiple systems across a variety of networks
Mechanism to establish physical and logical connections between systems

Figure 6: Gridwise Interoperability Context-Setting Framework

In this context, EU ecosystem tries and addresses platform-to-platform integration by open IoT platforms that support multiple applications, devices, and networks.

IERC partners consider that there is a need to make a particular effort on the IoT Architectures, define which are the future developments on Architecture Reference Model (ARM), revisit the existing IoT Architectures activities and provide an overview and estimation of the current IoT Architecture discussions.

The work is linked with activities of the AIOTI WG03 and IoT-EPI Task Force 02 on Platforms Interoperability (TF02) in order to provide recommendations with regard to gaps, issues facing IoT architectures and challenges for IoT technology deployment.

The IERC will work for providing the framework for the convergence of the IoT architecture approaches considering the vertical definition of the architectural layers end-to-end security and horizontal interoperability. IoT technology is deployed globally, and supporting the activities for common unified reference architecture would increase the coherence between various IoT platforms.

A common architectural approach requires focusing on the reference model, specifications, requirements, features and functionality. In particular, this issue would be important in preparation of the future large-scale pilots, although time schedule might be difficult to synchronise.

These issues are addressed in cooperation with AIOTI WG03 and IoT-EPI TF02 to initiate discussions with the Standards Developing Organizations (SDOs) working groups addressing the IoT reference architecture in order to provide a common framework convergence towards a common approach.

The matrix below gives a synthetic view of the barriers identified by distinguishing them towards the concerned stakeholders.

Table 4: Matrix of barriers identified by stakeholders

Category	Stakeholders concerned	Description
TRUST	**Data protection**	
	Services providers	***Towards techno providers and developers (including platforms)*** • Trust related to communication and storage of data • Trust related to the provenance and authenticity of IoT Data ***Towards regulators*** • To comply with legal framework
	End-users	***Towards developers and services providers*** • Trust related to communication and storage of (personal) data
	Privacy	
	Services providers	***Towards policy makers (regulators)*** • To comply with legal framework
	End-users	• Trust regarding the usage of personal data • Expectations regarding data minimization, control of personal data, etc.
	Working staff	*IERC, AIOTI (WG03, WG04)*
REGULATION AND LEGLISATION	***Techno providers, Developers and services providers***	***Pushed by policy makers*** • Lack of harmonisation between countries (fragmented legal framework) • Ex of smart metering
	Users	• Lack of protection of privacy and security of personal data
	Working staff	*AIOTI (WG3 & WG4)*
SKILLS AND COMPETENCIES	***Developers***	• **Basic Skills**: development language, development environment, etc. • **Specific skills** on IoT platform environment (e.g. API)
	Users	• Digital skills
	Working staff	*IoT-EPI task forces (TF05, TF01), IERC (AC01, AC03)*
MARKET BARRIERS	**Market fragmentation**	
	Developers and services providers	***Towards IoT technology providers*** • Choice of too many IoT platforms and lack of clear communication (benchmarking capacity) • Too many ecosystems and lack of alignments between them
	Business models	
	Developers and services providers	***Towards IoT technology providers*** • Risk of lack of sustainability of platforms ***Toward consumers (end users)*** • Immaturity of the market (is there a demand willing to pay the services and app developed?) • Lack of evidence base of working business models
	Users	***Towards services providers*** • Immaturity of the market

		• Lack of value / benefits • Lack of understanding of business models
	Working staff	*IoT-EPI task forces (*TF01, TF03, TF04*)*
INTEROPERABILITY	***Developers and services providers***	***Towards technology providers*** • Heterogeneity and diversity of IoT standards and lack of alignment and interoperability
	Working staff	*IoT-EPI task forces (*TF02*), AIOTI (WG03)*

4. STATE-OF-THE-ART OF EDUCATIONAL MATERIAL

4.1 Introduction

The challenges of education offer in IoT are multi-layered and complex.[21]

In the recent years, IoT has developed from a futuristic vision into a reality with clear market potential. **Referring to a firm-based questionnaire in 2015, by 2018, 95% of the companies will be employing IoT in one form or another**.[22] The emergence of IoT represents a shift in traditional courses and demands re-thinking of the academic offer in general. Three main changes can be considered:

1. the emergence of new jobs requires new skills;
2. more people demand IoT education;
3. consumers are becoming producers and consequently need to be educated[23].

Hence, the IoT future development depends on the education of its stakeholders.

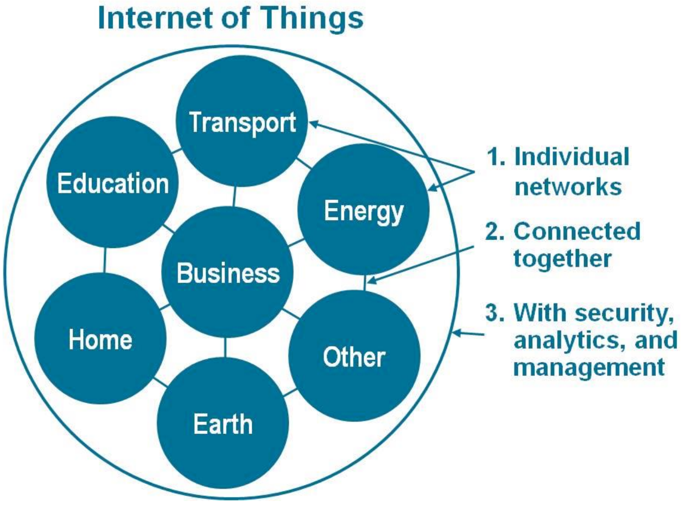


Figure 7: IoT network. Source: Cisco IBSG, April 2011

Higher Education Institutions (HEIs) are called to tailor their academic programmes to address these challenges and to make the academic offer more attractive for students, since in the next 10 years there will globally be two million unfilled jobs related to IoT.[24]

Hence, HEIs have to match the growing need for IoT talents by providing students with an investigative learning experience and hands in exposure[25].

To address these urgent needs there is an increasing number of short-term courses offered on specific IoT components, while the majority of them are offered online by both HEI and e-platforms. The latters in some cases are supported by business companies interested in IoT education either for their staff or their customers.

[21] There are several other definitions of the IoT, which you can come across in the education programmes such as: Industrial Internet, Internet of Everything, or Industry 4.0. In this document all these different definitions are considered under the umbrella of the IoT.

[22] http://www.ptc.com/news/2015/over-200-colleges-offer-iot-academic-program

[23] Kortuem, Gerd; Bandara, Arosha; Smith, Neil; Richards, Michael and Petre, Marian (2013). Educating the Internet-of-Things generation. Computer, 46(2) pp. 53–61.

[24] World Bank 2015. ICT for Greater Development. http://siteresources.worldbank.org/extinformationandcommunicationandtechnologies/Resources/WBG_ICT_Strategy-2012.pdf

[25] http://www.ptc.com/news/2015/over-200-colleges-offer-iot-academic-program

However there is not yet a well-established approach on how IoT applications will develop and be deployed relative to Research and Innovation.[26] Hence, it would be useful to complement the academic offer in the IoT with components related to innovation, providing a T-shape methodology[27] to appropriately connect research and business opportunities.

This document sketches, without claiming to be exhaustive, the academic offer in IoT, its characteristics, level of progress and a number of recommendations. To mirror the above mentioned developments in IoT education, the document is organized in five main sections: 1) specific dedicated education programmes/courses/activities on IoT (including undergraduate and graduate courses); 2) open online and commercial courses/platforms in education offer; 3) dedicated IoT courses for professionals; 4) degree of T-shape approach implementation in IoT education; 5) Teaching end-users/customers on IoT technologies;

4.2 Specific dedicated education programmes/courses/activities on IoT

The duality between needs/opportunities of the IoT experts on the one hand and the relative young age of this academic branch has caused an increasing pressure upon HEIs to start tailoring specific programmes dedicated to IoT. Drafting an academic offer though is not, according to most universities, an easy exercise, considering that it requires the connection of the physical world and digital world: information and communication engineering is the basis for IoT construction, while instrument science and technology is needed to manufacture physical devices for IoT implementation.[28] Moreover, embedded devices and technologies require an understanding of both hardware and software in a multidisciplinary approach, which is not present in most of the undergraduate programmes. In this way, more than a specific academic offer, **the IoT is considered a specialization in multiple disciplines** of students who already have either ICT or technological background.

The second challenge is that of setting an IoT as an independent major course for undergraduate students, since they need to master a range of common basic courses (either on ICT or technologies) prior to be introduced on IoT modules[29]. So the inadequate use of a multidisciplinary approach and insufficient knowledge of students at the start of the BSc studies seem to constitute two causes of a still limited and un-coordinated IoT education offer at the undergraduate level.

To match the quickly increasing variety of IoT clusters with specialized students in an ad-hoc approach and a limited strategic vision, HEIs have been launching in the last years different undergraduate programmes in IoT. However, this un-harmonized strategy has currently caused a further fragmentation and diversification of the current education offer, creating difficulties in establishing a standardized curriculum and training materials for an IoT major.

In response to these challenges, various universities especially in the UK and the USA have started creating majors only after 2010, a programme of re-thinking computer science education by offering a new introductory course designed around IoT concepts[30]. Universities have already

[26] Vermesan. O and P.Freiss. 2014. *Internet of Things-From Research and Innovation to Market Deployment*, River Publisher, Denmark

[27] https://mitprofessionalx.mit.edu/courses/course-v1:MITProfessionalX+IOTx+2016_T1/about; https://www.conted.ox.ac.uk/h600-72; http://axelta.com/AxOnlineIOTBootcamps.php

[28] http://onlinelibrary.wiley.com/doi/10.1002/dac.2373/full

[29] In China alone were newly launched 140 undergraduate majors on IoT in 2011.

[30] For a more detailed overview see the MIT, Open University in the UK, https://mitprofessionalx.mit.edu/courses/course-v1:MITProfessionalX+IOTx+2016_T1/about (accessed on February 2016)

started to revamp their courses in order to teach IoT at the core of the first year BSc curriculum so to increase students' awareness from the very beginning concerning the future changes in society and technology[31]. The courses focus on the importance of providing the broader concept of the IoT by merging physical and digital components introducing in this way a multidisciplinary approach since students possess either ICT or technological background. In other courses, students follow a more hands-on approach and are exposed to application examples from different aspects including IoT technologies, solutions and design in a methodological framework, which tends to inspire new ideas. Most of the education programmes focus on some of the fundamental concepts regarding the IoT such as: the merging of the physical and digital realms; increasing numbers of Internet connected devices from end-users including objects, sensors and actuators; the embedded device platforms and the appropriate use of a growing amount of data in terms of new applications related to vital sectors such as energy, transport and health[32].

Beyond hands-on teaching practices, the new undergraduate IoT courses focus on promoting an innovative and business oriented mind-set of students assessing the increasing market opportunities in the IoT applications[33]. The vertical technical knowledge is harmonized with horizontal soft-skills focused on market needs and innovation oriented modules. In this way, thanks also to the IoT interdisciplinary and market oriented nature, HEIs are increasingly promoting a T-shape approach in the undergraduate technical courses in general and the IoT in particular. The IoT undergraduate courses combine traditional engineering with a high-tech outlook: so electronic engineering is harmonized with Internet technologies, sensor devices, wireless communications, industrial design, software development and cloud computing in addressing concrete challenges and use-cases. An overview of the education programmes/courses shows that the principal IoT programming languages used are: *Assembler; C; Go; Rust; Python; JavaScript; C++*.

Other HEIs include the research community in building the features of the undergraduate IoT studies. The bottom line of this approach stands on the fact that IoT is a combination of other ICT and technology domains and in rapid development. Therefore, the IoT research groups of various universities are asked to bring their expertise concerning the state of the art of the research and help the academic team to set the priorities in terms of actual subjects of interests in IoT. In some universities are established even multidisciplinary research teams in IoT in order to achieve a twofold objective: a) being active and complementary in the IoT research by exploiting the diversity of researchers' backgrounds; b) help academics to provide a more encompassing academic offer to students[34]. Increasingly, academic courses are including in IoT frameworks the aspects of always connected devices and sensors in a sophisticated cloud infrastructure as a potential opportunity to boost new services. The purpose is to prepare students to be able to address the coming generation of connected things and the business opportunities it makes available.

Departments offering the IoT courses at the undergraduate and post-graduate level are different in various HEIs. This depends predominantly on the department, which is closer connected to IoT subjects such as the embedded systems, electronic systems, computing, departments which have developed an interdisciplinary approach to address in a more appropriate way the IoT applications.

[31] Kortuem, Gerd; Bandara, Arosha; Smith, Neil; Richards, Michael and Petre, Marian (2013). Educating the Internet-of-Things generation. Computer, 46(2) p.56.

[32] ibid.

[33] See for instance the 4-year undergraduate programme on IoT offered by the James Cook University in Australia https://www.jcu.edu.au/courses-and-study/courses/bachelor-of-engineering-honours-in-electronic-systems-and-internet-of-things

[34] See for example the multidisciplinary research teams belonging to the Waterford Institute of Technology https://www.wit.ie/courses/type/science/department_of_computing_maths_physics/bsc-hons-in-the-internet-of-things#tab=description

In some cases departments are established entirely dedicated to create the IoT education offer[35]. While at the undergraduate level the IoT courses have to be adopted, shaped or even oriented towards the already existing core majors, at the postgraduate level, the IoT programmes can be a product of more than one department. Beyond, avoiding the need to be channelled in one specific major, the participation of different departments in the post-graduate programmes ensures a multidisciplinary approach, crucial for the IoT encompassing nature.

In terms of graduate studies, setting the IoT as a major is more frequent as these students master the common basic knowledge so that they could receive specialization on one or more IoT pillars. Concerning the postgraduate programmes, most of the European universities do offer a master on IoT. There is an increasing pressure from stakeholders (companies and research institutes among others) for students with IoT background. The quickly increasing number of post-graduate programmes - more than doubled in the period 2010-2015 – is also the result of a less effort demanded to introduce IoT at the postgraduate level: thanks to less regulated institutional framework and more flexibility in setting the programmes to address current needs. Differently from the challenges mentioned above when reviewing the IoT undergraduate programmes, setting the post-graduate IoT programmes is relatively less challenging in terms of academic offer since the students have already the knowledge on both hardware and software components. Students are even familiar with IoT hardware platforms and can employ the latter for rapid prototyping, while the most frequently used are: *Arduino Yun; Arduino Uno; TinyDuino; Raspberry Pi; Beaglebone Black; Intel Edison; Pinoccio; WeIO; Libelium Wasmote; SIGFOX ; LoRa; Weightless; Axoloti; R-IoT microboard; DaDa machines; and Sam labs*. Therefore, students are capable of making the next step of connecting technologies and ICT. Furthermore, institutionally speaking, there are fewer obstacles in putting together a post-graduate rather than an undergraduate programme. The earlier allows also to be more specific on crucial issues, to involve industrial and/or research partners and to be more tailored towards the labour market needs and technological opportunities. Principally, the post-graduate programmes are a joint venture of various departments, which have been traditionally offering core courses on ICT and/or technologies. The characteristic of post-graduate programmes to be oriented towards an academic multidisciplinary approach is key enabler for a comprehensive IoT academic programme. Multidisciplinary approach, many scholars argue, it's fundamental in the case of the IoT and that's why it's inappropriate to regard the IoT as yet another major in terms of methodological approach. IoT has to be studied in a three dimensional model where ICT and technology are harmonized with the social layer, which will play an increasingly important role in shaping the IoT future.[36] In addition, postgraduate programmes can also benefit from international complementarities and financial support, especially in the Horizon 2020 framework, where comparative advantages of consortium partners and financial support are good basis for a well-crafted competitive IoT postgraduate programme. However, in terms of segmentation and availability of post-graduate programmes in IoT, there is still room for improving coordination among HEIs, in particular way with the United States and Australia, which are increasingly investing and promoting IoT education programmes at all levels.

Beyond the traditional IoT education programme offered by the Universities, a new alternative on IoT education is provided by commercial companies, which, alone or in cooperation with HEIs, prepare specific academic programmes dedicated to students. Commercial companies offer

[35] See https://www.jcu.edu.au/courses-and-study/courses/bachelor-of-engineering-honours-in-electronic-systems-and-internet-of-things

[36] World Bank 2015. ICT for Greater Development. http://siteresources.worldbank.org/extinformationandcommunicationandtechnologies/Resources/WBG_ICT_Strategy-2012.pdf

dedicated courses for increasing the matching capacity of current students (and future experts) with quickly developing needs of the labour market as well as for addressing the slow reaction of universities in adapting the academic curricula.[37] This is an interesting development for the future because it provides HEIs with a clear indication on the market needs and strengthens the cooperation between companies and education institutions.[38]

By combining ICT and technology, IoT provides a set of opportunities also for technical high schools. Technical schools and vocational training/education institutions are increasingly focused on the IoT education programmes. Drawing upon the principle that the IoT can be defined as the system of systems, various professional schools offer programmes, which are crafted in cooperation with industries as a way to increase the employability rate.[39] This approach is still experimental and despite promising results, it demands an institutionalized joint effort between academia and industries. However, it demonstrates a clear understanding from both HEIs and companies on the need of improving in terms of quality, expanding in terms of quantity, and focusing in terms of market needs, the education offer.

4.3 Open online and commercial courses/platforms in education offer

The increasing demand for IoT courses and the limited and still non adequate academic offer in consolidated IoT education programmes have contributed to an increasing number of courses offered either on free online or on commercial platforms. This is considered as an opportunity to match the labour market demand: in the next 10 years almost 10 million job positions will go unfilled in the IoT framework.[40] The principal actor in offering online courses is constituted by HEI institutions, which tend to provide ad-hoc courses for interested participants in order to somehow match the booming demand from both sides: a) students/professionals; b) and industries.

Considering their target customer/beneficiary needs, course structure varies in terms of content, length and topics. However, it seems to be a clear distinction between online courses offered to students and to professionals. Courses offered to students are more encompassing in terms of content compared to those for professional, and although thematic, tend to provide an overview of the IoT in a multi-disciplinary approach. The focus of the courses is not as narrow as in courses for professionals, which in exchange are shorter and tend to distribute the academic load over the weekends and on the evening hours. As a specific section is dedicated to IoT professional courses, we will focus on this section on the online courses for students. Despite specificities due to the topic of the course, approach and competences of the HEI in a specific field, most of online courses dedicated to students share three principal communalities:

1. **Orientation towards a multidisciplinary approach, fundamental for the IoT**. Most of online courses are not merely focused on potential IoT products or services but they dedicate part of the course on understanding interaction between ICT and technology when crafting a device and the latter's interfacing with physical world. Students learn also how to make design trade-offs between hardware and software, while being able to connect the devices to the Internet, as concluding steps in the path of multi-disciplinary approach.[41]
2. **Hands-on methodology** to address the mono-disciplinary background of participants since part of them holds an ICT background, while others have the technological knowledge. Hands-on approach of learning is increasingly useful even when expanding the education offer to

[37] See PTC IoT Academic Programme using ThingWorx application enablement platform: http://www.thingworx.com/academics/?_ga=1.92668317.1008018574.1462283042
[38] See http://www.ptc.com/news/2015/over-200-colleges-offer-iot-academic-program
[39] See http://www.iotlab.wisc.edu/
[40] See PTC IoT Academic Programme: http://www.thingworx.com/academics/?_ga=1.92668317.1008018574.1462283042
[41] See https://www.coursera.org/specializations/iot

potential students who have limited and/or even no knowledge on programming. Courses explain the current components of IoT devices and consider the capacity of students to produce innovative new designs and products as one of the learning outcomes of the courses.

3. **Provide a T-shape model of lecturing** by combining technical skills with soft-skills, vital when considering not only the go-to-market strategy for IoT services and products but also the important role of end-users in the success of IoT solutions.[42] So T-shape approach in various courses is not limited to the identification of business opportunities (as we will see more in detail in the respective section of this document) but it includes also an overall understanding of the importance of the IoT in society and how it can be employed to address societal challenges.

Most of HEIs offer courses online not only for their registered students but also for non-registered students. This approach of openness is adopted also by open online platforms in an attempt to address the increasing demand for IoT courses: in one free-online course focused on how the IoT and smart services will change our society, there were 18,300 registered learners[43]. Courses for non-registered students consist of a period, which varies from 3 days to 8 weeks, and are focused on specific topics employing predominantly online video-presentations and self-tests to be completed in each of the course's sections. In these courses the focus is on a thematic area of IoT application, while is assumed that participants do have the general knowledge on IoT.[44] However, an increasing number of online courses are offered to all interested people on IoT regardless whether their level of previous technical knowledge, opting for a learning approach based on comprehensive lecturing and on avoiding complex technicalities.[45] Table 5 provides a non-exhaustive overview on some of the free online thematic IoT courses by HEIs in the US and Europe.

Table 5: A Non-Exhaustive Overview on the Free Online IoT Courses

Course Name	HEI Institution	Via
Fog Networks and Internet of Things	Princeton University	Coursera
The Internet of Things	King's College London	FutureLearn
Internet of Things & Augmented Reality Emerging Technologies	Yonsei University	Coursera
Internet of Things: Multimedia Technologies	University of California	Coursera
Internet of Things: How did we get here?	University of California	Coursera
How the Internet of Things and Smart Services Will Change Society		openSAP
Internet of Things: Communication Technologies	University of California, San Diego	Coursera
Interfacing with the Arduino	University of California, Irvine	Coursera
The Arduino Platform and C Programming	University of California, Irvine	Coursera
Interfacing with Raspberry Pi	University of California, Irvine	Coursera
The Raspberry Pi Platform and Python Programming for the Raspberry Pi	University of California, Irvine	Coursera
Cambridge GSCE Computing Online	Cambridge University Press	Independent

[42] See http://learning.acm.org/courses/index.cfm

[43] See for further info openSAP open platform https://open.sap.com/courses/iot1

[44] See https://www.conted.ox.ac.uk/h600-72

[45] See for example: https://www.youtube.com/watch?v=lFhh5Up3kpA; https://open.sap.com/courses/iot1

Develop Java Embedded Applications Using a Raspberry Pi		Oracle
Introduction to the Internet of Things&Embedded Systems	University of California, Irvine	Coursera
Internet of Things: Setting Up Your DragonBoard Development Platform	University of California, San Diego	Coursera
Optics for Robots and Drones	University of California, Irvine	Coursera
Robotic Motion Systems	University of California, Irvine	Coursera
Introduction to Optobotics	University of California, Irvine	Coursera
Haptics: Introduction to Haptics	Stanford University	OpenEdx
Binaural Hearing for Robots	Inria (French Institute for Research in Computer Science and Automation	France Universitè Numerique
Internet of Things: Sensing & Actuation From Devices	University of California, San Diego	Coursera
Prototyping Interaction	Amsterdam University of Applied Science	Iversity platform

Source: Class Central Platform[46]

Some of the principal IoT platforms used today either as commercial or open source of online courses are: *SAPInternet of Things Solutions; IBM Bluemix; ARM; Intel; Microsoft Azure; Ayla Networks; Xively; Jasper ; AllJoyn, AllSeen Alliance; Bosch IoT Suite; OpenRemote; Arrayent; Echelon; Wind River; Contiki; SensorCloud; mnubo; Oracle Internet of Things; Swarm; Etherios; ioBridge; Zatar; Sine-Wave; EVRYTHNG; Exosite; Marvell; Swarm; Axeda; ThingWorx;.*

Considering the increasing demand from students for online courses there are different initiatives, which build online programmes by combining different free-online IoT courses offered by various universities.[47] Considering the booming demand and the non-standardized and structuralized IoT education offer, these free online education packages provide a double-layered advantage:

- A comprehensive IoT education offer, addressing in this way the segmentation of the actual IoT online programmes. A comprehensive education offer is also important because it provides students with a clear overview of the complexity, potentials and multidisciplinary framework of IoT.
- An opportunity to standardize the IoT academic offer. Online packages offer a chance to test various IoT educational offers and to comprehend, based on the feedback of students and their results in successfully implementing course concepts, what are the needs of both labour market and students. This can help to identify the most appropriate approaches to address those needs.

Beyond the free-online IoT courses, an increasing number of qualitative courses are also offered against a fee and through commercial platforms to all interested stakeholders turning the current gaps of the IoT education offer into a business opportunity[48]. In terms of content focus and teaching modules, they share common features with the free-online courses such as thematic orientation,

[46] See https://www.class-central.com/report/iot-free-online-courses/

[47] See for example: https://www.class-central.com/tag/internet%20of%20things

[48] https://mitprofessionalx.mit.edu/courses/course-v1:MITProfessionalX+IOTx+2016_T1/about; https://www.conted.ox.ac.uk/h600-72; http://axelta.com/AxOnlineIOTBootcamps.php

length of course, introduction of soft skills and even the capacity to be comprehensive for learners without the IoT background. The customers' profile of these courses is not limited to professionals or students/researchers but also to business people, who regardless their limited technical knowledge on IoT, consider it the next development opportunity and as such are interested to know better the present potentials and prospects.

Regardless an increasing number of IoT modules taught in blended courses, with the academic offer still undergoing the process of development, there are still some problems to be addressed. In terms of courses offered to registered students, it holds the concern of how to recognize these courses in the academic curriculum considering that there is not yet a widely-accepted mechanism of online evaluation for students tests. Moreover there is another encompassing problem related to the IoT online learning in general: few students do have at home access to embedded network devices, while limited solutions are available for teaching internet-scale programming of sensor applications[49].

4.4 Dedicated IoT courses for professionals

The pressing increase demand of the labour market to address both needs – more IoT experts in general and specialization of current experts in thematic IoT areas – makes the personnel training a fundamental component of IoT development. Professional courses are offered predominantly to professionals with an ICT background but an increasing number of modules invites to participate business people regardless their background. So the shortage of qualified personnel in IoT, further specialization in one IoT sector and the demand of business people to know more about ICT are the principal factors to shape the IoT professional education offer. Consequently, we can identify three current branches in the IoT professional education:

- The first branch of IoT courses is dedicated to those professionals who have either ICT or engineering background and decide to move to the IoT multidisciplinary ground;
- The second focuses on increasing the specialization of IoT staff on dedicated IoT sectors which demand specific solutions and services;
- The third branch is dedicated to managers and business people, who don't have a technical knowledge but are interested in understanding better how the IoT development can create market opportunities.

The principal focus on courses for professionals is to set a multidisciplinary framework and allow participants to envision the IoT as a system of systems to enable the development of new products and services. Despite a shared understanding of the IoT bridging position, convincing professionals to leave their comfort zone and move towards an innovative multidisciplinary approach is not a straight-forward exercise. Various training courses focus on explaining to the IT and operational technology professionals the significant complexities of the converged environment, where the IoT operates.[50] As we will see in the following section, the professional courses are progressively characterized by the introduction of soft-skills in the curriculum so as to enable participants to realize the IoT market opportunities and appropriately identify societal challenges.

Courses dedicated to IoT professionals operating in the field, are focused on enabling IoT experts to specialise in one or more specific areas including sensors, localization, wireless protocols, data storage and security, IoT analytics etc.[51] Data storage and security as well as networking concepts

[49] Kortuem, Gerd; Bandara, Arosha; Smith, Neil; Richards, Michael and Petre, Marian (2013). Educating the Internet-of-Things generation. Computer, 46(2) p. 53.

[50] http://www.rockwellautomation.com/global/services/training/certificates/cisco-iot.page

[51] http://www.kdnuggets.com/2015/09/data-science-iot-practitioner-course.html

are increasingly receiving a dominant role on the overall IoT education offer, thanks to a growing concern from the end users in terms of data security and privacy. The overall conceptualization of the IoT is then followed in the course programme by the exploration of technologies, architectures, standards, and regulations. Many courses are tailored to employ hands-on methodologies including in the programme the development and implementation of IoT technologies, solutions, and applications.[52]

In the case of IoT courses tailored to participants with business background, the courses have more of an introductory role to the IoT opportunities.[53] Here the principal idea is to provide a clear understanding on what opportunities IoT can create. This openness towards business profiles in the IoT professional courses has also another advantage: it helps IoT professionals to have an open mind-set and to consider not only technical aspects when proposing IoT solutions/services, but also to understand which are the market needs and how these needs can be addressed on a business perspective.

Beyond the thematic aspect and content needs, online courses offered to professionals are crafted around the professionals schedule and possibility to attend the course. To address the professionals' availability problems during the week, the course workload is concentrated over the weekend while the length varies from 2 to 6 weeks. Some courses are offered on-site by the training teams, as to facilitate the participation of professionals mainly for big corporations and important companies.[54]

In some cases, companies operating in the IoT field pair with HEIs or other companies[55] to establish professional IoT courses dedicated to their staff's specific needs. The purpose is to offer a training programme, which trains the staff professionally by following the company's vision for future development.[56] These courses are frequently opened to professionals from other companies or even to students with a clear strategy in mind: training professionals quickly and in line with company's development strategies, to address in the short and mid-term period the problem of limited number of skilled human resources.

4.5 Degree of T-shape approach implementation in IoT education

Throughout the different levels of the IoT education offer analysed in this document, it clearly emerges the need and implementation steps in introducing the business and innovation component in the teaching modules. Nowadays there is an increasing understanding among teachers' community (especially in ICT and technological engineering) that technical skills are necessary but not sufficient to identify innovative solutions and services[57]. Therefore, the education programmes especially at the post-graduate or professional learning level are increasingly implementing the T-shape as an integral part of the courses.[58] However, in the case of the IoT education, there is a major push in this direction that seems to be shared by all the stakeholders. One of the principal reasons behind is the need of IoT professionals to be equipped with the soft-skills to be able to address the societal challenges, interact with end-users more successfully,

[52] https://mitprofessionalx.mit.edu/courses/course-v1:MITProfessionalX+IOTx+2016_T1/about

[53] http://www.computerworld.com/article/3024912/internet-of-things/mit-offers-internet-of-things-training-for-professionals.html

[54] https://www.experfy.com/big-data-hadoop-training/courses/iot-training:-internet-of-things

[55] http://www.rockwellautomation.com/global/services/training/certificates/cisco-iot.page

[56] https://www.qualcomm.com/news/onq/2015/10/13/build-your-own-internet-things-coursera

[57] See for example the entire Knowledge Innovation Communities initiatives (KICs) financed by the European Institute of Technology (EIT) where the I&E component is an integral and mandatory component of the education programme to receive the EIT label.

[58] https://mitprofessionalx.mit.edu/courses/course-v1:MITProfessionalX+IOTx+2016_T1/about

consider the market needs and potentials so to come up with a product/service in demand by customers and above all employ a mind-set, which is driven by the involvement of different stakeholders. This is important since, for many experts, the IoT is the next industrial revolution.[59] In this perspective, IoT offers unique opportunities for innovation and business, but IoT professionals have to be equipped with the necessary soft-skills to exploit them.[60]

An increasing number of the IoT courses (online and on-site) offer a T-shape approach to learners considering it as a fundamental skill for an IoT expert. The increasing awareness of various IoT stakeholders on the implementing a T-shape education model is clearly illustrated by a growing number of courses dedicated only to soft-skills capacities but targeting the IoT experts/students, who are willing to develop a T-shape professional background.[61]

This approach is also supported by the industrial actors, who are not simply looking for IoT experts but for inventors, dreamers, doers in the field of IoT.[62] In all IoT courses offered thanks to the cooperation between HEIs and industrial partners, the business and innovation modules are constantly present. Industrial partners are also establishing IoT Labs, contests or challenge camps, where learners come together to address concrete problems faced by companies by offering solutions, which are technically doable and feasible from the business view-point.[63]

However, there is not yet a coordinated programme and each course has different characteristics in terms of T-shape approach. Some courses focus more on providing insights on how to identify end-user's needs and challenges for increasing the capacity of the latter to interact with proposed technical solutions, while in other cases, the focus is on understanding the market opportunities offered by the IoT.

Other courses maintain that IoT offers more opportunities of coming up with innovative ideas by combining existing applications/services, while in other sectors, one has to introduce a new application/service in one specific sector, facing in this way a very competitive and quickly improving battlefield. So harmonizing the efforts on introducing a T-shape approach in the IoT education and a common virtual space, where these experiences and best-practices can be shared and exchanged, could be a good starting point for a less fragmented T-shaped IoT offer.

4.6 Teaching End-Users on IoT

The end-users education is fundamental in the case of IoT as its significance doesn't stand on the technology alone, but in its implications for the society and its impact on the computing discipline itself.[64] Various analysis and research papers argue that regardless its growth, the IoT expansion is still hindered by the degree of users' acceptance and technological capacity to fully benefit from the services IoT can offer.[65]

In this respect the end-users literacy to use IoT services and if needed to provide specific feedback on the product, remains fundamental for the IoT development. Moreover, the end-users' capacity

[59] https://www.youtube.com/watch?v=lFhh5Up3kpA

[60]https://www.accenture.com/us-en/insight-ceo-briefing-2015-productivity-outcomes?c=str_itdigdisrpfy16psgs&n=IIOT_Trends_-_IT&KW_ID=sjAsrSmCv_dc|pcrid|84332153775

[61] http://learning.acm.org/courses/index.cfm

[62] https://www.qualcomm.com/news/onq/2015/10/13/build-your-own-internet-things-coursera

[63] See for example http://www.iotlab.wisc.edu/

[64] Kortuem, Gerd; Bandara, Arosha; Smith, Neil; Richards, Michael and Petre, Marian (2013). Educating the Internet-of-Things generation. Computer, 46(2) p. 53.

[65] M. Roelands et al., "Orientation towards Do-It-Yourself Internet-of-Things Mass Creativity: What Can the Internet of Things Do for the Citizen?" *Proc. Pervasive Computing Conf.*, 2010;

to communicate challenges and to provide feedback on solution/products would constitute an important information source for aligning industry-strategies with end-users' requirements.

Teaching end-users IoT is a paradigm shift in education (and not only) as it demands a change in the mentality of teaching audience and requires a new attitude towards a unique and inter-disciplinary learning experience. Although this approach is still considered as a novelty, it seems to have the support of the entire community of the IoT stakeholders:

- *HEIs* are interested to increase the number of potential learners to their education programmes, while having a valuable interactive audience ready to provide feedback especially on education programmes dedicated to people with a non-IoT background. Moreover, young end-users may constitute future potential students if they get familiar with the IoT concepts and see their potential. In this respect, such courses are also a marketing tool for universities based on the paradigm: don't tell your values, show them;
- *Researchers/experts* are interested to lower the barriers in IoT implementation and making it more pervasive. A literate end-user can also provide a more sophisticated and focused feedback on the products/services.[66] If end-users are more familiar with the IoT potentials they can direct the attention of researchers/experts towards daily problems providing a sort of needs' priority list. This will contribute to IoT development towards societal challenges, introducing a more social oriented academic research and a more customer-oriented model of the IoT industry.
- *Companies* are interested to increase the number of potential customers thanks to the capacity of using in a more appropriate way and more frequently the products/services. Even in this case, the feedback by the customers offers a unique opportunity for the service/product validation.[67]
- *End-users* have the proper benefits: getting gradual access to concepts and content of the dedicated education programmes will offer them the opportunity to benefit from an increasing number of IoT services as well as will contribute to create a web-community where they can share experiences, knowledge and support.

Beyond specific benefits for each stakeholder, the introduction of education courses for end-users offers a common positive development to HEIs, researchers/experts and companies: the end-user moves gradually from being part of the problem to being part of the solution. Literate end-users can increasingly either provide some disruptive innovative solutions or improve the actual products/services starting from in-situ user experience. Hence, the end-users education increases the potential for innovative solutions in the IoT.

[66] http://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/education_internet.pdf

[67] http://www.ptc.com/news/2015/over-200-colleges-offer-iot-academic-program

5. OPEN PLATFORM TO ADDRESS EDUCATION CHALLENGES

The previous sections presented the barriers and education challenges for IoT adoption from different stakeholders' perspective. In this section, we present how UNIFY-IoT (in conjunction with the EPI projects) will support the community to address those challenges.

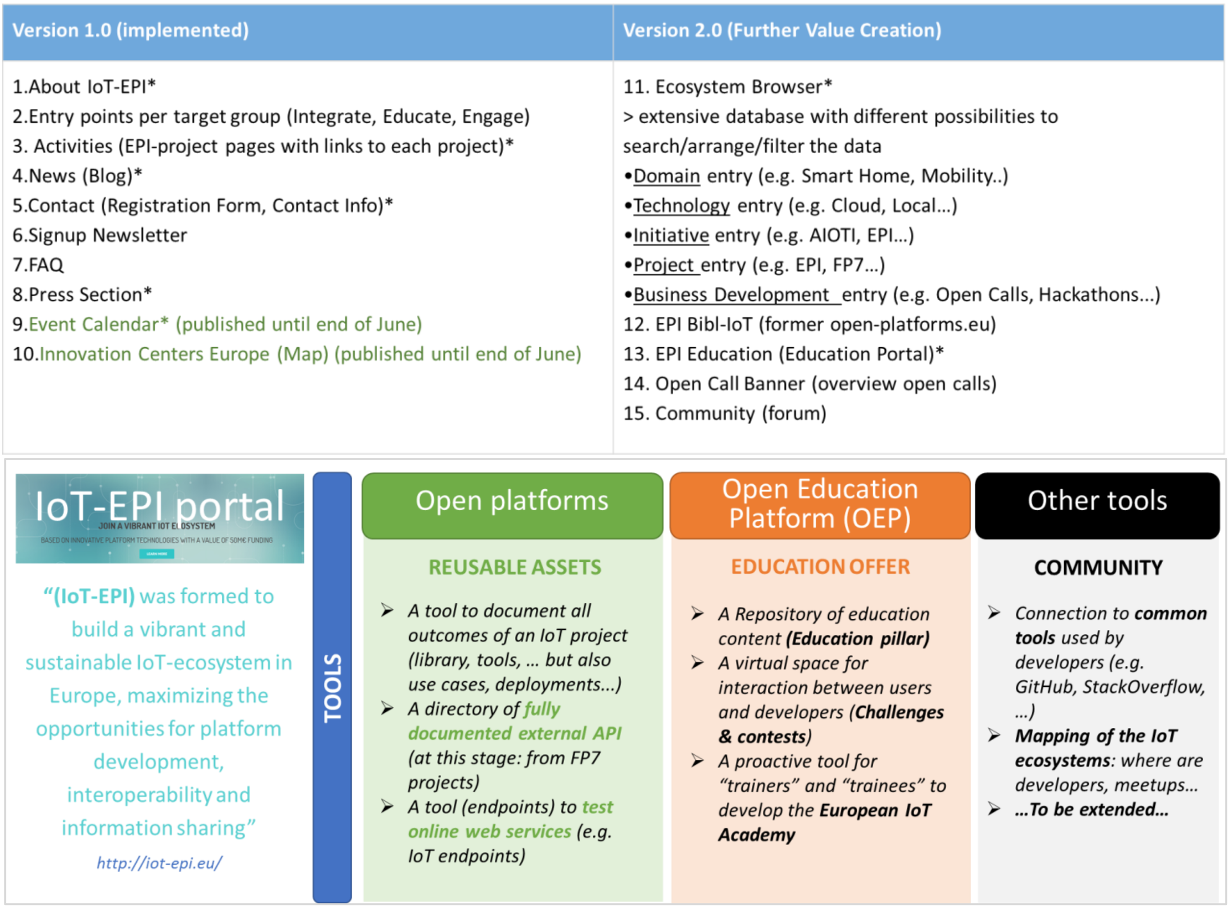
Two perspectives should be taken into account:

- **Supporting the RIA's in their development**
- **Supporting projects to spread their results and especially their good practices and reusable assets to the ecosystem.**

Two complementary tools will be developed within the umbrella of the project:

- The Bibl-IoT, shaped on the previous experience of the open-platforms
- The Open Education Platform (OEP).

In this section, we present the principles of these two platforms. The elements reported below have been presented, discussed and validated within the IoT-EPI. Both of those tools are part of the IoT-EPI web landscape.



Version 1.0 (implemented)	Version 2.0 (Further Value Creation)
1.About IoT-EPI* 2.Entry points per target group (Integrate, Educate, Engage) 3. Activities (EPI-project pages with links to each project)* 4.News (Blog)* 5.Contact (Registration Form, Contact Info)* 6.Signup Newsletter 7.FAQ 8.Press Section* 9.Event Calendar* (published until end of June) 10.Innovation Centers Europe (Map) (published until end of June)	11. Ecosystem Browser* > extensive database with different possibilities to search/arrange/filter the data •Domain entry (e.g. Smart Home, Mobility..) •Technology entry (e.g. Cloud, Local…) •Initiative entry (e.g. AIOTI, EPI…) •Project entry (e.g. EPI, FP7…) •Business Development entry (e.g. Open Calls, Hackathons…) 12. EPI Bibl-IoT (former open-platforms.eu) 13. EPI Education (Education Portal)* 14. Open Call Banner (overview open calls) 15. Community (forum)

"(IoT-EPI) was formed to build a vibrant and sustainable IoT-ecosystem in Europe, maximizing the opportunities for platform development, interoperability and information sharing"

http://iot-epi.eu/

Open platforms

REUSABLE ASSETS

- *A tool to document all outcomes of an IoT project (library, tools, … but also use cases, deployments…)*
- *A directory of **fully documented external API** (at this stage: from FP7 projects)*
- *A tool (endpoints) to **test online web services** (e.g. IoT endpoints)*

Open Education Platform (OEP)

EDUCATION OFFER

- *A Repository of education content **(Education pillar)***
- *A virtual space for interaction between users and developers (**Challenges & contests**)*
- *A proactive tool for "trainers" and "trainees" to develop the **European IoT Academy***

Other tools

COMMUNITY

- *Connection to **common tools** used by developers (e.g. GitHub, StackOverflow, …)*
- ***Mapping of the IoT ecosystems**: where are developers, meetups…*
- ***…To be extended…***

Figure 8: Overview of the iot-epi.eu

5.1 Bibl-IoT

Bibl-IoT, as known as open-platforms.eu (former name) is a web platform, which provides IoT projects' teams with a common repository to document their outcomes. This work was initiated in 2013/2014 as part of IERC AC01 and then supported by the FP7 BUTLER project (which documented all its achievements).

The purpose of the Bibl-IoT initiative is to encourage development and industrial communities to leverage on existing achievements. While it focusses at this stage on EC-funded projects, it will be extended to any "open" projects related to IoT.

In its actual version, Bibl-IoT is a set of components: a tool to document all outcomes of an IoT project (library,tools, but also use cases, deployments, etc.), a directory of fully documented external API (at this stage: from FP7 projects) and a tool (named endpoints) to test online web services (e.g. IoT endpoints).

The upcoming version of Bibl-IoT will be fully integrated with the IoT-EPI website (and will be supported by both UNIFY-IoT and Be-IoT) and its look and feel will be updated to the IoT-EPI branding (same colours, fonts, etc.). Additionally, the navigation will be improved, thus facilitating users' navigation between the various sections of the IoT-EPI website.

The main principles of the Bibl-IoT platform are:

- To present innovative findings to encourage employment of results by developers and industrial communities.
- To make available good practices /reusable assets, use-cases to ecosystems for further use and/or development.
- To bridge and create compatibility between end-users' needs and projects' results.
- To test online web-services.
- To create a virtual space and community where stakeholders (soft-developers, platform developers, architects) can interact.
- To map the IoT ecosystems: where are developers' match-making needs and opportunities.

5.2 Open Educational Platform

5.2.1 Background and Needs

The analysis on the current situation of the IoT Education has highlighted that there is not yet a well-established approach on how IoT applications will develop and be deployed relative to Research and Innovation. Furthermore, the IoT education offer is still distant from addressing the abrupt demand for IoT experts as well as from being consolidated and standardized. Hence, the potential content of the OEP will be focused on addressing to principal problems considering stakeholders needs: a) support a converging and complementary IoT education for all stakeholders (students, developers, professionals, businessmen); b) create a common space where IoT educations is harmonized with innovation, business opportunities and industrial challenges.

To address the present needs related to IoT education, innovation and stakeholders, the OEP has to combine in a T-shape approach the content, which appropriately connects education, research and business opportunities. The platform architecture and content is conceptualized to address the above mentioned needs in IoT education.

In doing that, the OEP has to face different challenges such as:

- **Not duplicate existing contents (e.g. HEI online courses).** To address this challenge the OEP will act as both **content repository** and **links directory** to give access in a unique place to original content and relevant links.
- **Guide the users through heterogeneous content.** That's why the OEP will organise the content according to **the profile of the beneficiaries** (e.g. students, professionals, end-users, etc.)
- **Create a dynamic platform that relays on actual needs and challenges of IoT community.** In that respect, beyond feedback provided by users, there is also a virtual space dedicated to

post contests between the challenges provided by **industrial actors** and solutions provided by **developers/researchers.**

The added value of the OEP is to create a single portal for users and promoters and content developers of education modules.

5.2.2 Objective

The OEP will highlight the role of the IoT as the system of systems ensuring a connection with enabling technologies and especially the needs of stakeholders. The OEP is a first step towards a common effort to a comprehensive, coherent and standardized education offer on IoT. Our purpose is to build an IoT academy at European level: **"One stop shopping for IoT courses".**

In terms of content, the platform will address different needs including methods to extend the concept of IoT Academy/Institute to the IoT ecosystems and introduce the IoT education programmes in schools and universities curriculum, open modules, "how-to guidelines"; its usage will be promoted thanks to education online modules for current or future IoT developers, adopters, business developers, students, professionals and end-users.

5.2.3 Architecture and Potential Content

To facilitate these objectives and to address the principal stakeholders' needs, the OEP will be organized around two main pillars/categories: a) the **education pillar**, which will offer educational content; b) IoT Academy (or **Challenges Area** of companies/start-ups), where the latter can share with beneficiaries the most updated results and specific challenges. A landing page will guide the OEP users to the content he/she is interested in. Under each of the two above mentioned pillars, the content will be organized in sections mirroring the stakeholders' needs.

This architecture was the result of two distinct set of actions:

a. the challenges identified in the present deliverable 4.1 where the principal barriers on IoT usability and education offer have been identified thanks to a non-exhaustive desk-research;
b. interaction with the members of the TF05 on Education. The Task Force was composed by IoT experts either on IoT education, private companies, research institutions and other public/private stakeholders, who provided feedback in the process of identifying challenges and in crafting the adequate OEP architecture for addressing those challenges.

Education Pillar: The added value of the educational content is to codify and provide on-line the available education offer on IoT, mirroring the end-users' needs and facilitating their access. The benefit of content providers is that each course will be equipped with feedback mechanism, creating the opportunity to be used as a testing tool for assessing the quality of the teaching modules and an opportunity for improving it. This comprehensive offer provides a thorough IoT education offer in a sort of one-stop-shop: everything concerning the available IoT education, just two clicks away.

So under the **Education Pillar,** the learning offer is conceptualized in four thematic sections:

1. ***Undergraduate and Post-Graduate Education Offer.*** This academic offer is dedicated to current IoT students, lecturers, researchers and developers. The section is organized in three sub-sections:
    a. ***Education offer for Beginners*** focused on students who have completed or are in the process of completing it BSc degree. Courses here are at the BSc level, predominantly offered by HEIs;
    b. ***Education Offer for Intermediate Level***. The academic offer here will include courses taught at the Master Degree Programmes. There is an increasing number of courses at the MSc in IoT since students have the basic necessary knowledge to start appropriately combining the ICT and technological knowledge.

   c. ***Education Offer for Advanced Users.*** The technical IoT courses will be combined here with courses dedicated to the techniques on how to connect/adapt/focus your research towards societal challenges. The idea behind is to connect research and innovation to the market.

2. ***Life-Long Learning Education Offer.*** The courses here are dedicated to two groups of professionals: a) IoT professionals, who have the need for either further or more specific specialization; b) and professionals either ICT or business people who decide to specialize on IoT technologies.
3. ***Transversal Soft-Skills Education Offer.*** This section will contain courses targeting participants in each of the above-mentioned stakeholders, who feel the need or opportunity for transversal education in soft-skills (including business & innovation courses). A specific attention is dedicated to courses on **Intellectual Property Rights (IPR)**, which include modules and guidelines on how to preserve IPR while presenting the innovative ideas.
4. ***Education Offer for end-users***. These courses are dedicated to end-users considering that the latter capacity to interact with IoT services/solutions is one of the principal factors hindering the further expansion of the IoT technology. These courses aim at increasing the users' acceptance by providing modules on how to use IoT services and technologies. In this way, end-users can benefit much more from the available services and can contribute to improve the offered solutions.

Challenges Area (IoT Academy) sets a virtual space for constant interaction between industries, open source projects, which interact with their users, and developers. Companies can share with beneficiaries not only their research/technological results but can put forward challenges where stakeholders (IoT developers, adopters, business people, students, professionals, start-ups and end-users) can contribute by proposing solutions. So companies are not only providers of content/results but they can also receive potential solutions to their challenges. Developers/end-users can present their solutions in a pitch-presentation model.

A specific template it will be provided to developers helping them to craft an idea presentation, so they can hook the company as well as share their ideas with a wide range of stakeholders contributing to a wide-spread of innovative ideas, while keeping cards close to their chest in terms of the proposed solution. The courses on IPR in the soft-skills section may help developers on how to preserve the intellectual property of their solutions. However, the platform is offering a match-making opportunity, while the contractual terms (in case interesting solutions are proposed) will be set by the company providing the challenge or company/developer offering the solution. This service's workflow will be similar to the one used by companies which create bug bounties in order to assess the security of their products.

Another added value of the challenges area for the companies, is that the latter can use this virtual space as a Test-bed for their new products/services and build a community of literate customers, who can not only provide helpful feedback but also some productive suggestions to improve the solutions.

So the **IoT Academy Pillar** is the interaction area between industries, developers and end-users and is conceptualized around two thematic areas:

1. The ***Challenges*** dedicated to challenges presented by companies and solutions presented by IoT developers, adopters, business people, students, professionals, start-ups, end-users, etc. Prizes (either in material terms or in recognition) may be offered. Challenges workflow will be similar to the one used by companies, which create bug bounties programmes in order to assess the security of their products;

2. The ***Test-Bed*** where companies present their solutions and end-users can participate providing feedback and potential improvements on new products/features.

5.2.4 Content Providers and End-Users

HEIs and other stakeholders involved in IoT education will provide the content for education courses based on the modules they have been already offering in their education programs.

We will urge contributors to provide the content as links (e.g. the OEP will store a few meta-data on the content plus a description, but the main content, e.g. the course itself for example, will be located outside of the OEP), which can be automatically updated anytime the contributor updates it. Companies/start-ups will provide the most up to date results and specific challenges related to research and carried on technological projects. OEP will act as a repository.

The uploaded education related content will be originated not only from materials prepared in running Horizon 2020 financed projects, but also in other related projects.

Beneficiaries (e.g. users of the OEP contents/services) of the OEP can be summarized in the following categories:

- Developers;
- Adopters;
- Business developers;
- Students;
- Professionals;
- IoT end-users (e.g. citizens); lecturers and trainers of IoT professional programmes.

There are concrete benefits for content providers to participate in the OEP:

- They can bring in **their challenges/experiences** so the open education platform will be crafted considering their needs. This will contribute to have a portal, where different initiatives, solutions and best-practices provided thanks to the stakeholders' contribution (members of Task Force on Education or partners in their respective networks) will converge **to construct a common education offer on IoT**.
- This platform will provide a **unique opportunity** in terms of institutional benefits for the High Education Institutions (HEIs).
    - The latter can increase their academic offer for BSc students, post-graduates and researchers as well as share some best-practices with other HEIs and can receive feedback from users on how to further improve their programmes. Since each uploaded material will be equipped with a feedback mechanism, the platform can also act as a validation tool for courses (both new and updated ones). A short questionnaire of maximum six questions will be provided. Students will vote and tag the course creating a category of "champions" or most attractive courses. This will act as a tool for improving the quality of modules for all those lecturers, who update their courses.
    - By sharing education modules in the platform, HEIs will increase their visibility and consequently consider the OEP as a marketing opportunity. This is not limited only to the marketing of online courses but to all academic offers of universities. For instance, on the top of the online course, the university can provide the entire IoT academic offer (regardless whether these are courses, which can be attended only by physical presence in the campus or even multi-annual programmes such as BSc or MSc).
    - Moreover, HEIs have the chance to be front-runners in a process, which aims at promoting a unique European IoT education programme, by converging the existing education programmes to the stakeholders' needs. **This can further increase their institutional role at the European level.**
- As the platform will be dedicated also to education needs of professionals, non-HEIs Task Force members (start-ups, companies, developers) will also benefit. They can offer to their

staff the opportunity to **update their knowledge or adequately specialize** thanks to a more complete education offer related to IoT issues. Some Task Force members can share their professional learning programmes and receiving feedback from the OEP users on how to improve them. Needless to say the marketing opportunity thanks to the visibility of the platform.

- By providing a challenge area between demand of some stakeholders and offer of some other ones, OEP creates a win-win model. Companies can bring in technological or professional education challenges, while universities, students/researchers or developers may offer solution to the posed challenges.
- The Task Force activities/deliverables can match or support the activities/deliverables, which some of the Task Force members may have on their respective project tasks, creating in this way complementarities' or added values' opportunities.
- Being tailored to address stakeholders' needs, this OEP may constitute an institutional, oiled and well-functioning tool, which can continue to operate after the respective projects' lifespan thanks to the cooperation between Task Force members (and other industrial, education or research partners, which will contribute).

The Figure 9 shows a synthetic presentation of the OEP.

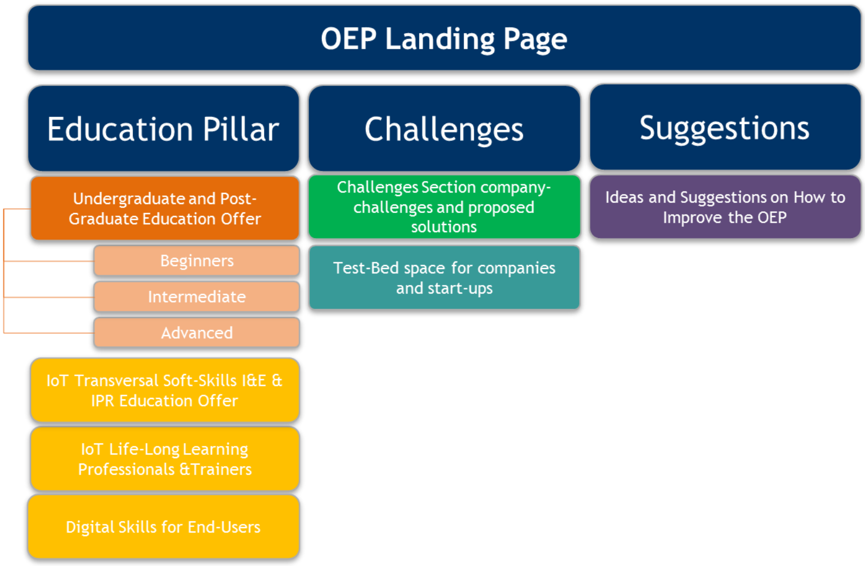

OEP Landing Page
Education Pillar
Challenges
Suggestions
Undergraduate and Post-Graduate Education Offer
Beginners
Intermediate
Advanced
IoT Transversal Soft-Skills I&E & IPR Education Offer
IoT Life-Long Learning Professionals &Trainers
Digital Skills for End-Users
Challenges Section company-challenges and proposed solutions
Test-Bed space for companies and start-ups
Ideas and Suggestions on How to Improve the OEP

Figure 9: Overview of the OEP structure

5.2.5 Regulatory Framework

This is obviously a very important and delicate issue. The term "open" here refers to an open source platform, meaning that this will be public and everyone will have access. The agreed rule is that each contributor will publish in the platform only open source materials.

Any stakeholder can use these materials for training/teaching purposes in exchange to the appropriate reference to the author. It will not be simple to use the content by other users violating the IPR rules as courses will be marked by logos institution/individual of the issuing the course. In case, the published content will be re-worked by the user, then the above mentioned rule of quotation applies.

We believe that the issue is clear on those content materials, which are developed within the Horizon 2020 projects. According to the Horizon 2020 guidelines they are open source (unless clearly specified in particular projects). Various partners may have materials developed prior to the actual Horizon 2020 project and in this case the quotation above-mentioned rule applies.

In cases when the content is not an open source, we can let partners to upload teasers for courses, by providing a link. This can be done only in the case an open-source material is also provided. So the end-user will follow the link and get on the contributors website, where the latter's rules and regulations will apply (receiving access in the course against payment, registration, or in exchange of providing feedback to the course etc.) This could be a productive way to attract institutions to contribute with content on the platform (if they have open source materials) or by providing links to licensed materials. In this way, we will provide end-users with a well-crafted catalogue of education offer for their needs. In this way, in each thematic section of the OEP we can have the open source offer and the link for the modules offered not for free.

5.2.6 Operational Framework

The description here of the operational framework is more related to the organization of work rather than focusing on a detailed technological explanation.

The fundamental component of the operational framework is that two partners from the Task Force on Education will act as gate-keepers in each section of the OEP. Their role goes beyond collecting information for their specific area: they have to also ensure the quality of the material that is proposed by other partners to be uploaded. So they will validate the content and then upload the material on the platform. This is crucial to avoid open access to platform administration and to ensure the quality of the proposed products.

The OEP will not duplicate existing contents (e.g. HEI online courses). The OEP will act as both content repository and links directory to give access in a unique place to original content and relevant links.

To offer guide to the users through the heterogeneous IoT education content, the OEP will organise the content according to the profile of the beneficiaries (e.g. students, professionals, end-users, etc.). This will help to create dynamic platform that relays on actual needs and challenges of IoT community.

The success of the OEP will depend on how stakeholders (at large, e.g. content providers and "students") are involved. Therefore, the IoT community of experts involved in IoT projects will be employed to disseminate the information, which is important on two ways:

- Enlarge the community of users helping to create a critical mass necessary for the sustainability of the platform;
- Increase the number of potential contributors in the platform.

In the Challenges Area, the platform will promote the interaction between industries and developers/end users. Challenges will be proposed by companies to:

- Get feedbacks from users on their platform
- Disseminate new products/features
- Engage users
- Offer prizes

Challenges workflow will be similar to the one used by companies which create bug bounties programmes in order to assess the security of their products.

The platform will be built on the top of existing open source solutions. Design (user interface elements) will be developed on top of the IoT-EPI. The platform will be hosted under the iot-epi.eu domain

A schematic presentation provides a sketch on how the OEP will work.

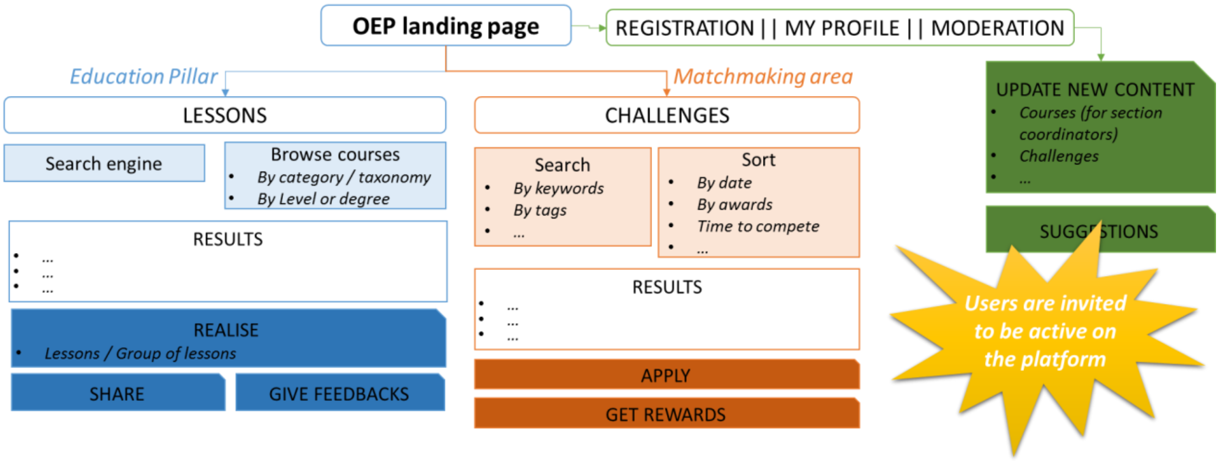


Figure 10: Overview of the proposed flow on the OEP

5.2.7 Conclusions

The value co-creation is not the objective but the result of the OEP since stakeholders will bring their challenges and best-practices, and together will identify the appropriate solutions. For example, **thanks to the course evaluation and feedback students or lecturers will help HEIs to craft courses** addressing their real needs. In the same approach, **companies/start-ups or developers will provide input to the OEP and suggest their education challenges** increasing the life-long learning impact but at the same time can also share the most updated technological results.

The OEP goes beyond offering a training/lessons content. It creates an interaction space between IoT stakeholders. The success of the OEP will depend on how stakeholders are involved to act as experts, future contributors, promoters and users to design and provide content to the **(OEP)**.
To summarize we can say that the OEP:

- Goes beyond training/lessons contents;
- Provides materials proposed by stakeholders and uploaded by the gate-keepers (OEP administrators);
- Invite experts / IoT champion / Recognized user will be asked to propose contents;
- Create links to existing IoT tutorials on the Internet.

6. CONCLUSIONS AND NEXT STEPS

6.1 Conclusions and Recommendations

The non-exhaustive overview provided by this document shows clearly that the IoT education offer is still distant from addressing the abrupt demand for IoT experts as well as from being consolidated and standardized. The principal challenge, but at the same time opportunity, is that the IoT, until recently, has not been considered a major subject on its own and it's still relatively new branch of the academic offer.

The characteristics of the IoT as the system of systems pose difficulties to set up a thorough and comprehensive programme on the IoT. In many universities, there is still hesitance to consider the IoT as a major to be introduced in the undergraduate programme, since the combination of ICT and technology demands a certain level of knowledge, which first year graduate students do not yet master.

In addition, IoT involves more than one discipline, thus demanding a multidisciplinary approach in drafting the programme, which is not yet a common practice. In terms of undergraduate curriculum development, many scientific issues on IoT are still to be studied. Textbooks' content and curricular system need to be gradually standardized and improved.

Since the core of the IoT lays in the unity of the physical world and digital world, many cross-cutting areas and the corresponding training will be generated in the future. Nevertheless, there are some initiatives form HEIs in the USA, Australia and Europe to implement undergraduate IoT programmes.

Introducing the IoT as a component of vocational training in the professional schools is another strategy to avoid the undergraduate major trap and to increase the number of IoT experts. However, these initiatives have to be coordinated and exchange their experience/best practices in order to accelerate the process of establishing an IoT academic undergraduate curriculum.

The education offer for IoT post-graduate programmes, instead, has recognized a quicker development thanks to a set of factors:

- Graduate students have the necessary knowledge to be further specialized on the IoT;
- The multidisciplinary approach, vital for IoT education, is an integral component of post-graduate programmes so coordinators of these programmes are better equipped and have the appropriate experience to establish these courses,
- The opportunity to be financed by various funding schemes (including Horizon 2020 and other instruments) has contributed to ensure excellency in post-graduate programmes by bringing together different HEIs.

Coordination of academic offer from various HEIs in this early stage of the IoT education development is fundamental for setting up a qualitative programme. While clearly performing better, the IoT post-graduate programmes still need a considerable work to coordinate their efforts within HEIs but also with industries for better addressing the labour market needs for expertise and for understanding market opportunities.

The rapid expansion of the IoT has caused an increasing pressure from the labour market in general and industries in particular to have more and better specialized students from the universities.

The above mentioned difficulties and the quickly increasing opportunities in the IoT have contributed to the prompt emergence of thematic and short-term courses. The majority of these courses are offered online and share some communalities such as:

- Orientation towards the multi-disciplinary approach fundamental for the IoT;
- Hands-on methodology to address the mono-disciplinary background of participants;
- Thematic orientation;
- Short-term period (most of them vary from 3 days to 6 weeks).

These courses provide a good opportunity for increasing the number of future IoT experts and further specialization of the IoT professionals. Although, the diversity of courses has contributed to a variety of addressed topics, they mirror the same problems of the education offer at the undergraduate and post-graduate level: non-coordinated, convergent offer with a clear strategic vision on education, but instead, an ad-hoc programme seeking to address immediate needs undermining a structural offer capable of focusing on the fundamental IoT needs. Another critical aspect is that the majority of learners lack the adequate infrastructure (especially the technological one) at home, undermining the possibility of considering on-line courses as a satisfactory substitution of the insufficient undergraduate and postgraduate academic programmes.

Training of the IoT professionals is another expanding education trend. Bearing the well-known characteristics of professional learning courses in terms of methodological model, the IoT professional education exposes some particularities in terms of the target group divided into three main paths:

- The first is dedicated to those professionals who have either ICT or technology background and decide to move to the IoT interdisciplinary ground;
- The second is dedicated to IoT professionals demanding a more focus oriented knowledge;
- The third is dedicated to managers and business people, who don’t have a technical knowledge but are interested in understanding better how the IoT development can create market opportunities.

Targeting learners without specific technical background is increasingly becoming part of the online-academic offer on IoT. This non-orthodox approach is steamed by the need of principal stakeholders to offer IoT courses for end-users. They don’t necessary possess prior programming skills, which makes end-users courses, the next challenge of the IoT education. This is fundamental for IoT development considering that the end-users difficulty to fully use the technology is one of the major reasons in terms of users’ barriers.

Training users is becoming increasingly important since understanding both the technical underpinning and wider societal impact of the IoT will be crucial for digital citizens of the future[68]. This education effort is crucial for posing the basis necessary for the establishment of the IoT generation and addressing the companies’ needs for specialized staff.

An increasing involvement of industrial partners in establishing on-line courses and the clear potentials of the IoT in exploiting market opportunities have contributed to another cross-cutting characteristic of the IoT education programmes: provide a T-shape model of lecturing by combining technical skills with soft-skills, necessary for understanding market potentials and considering the important role of end-users in the success of IoT solutions. In this respect, the opportunity of the IoT courses to be built, sometimes from the scratch, offers the opportunity to introduce from the start one of the most prominent education development: T-shape educated students, in order to substitute engineers with entrepreneurs, who possess the appropriate technical skills.

[68] (Kortuem, Gerd; Bandara, Arosha; Smith, Neil; Richards, Michael and Petre, Marian (2013).

Regarding the factors of acceptance, this deliverable wants to give a snapshot of the situation faced by the EPI-IoT project and the IoT community. The first step of this deliverable has been achieved by identifying the barriers related to the IoT acceptance. The work with the EPI-IoT projects has successfully started and has highlighted one of the main objective of UNIFY-IoT: to support the RIA projects to address the barriers identified in section 3. Strong interactions with the EPI-IoT projects are planned and will be done through diverse channels such as the EPI-IoT workshops, exchanges of best practices through the Open Platform, development of users' soft skills via the Open Education Platform.

The UNIFY-IoT consortium will continue to develop and enforce these tools, bearing in mind that the IoT legislative framework is constantly evolving. The new principles established in the GDPR have a strong potential to contribute to the increase of the trust towards the IoT applications and services, only if they are really and correctly implemented by 2018. In this respect, UNIFY-IoT plans to take this issue into account in its future work and to raise awareness to support the societal acceptance of IoT.

6.2 Next steps

The next steps in the UNIFY-IoT project to address the needs for an education offer and to address the identified barriers include strong connexion with the community:

- **Institutionalization of cooperation among RIAs**. The finalization of the OEP platform will demand a constant cooperation among partners in all RIAs and especially among the members of the Education Task Force. Their commitment is essential to provide input for the OEP, to coordinate the different components of the OEP and to disseminate through their network the added value of the OEP so to establish a critical mass in terms of platform users. Dissemination demands also the support of the other Task Forces. However, the cooperation with other Task Forces will not be limited only to dissemination: innovation, interoperability and business related Task Forces are called to provide their input in the components of the platform related to technical professional and soft-skills courses. So in the preparatory stage of the OEP, it will call for cooperation, which will add on synergies among RIAs.
- **Involvement of external IoT Stakeholders.** The education and challenge pillars of the OEP will raise the interest of external stakeholders. So stakeholders beyond RIAs, such as students, companies, developers, professionals will start participating, in the next step, in the activities of the OEP creating a dynamic environment where stakeholders can have an interaction space between lecturers and students, professionals and end-users, companies and developers, helping the IoT community to identify and address current barriers and challenges. So the next step will ensure a cooperation between IoT-EPI RIAs (which can participate either by presenting their project-results or share their activities) on the one hand and adopters (start-ups, SMEs, open-API developers) on the other, creating a value co-creation chain. This cooperation will increase the value proposition that IoT-EPI RIAs projects' results can offer to adopters in addressing their daily challenges, while enhancing the comprehension of RIAs activities from the stakeholders.
- **Contribution of end-users.** The end-users will be the following step of the OEP development. The analysis of the IoT barriers has demonstrated that end-users are a serious obstacle in increasing the degree of IoT technologies implementation. The OEP will involve stakeholders in three principal activities: a) offering courses for end-users on how to use technologies; b) asking end-users to participate in the process of idea validation (developers/start-ups) and/or product validation (companies and projects testing prototypes); c) end-users can contribute to solutions considering that they know much better their respective needs and what the offered solution/service/product is still lacking to provide for addressing end-users needs. So they can actively participate in improving

the solution. This involvement of end-users will promote what in the figure of value co-creation is defined as the Spillover-Result.

- **Taxonomy.** By creating a technical and business taxonomy, which will facilitate the process of searching for a specific piece of information, the OEP will ensure adherence between the developers and business community, while mapping participating stakeholders. This is going to promote the value co-creation mechanisms in the wide-ranging IoT ecosystem.
- **Axes of co-creation boosted by OEP.** As explained above, the next steps of the OEP will contribute to the value co-creation activities, not only in harmonizing the RIAs results in a complementarily approach, but also in promoting the process of adoption (developers, start-ups, companies, test-beds), monetization (challenge area where new innovative ideas may come up and be of interest of companies/investors) and social awareness/acceptance (thanks to the involvement of end-users other in testing results or in providing feedback). Hence the next-steps planned for the OEP development will kick-off a process, which will produce direct positive value co-creation effect.

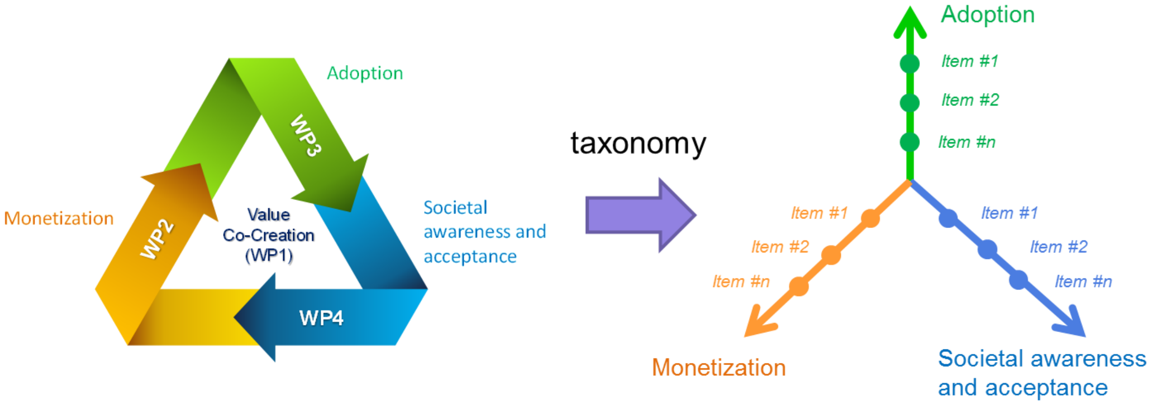


Figure 11: Co-creation principles of Unify-IoT

7. REFERENCES

[1] Accenturestrategy. Driving business strategies with the Internet of Things. https://www.accenture.com/us-en/insight-ceo-briefing-2015-productivity-outcomes?c=str_itdigdisrpfy16psgs&n=IIOT_Trends_-_IT&KW_ID=sjAsrSmCv_dc|pcrid|84332153775 (accessed on April 2016).

[2] CISCO. Industrial Internet of Thins Curriculum. http://www.rockwellautomation.com/global/services/training/certificates/cisco-iot.page (accessed on March 2016).

[3] Class Central. Internet of Things online courses. https://www.class-central.com/tag/internet%20of%20things (accessed on May 2016)

[4] Department for Continuing Education, University of Oxford. Data Science for the Internet of Things (IoT) https://www.conted.ox.ac.uk/h600-72, (accessed on April 2016)

[5] eExperfy. IoT Training: Internet of Things. https://www.experfy.com/big-data-hadoop-training/courses/iot-training:-internet-of-things (accessed on February 2016).

[6] FutureLearn. The Internet of Things – free online course. https://www.youtube.com/watch?v=lFhh5Up3kpA (accessed on February 2016).

[7] Huansheng Nin and Sha Hu. "Technology classification, industry, and education for Future Internet of Things", Volume 25, Issue 9, pages 1230–1241, September 2012.

[8] James Cook University. Bachelor Engineering in Electronic Systems and Internet of Things https://www.jcu.edu.au/courses-and-study/courses/bachelor-of-engineering-honours-in-electronic-systems-and-internet-of-things (accessed on March 2016).

[9] Jeremy Rifkin. Third Industrial Revolution. Palgrave Macmillan, 2011.

[10] Kortuem, Gerd; Bandara, Arosha; Smith, Neil; Richards, Michael and Petre, Marian (2013). Educating the Internet-of-Things generation. Computer, 46(2) pp. 53–61.

[11] Learning Center acm. Skillsoft Learning Programme. http://learning.acm.org/courses/index.cfm (accessed on February 2016).

[12] Michelle Selinger, Ana Sepulveda and Jim Buchan. Education and the Internet of Everything: How Ubiquitous Connectedness Can Help Transform Pedagogy. http://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/education_internet.pdf (accessed on January 2016)

[13] Miller, Vincent. Understanding Digital Culture. "Convergence and the Contemporary Media Experience." Sage.

[14] 2011.

[15] MIT Professional Education. Internet of Things : Roadmap to a Connected World. https://mitprofessionalx.mit.edu/courses/course-v1:MITProfessionalX+IOTx+2016_T1/about (accessed on February 2016).

[16] M. Roelands et al., "Orientation towards Do-It-Yourself Internet-of-Things Mass Creativity: What Can the Internet of Things Do for the Citizen?" Proc. Pervasive Computing Conf., 2010; www.slideshare.net/trappenlresearch-orientation-towards-doityourself-internetofthings-mass-creativity-concepts-pervasive 2010

[17] openSAP. How the Internet of Things and Smart Services Will Change Society. https://open.sap.com/courses/iot1 (accessed on April 2016)

[18] PTC. The PTC IoT Programme: A Passport to the Future for Students, Makers and Researchers. http://www.ptc.com/academic-program/products/internet-of-things (accessed on March 2016).

[19] QUALCOMM. Build your own Internet of Things with Coursera. https://www.qualcomm.com/news/onq/2015/10/13/build-your-own-internet-things-coursera

[20] (accessed on February 2016)

[21] UCI. Design, create and deploy a fun IoT device using Arduino and Raspberry Pi platforms. https://www.coursera.org/specializations/iot (accessed on February 2016).

[22] University of Wisconsin – Madison. Internet of Things Lab. http://www.iotlab.wisc.edu/ (accessed on February 2016).

[23] Vermesan. O and P.Freiss. 2014. Internet of Thing –From Research and Innovation to Market Deployment, River Publisher, Denmark

[24] Vision Mobile, Best Practices for IoT developer programmes, IoT Report Series, January 2016

[25] Waterford Institute of Technology: BSC in the Internet of Things https://www.wit.ie/courses/type/science/department_of_computing_maths_physics/bsc-hons-in-the-internet-of-things#tab=description (accessed on March 2016).

[26] World Bank 2015. ICT for Greater Development. http://siteresources.worldbank.org/extinformationandcommunicationandtechnologies/Resources/WBG_ICT_Strategy-2012.pdf (accessed on February 2016)

8. Appendix

8.1 Barriers for Innovation eco-system

This section provides an overview of the responses of the EPI-IOT projects, which have contributed their views on barriers for adoption of IoT platform ecosystems.

Project Name	Barriers for adoption of successful IoT innovation ecosystems
AGILE	• Delivering too late (becoming obsolete since IoT is moving too fast)/ not catching up with competition, • Fail to create user engagement, • Lack of user trust (or proper communication) in EU project outcomes • What are the incentives to entry for developers? These will be different for hard- and software builders and can vary wildly depending on the use case. Overall, the IoT market is still chrystallising and remains in a state of flux. The balance between the role of large corporations 'versus' SMEs and startups remains unclear. Showing the value proposition of AGILE as a platform and clearly communicating/demonstrating this will be a challenge.
TagItSmart	• How to maintain open communication between multiple project partners- • How to invent use cases utilizing the full capability of functional codes- Engaging consumers into ecosystem- Accessibility of information
SymbIoTe	• Lack of effective collaboration between academia/research performers and private commercial companies. • Lack of willingness of service providers to federate • Jungle of standards in the IoT domain • Closed systems not communicating each other - different devices, different operating systems, different formats, etc (IoT interoperability framework) • Security and Privacy issues for actracting End Users and stimulate market demand: End-users might be afraid of potential security leaks
INTER-IoT	• Interoperability of different IoT platforms requires that reliability, security, privacy and trust aspects are analyzed and considered in each layer. In particular, a cloud infrastructure bridging the IoT devices and data consumers needs to be secure because information flows from one IoT platform device through a non-owned platform may require special attention; moreover, privacy issues are critical in INTER-Health scenarios since sensitive data could be captured, transmitted and stored. Reliability of integrated IoT platforms need to be carefully addressed as it may be arising during the integration process. • Finally, trust is also a crucial challenge as integrated platforms need to be trustworthy with each other and selfish behavior can compromise the global system. Last but not least, medical doctors and port transportation operators need complex information, so it is necessary to incorporate information from different sources and additionally the data flow needs to traverse different infrastructures in a transparent way.

BIG IOT	Main challenge is not being "yet another project" addressing IoT interoperability issue. Past EU projects&initiatives did not solve the question of bridging the gap (among existing platforms and IoT stakeholders). What we see as barriers: • 1) Legislation: security and privacy issues and bureaucratic procedures for sensors management in public spaces. In addition, lack of harmonization among different national contexts is a barrier to flourishing of international marketplaces. • 2) Lack of a common semantic and interoperability standards is a specific topic addressed by the Project as a whole, but this is "the" issue; • 3) Investments needed to consolidate and standardize the BIG IoT model, once implemented, continuity and quality of marketplaces and APIs services are the big challenge for the future (how to ensure continuous and effective processes of data production, gathering and supply); • 4) Availability of big volumes of data, especially open data, with different business models (i.e. open data are free but with low quality; tariffs for high quality data, i.e. online updated data).
VICINITY	The principal barriers are not only technical since if there is an articulated requirement of IoT end-users for collaboration then the technical solution can be always provided. Although the VICINITY project will finish the analysis of IoT interoperability barriers in September 2016, here rare several preliminary thoughts on that topic: • Reluctance of potential IoT end-users to collaborate among themselves. Convincing business cases need to be offered to them to make their collaboration to happen. • Certain commercial players in the IoT field are benefiting on the existing vendor locks and therefore might be reluctant to support the interoperability efforts. • In certain domains such as health and energy there are significant regulatory barriers that can inhibit the IoT end-users collaboration. • Connecting different IoT ecosystems raises specific questions on security and privacy. These are: o New type of security issues are introduced by the fact that interoperability systems can implement security measures only on the links that are connecting different IoT infrastructures. Assuring security over data in the connected IoT infrastructures has to be done by the operators of those infrastructures. Question is how these operators can be obliged to implement the appropriate security measures. Can it be done with technology or specific regulations and certifications are needed, o Assuring the trust on data from IoT nodes in human sense. (E.g. how can the end-user trust on the authenticity of data that are provided by a device in a foreign infrastructure? Are those data authentic? Are they provided by the device as claimed? Does that device exist with the claimed attributes?). These issues become even more important once the data really become a marketable asset that can be monetized. o Once physical assets will be traded through IoT, there must be mechanisms that prevents false claiming and double selling of such assets. Example can be when an owner of residential energy

	generation resource offers certain amount of energy for sale. It shall be assured that the offered energy generation capacity exists and is sold only once.
bIoTope	• Conservatism in using open source technologies, access to data sources, integration on harmonized manner. • Credibility as commercial product, originated from an EC project,= Lack of market confidence in EU project outcomes. • Non maturity of Security/Privacy/Trust solutions in the IoT • Reluctance of industrial IoT players to support interoperability efforts • Lack (or slow evolution) of EU regulation about the data ownership from an end-user perspectives.