Grant Agreement No.: 723227
Call: H2020-ICT-2016-2017
Topic: ICT-37-2016
Type of action: CSA

D3.5: Interop Guidelines for IoT, version 1

Work package	WP3 - Standardisation and Interoperability
Task	Task 3.2 - Identification of global interoperability opportunities for IoT and 5G (with a focus on Europe and China)
Due date	31st October 2017
Initial submission date	15th November 2017
Re-submission date	16th February 2018
Deliverable lead	UPMC
Version	2.0
Authors	Amira Bradai, Detlef Fuehrer, Polo Zhang
Reviewers	Sebastien Ziegler

Abstract	In this Deliverable, the definition of interoperability is first introduced. Then, the existing situation with respect to funding and ongoing activities in Europe and China concerning IoT are identified. Moreover, an analysis of the requirements leading to a possible integration of activities between China and Europe is made. This will be considered as an input to the proposed model and guidelines for interoperability.
Keywords	IoT, China, Europe, Interoperability

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	16/10/2017	ToC drafted	Amira Bradai, Émilie Mespoulhes, UPMC
V0.2	29/10/2017	1st Draft version	Amira Bradai, UPMC
V0.3	30/10/2017	Inputs on Existing IoT activities	Detlef Fuehrer,UL
V0.4	31/10/2017	Inputs on IoT Situation in China from EXCITING Webinar Memo	Polo Zhang, BII
V0.5	02/11/2017	Formatting	Émilie Mespoulhes, UPMC
V1.0	15/11/2017	Final reviewing (v1)	Amira Bradai, UPMC, Martin Potts, Martel
V1.1	13/02/2018	Update, following 1st project review	Andrea Ferlini, Giovanni Pau, SORBONNE University
V2.0	16/02/2018	Final version (v2)	Andrea Ferlini, Émilie Mespoulhes, Giovanni Pau, SORBONNE University

Disclaimer

Copyright notice

Acknowledgment

This deliverable has been written in the context of a Horizon 2020 European research project, which is co-funded by the European Commission, the Chinese government and the Swiss State Secretariat for Education, Research and Innovation. The opinions expressed, and arguments employed do not engage the supporting parties.

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:	R*	
Dissemination Level		
PU	Public, fully open, e.g. web	✓
CI	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to EXCITING project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

EXECUTIVE SUMMARY

This report is an introduction to how the global interoperability testing, with the focus on the EU and China, is being used to validate research and innovation in the IoT domain. We identify the current status in both Europe and China (initiatives, federation projects, standards, platforms, key players, funding, etc.).

Nowadays, there is a growing interest in the IoT field. The number of industries that are moving towards a more digitalised ecosystem, is continuously increasing. This represents a rising trend for both China and Europe. Indeed, the massive use of heterogeneous Internet-connected devices, inevitably leads to the need of establishing some standards to ensure interoperability among different devices and domains.

This work helps to identify the requirements that have to be guaranteed to achieve the wanted results in terms of interoperability. Furthermore, it proposes some recommendations and hints for present and future interactions between China and Europe.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

6LowPAN: IPv6 Low Power Wireless Personal Area Networks
AII: Alliance of Industrial Internet of Things Innovation
AIOTI: Alliance for Internet of Things Innovation
CCSA: China Communications Standards Association
CNGI: China Next Generation Internet
CoAP: Constrained Application Protocol
DLNA: Digital Living Network Alliance
HTTP: Hyper Text Transfer Protocol
ICT: Information and Communications Technology
IoT: Internet of Things
IoT-EPI: IoT-European Platforms Initiative
LSP: Large Scale Pilot
MIIT: Ministry of Industry and Information Technology
MoF: Ministry of Finance
MQTT: MQ Telemetry Transport
OEM: Original Equipment Manufacturer
SME: Small and Medium Enterprise
SDO: Standards Developing Organisation
TCP: Transport Control Protocol
UDP: User Datagram Protocol
UPnP: Universal Plug and play

1 INTRODUCTION: OVERALL APPROACH

1.1 Definition of interoperability

Interoperability must not be confused with compatibility ("the capability of a functional unit to meet the requirements of a specified interface without appreciable modification") and portability ("the capability to be interpreted, understood, or executed on various types of data processing systems without conversion and with little or no modification").

Generally, interoperability is defined as "the ability of a system to work with, or use, the parts, or equipment, of another system". In a global market, interoperability is an essential topic of concern for IoT research and industrial communities. Coordination with countries around the world is therefore very important.

A representation of interoperability can be as follows:

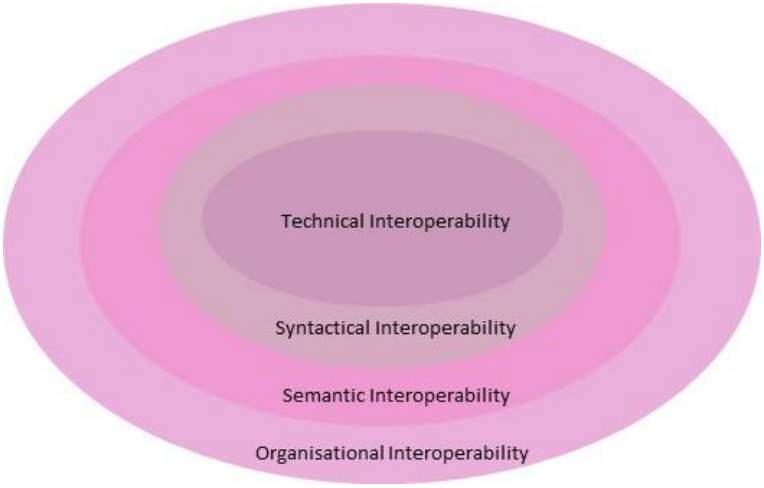

***Figure 1**. Interoperability*

- Technical interoperability is the ability to enable a machine-to-machine communication. It is about especially the protocols and the infrastructure needed.
- Syntactical interoperability is about the definition of the data syntax and encoding.
- Semantic interoperability is about the meaning of the content (the exchanged information has an unambiguous, shared meaning).
- Organisational interoperability is the ability of organisations to effectively communicate and transfer information. It is very linked to a successful technical, syntactical and semantic interoperability.

1.2 General objectives and goals

Interoperability provides advantages throughout the supply chain: users have a much greater choice of products and manufacturers can benefit from the economies of scale that a wider market brings.

The most important challenge in IoT is the enablement of seamless interoperability on a technical and

semantic level. Therefore, the IoT requires standards to enable horizontal platforms that are communicable, interoperable, and programmable across devices or industry.

Several aspects of interoperability have been addressed in the first year of the project, such as technical, semantic, syntactic and business interoperability. With the challenges of adding information from big data, there is a particular attention in many Standards Developing Organisations (SDOs) on addressing semantic interoperability.

The objective is then to analyse these challenges and requirements and to give a first version of guidelines to operate successful interoperability. This version will be refined and updated by the end of the project.

2 IOT INTEROPERABILITY FRAMEWORK IN EU AND CHINA

2.1 Existing IoT interoperability test activities

Currently, there are many alliances, SDOs, projects and platforms that are active and competing in the IoT field.

2.1.1 In Europe

2.1.1.1 Initiatives

This section describes the main European alliances that have a worldwide impact in the IoT area.

***Table 1**. IoT European initiatives*

	Description	Activities
IoT- Forum	Member-based organisation.	International dialogue. Organise events and conferences. Develop synergies with and among its members.
AIOTI Alliance for internet of Things Innovation	Non-profit organisation 13 working groups 170 members.	Reports. Develop a dynamic European IoT ecosystem.
IoT-EPI http://iot-epi.eu/	IoT-European Platforms Initiative.	European Initiative addressing IoT platform development. Formed to build a vibrant and sustainable IoT-ecosystem in Europe, maximising the opportunities for platform development, interoperability and information sharing. Its core is composed by 7 EU-funded H2020 research and innovation projects: Inter-IoT, BIG IoT, AGILE, symbIoTe, TagItSmart!, VICINITY and bIoTope.

IoT-European Platforms Initiative (IoT-EPI):

The IoT-European Platforms Initiative (IoT-EPI) is further described in Figure 2. We have highlighted the important projects that are then described in Table 2.

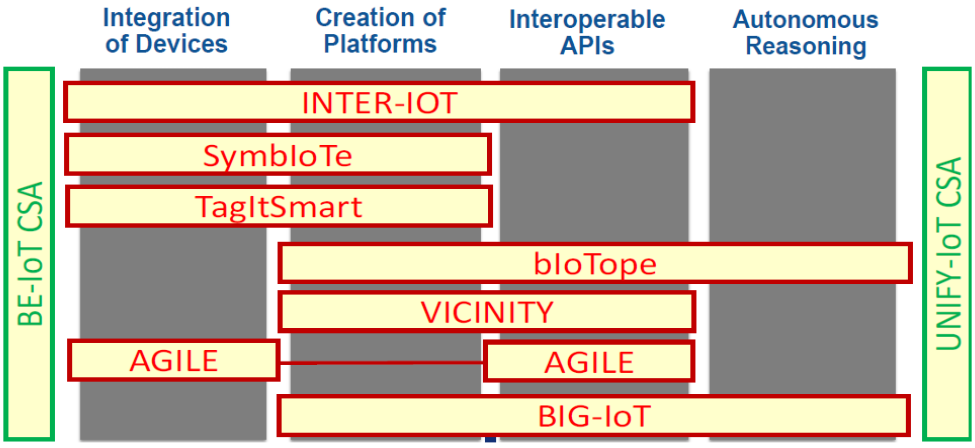

***Figure 2**. IoT-European Platforms Initiative (IoT-EPI) projects*

2.1.1.2 Projects

***Table 2**. IoT projects in Europe*

	Description
Onelab	OneLab is designed to be able to test a variety of diverse networked communication environments, including IoT networks with mobility and sensing capabilities, ad-hoc wireless and wireless broadband access networks, global, public, fixed-line Internet, Cloud and SDN networks. Both wireless and fixed-line emulated environments are available.
Fiesta-IoT	FIESTA-IoT (Federated Interoperable Semantic IoT Testbeds and Applications) The main goal of the FIESTA project is to open new horizons in the development and deployment of IoT applications and experiments. The project operates both at EU and global scale, and it is based on the interconnection and interoperability of diverse IoT platforms and testbeds. FIESTA-IoT is providing a meta-testbed IoT/Cloud infrastructure to enable the submission of experiments over the interconnected/interoperable underlying testbeds. Hence, researchers and engineers will utilise a single-entry point to all FIESTA-IoT EaaS services using a single set of credentials. They will be able to design and execute experiments across a virtualised infrastructure i.e. access the data and resources from multiple testbeds and IoT platforms using a common approach. FIESTA-IoT offers tools i) to design and execute experimental workflows, ii) dynamically discover IoT resources, and iii) access data in a testbed agnostic manner. FIESTA-IoT provides IoT Experiment as a Service atop of a middleware infrastructure that adapts and federates existing IoT platforms and testbeds. This entails the adaptation of the testbeds data to a common FIESTA-IoT ontology (i.e. compliance to common semantics). Necessitating also the provision of a common API standard, to access the testbeds IoT services and thus the wealth of heterogeneous IoT data in them.
Fed4FIRE	Fed4FIRE is an initiative to bring together heterogeneous facilities across

	Europe so as to target experimentation across the whole Future Internet field i.e., networks, software and services, and IoT. Fed4FIRE federates testbeds, bringing together Cloud, IoT, wireless, wireless mobile, LTE, cognitive radio, 5G, OpenFlow, SDN, NFV and network emulation technologies.
F-interop	F-interop is a European research project which studies and develops online interoperability and performance testing tools as a support to the emerging IoT-related technologies from standardisation to market introduction. It also supports research, product development by SMEs, and standardisation processes. Its aims and objectives are: - to integrate and extend several European testbed federations with a shared "Testbed as a Service". This is done by interconnecting three European testbed federations (Fed4FIRE, OneLab, IoT Lab), bringing together over 32 testbeds and 4,755 nodes; - to research and develop online testing tools for the IoT. The tools are used to test interoperability, conformance, scalability, Quality of Service (QoS), Quality of Experience (QoE), and Energy efficiency; - to support IoT standardisation and enable cooperation with the industry. This will be possible thanks to a close collaboration with SDOs such as ETSI, OneM2M, IETF and W3C, combined with the research and development of online certification and labelling mechanisms. F-Interop will enable an easier participation of researchers and industries in the standardisation process; - to organise open calls for SMEs and developers, using and enriching the testing platform with additional modules and extensions (additional test tools, tests specifications, etc.). F-Interop works in close collaboration with several standardisation bodies. It directly contributes to three IoT standardisation processes: OneM2M, 6TiSCH (IETF) and the Web of Things (W3C). It also explores the possibility to support and enable new online certification and labelling mechanisms, including the "IPv6 Ready" logo.
IoT Lab.eu	IoT Lab has recently concluded. It unified IoT and crowdsourcing/crowd-sensing testbeds, including smart campus, smart buildings and smart offices testbeds.
SOFIA2	SOFIA2 is a middleware that allows the interoperability of multiple systems and devices, offering a semantic platform to make real world information available to smart applications (IoT). It is multi-language and multi-protocol, enabling the interconnection of heterogeneous devices. It provides publishing and subscription mechanisms, facilitating the orchestration of sensors and actuators in order to monitor and act on the environment. SOFIA2 is one of the several IoT platforms which has the potential to be considered for the interoperability of heterogeneous IoT platforms in this project.
INTER-IoT	The INTER-IoT project aims at the design, implementation and experimentation of an open cross-layer framework, an associated methodology, and a set of tools to enable voluntary interoperability among heterogeneous IoT platforms. The project will enable the effective and efficient development of adaptive and smart IoT applications and services. It

	will work with several heterogeneous IoT platforms, spanning single and/or multiple application domains. The developed framework will be tested in two application domains: port transportations and logistics, and mobile health. Additionally, it will be also validated in a cross-domain use case.
BIG IoT	The objective of BIG IoT (Bridging the Interoperability Gap of the Internet of Things) is not to develop yet another IoT platform, as several other projects already do. Instead, it will establish interoperability by defining a unified Web API for IoT platforms: the BIG IoT API. This Web API is aligned with the standards currently developed by the W3C Web of Things group. The project approaches the existing interoperability gap based on (1) a common Web interface, called the BIG IoT API, (2) a semantic description of resources and services, as well as (3) a marketplace as the core driver of the ecosystem. This has to provide functionalities such as authentication, discovery and charging. The BIG IoT API will be designed as an open community process and the project consortium will engage with current standardisation initiatives to receive inputs and deliver contributions. As part of the project, 8 smart object platforms will implement BIG IoT API. Hence, allowing a real and widespread exploitation of their data and application heritage. The BIG IoT Marketplace will allow different IoT providers to easily offer and monetise accesses to their resources as well as IoT consumers to discover and use them.
VICINITY	The objective of VICINITY is to build and demonstrate a device and standard agnostic platform for IoT infrastructures that will offer "Interoperability as a Service". It will rely on a decentralised and user-centric approach that offer a complete transparency across vertical domains while retaining full control of the ownership and distribution of data.
bIoTope	The bIoTope platform aims to enable IoT product and service providers to develop and deploy IoT solutions utilising heterogeneous information and services together with multiple systems (OpenIoT, FIWARE, city dashboards, etc.). Based on recent IoT standards, as O-MI (Open Messaging Interface) and O-DF (Open Data Format), bIoTope applies an “Everything as a Service” concept to enable a rapid development of new IoT systems and a reduction of development costs.
UNIFY-IoT	UNIFY-IoT is the “working partner” of the Alliance for Internet of Things Innovation (AIOTI) and the Internet of Things European Research Cluster (IERC) by coordinating and supporting the activities on innovation ecosystems, IoT standardisation, Policy Issues, Research and Innovation. The UNIFY-IoT project’s website is the place to get all the news, information about events and developments regarding the IoT-EPI initiative. The project’s objectives are to stimulate and support the collaboration between IoT projects and potential platforms. The support aims to sustain the whole IoT ecosystem. It focuses on complementary actions, e.g. fostering and accelerating the acceptance of IoT technology, as well as on the means to understand and overcome the obstacles to the IoT deployment and value creation.

2.1.1.3 IoT Platforms

IoT platforms are emerging to simplify devices’ connectivity management and application

enablement.

According to « https://www.xipi.eu/Infrastructures », there are nine dedicated IoT platforms in Europe.

***Table 3**. IoT platforms in Europe*

	Country	Description
Fit – Future Internet of Things	France	FIT is a large-scale testbed for testing performance, interoperability, and security. It uses nine sites across France, including Paris, Grenoble, Lille, Strasbourg, and Lyon. It is part of the OneLab federation.
CROSS-TEC LABORATORY of ENEA TECHNOPOLE in Bologna	Italy	The CROSS-TECH structure is composed of two main infrastructures: 1- Testbed environment for standard compliance and for networked enterprises interoperability; 2- Lab for prototyping, 3D design and production technologies as a support to the designed based goods. Notice that while the laboratory is already running, the testbed is not fully developed, yet.
Fraunhofer FOKUS SmartTV Lab	Germany	The Fraunhofer FOKUS Smart TV Lab offers a comprehensive test and development environment for cutting-edge, hybrid TV technologies and devices. Including brand new TV formats, interactive content, HbbTV and cross-platform applications. The Lab provides support for both application and content providers, as well as CE manufacturers. Thus, they allow their customers to test and validate their solutions against standards (HbbTV, CE-HTML) in regard to interoperability.
Open Overlay Lab (UPC)	Spain	The Open Overlay Lab offers a running overlay network for experiments. The experimental network spans over 20 countries with about 200 nodes and is managed by UPC.
PerformNetworks	Spain	PerformNetworks is a FIRE+ experimental platform. Its main goal is to offer a realistic experimentation environment able to deal with LTE, LTE-A and future networks. The testbed is based on commercial off-the-shelf solutions (both in the radio and core network), software defined radio equipment and conformance testing equipment. It offers a wide range of possibilities like covering

		pilots, interoperability, performance evaluation, QoS, QoE and more. PerformNetworks is operated by the MORSE research group at the Universidad de Málaga.
ETOMIC SONoMA	Hungary	SONoMA is a common and extensible network measurement platform. It proposes an alternative to define and perform distributed network experiments. This SOA-based approach aims to significantly decrease the required time and effort for network experiment implementation.
Wisebe hobnet-crowdsourcing	Switzerland	It offers the ability to interconnect many heterogeneous IoT devices, by providing support for testbed federation.
SmartSantander Testbed	Spain	The SmartSantander testbed provides a set of Smart City facilities through large-scale deployments of sensor networks. Applications and services can be developed on the top of it. Furthermore, Sunrise is a federation of sensor network testbeds that provides monitoring and exploration of the marine environments. In particular, they support experimentation in terms of the underwater IoT.
Intel Intelligent Systems Framework		Intel Intelligent Systems Framework is a set of interoperable solutions to address, connect, manage, and secure devices in a consistent and scalable manner. It provides solutions that allow smart objects to Connect, Share and Drive value from the Data. The Intelligent Systems Framework permits OEMs to shift their investments from achieving interoperability to unlocking the value of data. ISF allows faster-time-to-Market, since it enables innovative services (due to the exploitation of the unlocked value of the data), and lower development and deployment costs. Intel and its ecosystem partners supply the components to address connectivity, manageability, and security. The aforementioned components, as well include software and middleware from Wind River and McAfee. ISF is a product which can be considered as an interoperability device-to-device layer.

2.1.1.4 The IoT European Large-Scale Pilot Programme

Under the H2020 programme, the European Commission is currently co-funding five IoT Large-Scale Pilots. The IoT European Large-Scale Pilot Programme provides a financial contribution of €100 million from the EU. The projects started in January 2017 and address the following areas:

- Smart living environments for ageing well (ACTIVAGE)
- Smart Farming and Food Security (IoF2020)
- Wearables for smart ecosystems (MONICA)
- Reference zones in EU cities (SYNCRHONICITY)
- Autonomous vehicles in a connected environment (AUTOPILOT)

The coordination of these projects is supported by two additional CSA projects: U4IoT and CREATE-IoT. A detailed description about these LSP Programmes is given in the EXCITING deliverable D4.1 [1].

Through the selected IoT Large-Scale Pilots, the EU seeks to support the testing and experimentation of new IoT related technologies. These Pilots are expected to also accelerate the standards setting across different business sectors, thereby boosting further the IoT technology. Privacy and security, business models, usability as well as other legal and social challenges, are also important factors that the EU's IoT Large-Scale Pilots are tackling.

2.1.1.5 Standards

As we introduced before, the AIOTI includes 13 working groups [2], as shown in the following Figure 3:

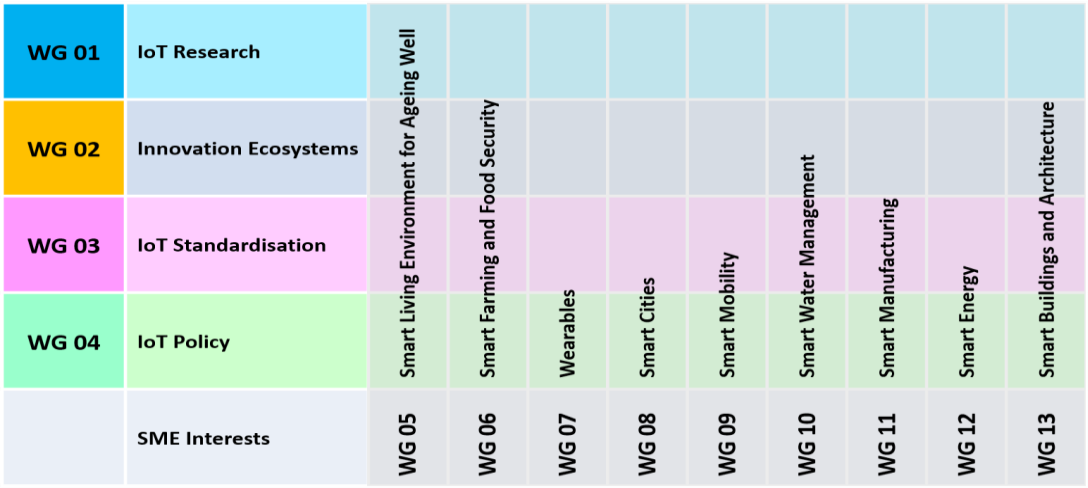

***Figure 3**. AIOTI Structure*

WG 03 in the AIOTI identifies and, where appropriate, makes recommendations to address existing IoT standards. It analyses gaps in standardisation, developing strategies and use cases aiming for:

- The consolidation of architectural frameworks, reference architectures, and architectural styles in the IoT space;
- The (semantic) interoperability;
- The personal data & personal data protection to the various categories of stakeholders in the IoT space.

To better understand how to develop those strategies, an overview of the IoT standards is needed. Standards are needed for interoperability both within and between domains. Interoperability ensures cooperation between the engaged domains, being more oriented towards IoT deployments in real-life situations. The most important SDOs are identified below. More details can be found in the EXCITING deliverable D3.1:

- **ETSI** [http://www.etsi.org/] Initiative: (European Telecommunications Standards Institute) It produces globally-applicable standards for ICT, including fixed, mobile, radio, converged broadcast and internet technologies.
- **IETF** [http://www.ietf.org/] (Internet Engineering Task Force): The mission of IETF is enhance the Internet. That is done by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet itself. The IETF Mission Statement is documented in RFC 3935. The IETF has an IoT directorate to deal with IoT specificities. The ETSI Standards Association addresses the organisational interoperability.
- **IEC International Electro Technical Commission**: It covers all the electro-technical aspects, from plugs, wires, voltage levels to automation, control and management. Various protocols are supported, such as: IEC61850, IEC 61968/61970 (CIM), XMPP, DLMS/COSEM, OPC-UA. The IEC Standards Association addresses the syntactical, technical, and semantic interoperability.
- **OneM2M** [http://www.OneM2M.org/]: The purpose and goal of OneM2M is the development of technical specifications that have to address the need for a common M2M Service Layer. The Service Layer should be easily embedded within various hardware and software. Furthermore, it has to rely upon the myriad of connected devices in the field of M2M application servers worldwide. A critical objective of OneM2M is to attract and actively involve organisations from M2M-related business domains such as: telematics and intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc. The OneM2M Standards Association addresses the syntactical, technical, and semantic interoperability.
- **IEEE Standards Association**: Its mission is the advancement of technology for the benefit of the humanity. It perpetrates that by providing a globally open, inclusive and transparent environment for market relevant, voluntary consensus standardisation. The various standards of the IEEE Association address all the different levels of interoperability.
- **3GPP** (3rd Generation Partnership Project) [http://www.3gpp.org/]: The project covers cellular telecommunications network technologies, including radio accesses, the core transport networks, and service capabilities, like codecs, security, QoS, etc. providing a complete system specification. 3GPP specifications and studies are contribution-driven. The member companies (originating from its Organisational Partners) give the contributions, they are organised into Working Groups and Technical Specification Groups.
- **OASIS**: It is a non-profit consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, IoT, cloud computing, energy, content technologies, emergency management and other areas. OASIS describes IoT as (OASIS, "Open Protocols," 2014): "System where the Internet is connected to the physical world via ubiquitous sensors." OASIS describes the ubiquity of sensors as existing in: "every mobile, every auto, every door, every room, every part, on every parts list, every sensor in every device in every bed, chair or bracelet in every home, office, building or hospital room in every city and village on Earth."

Each application in the IoT is recommended to use standards based on well-known organisation (e.g.

ETSI, IEEE, W3C, OneM2M, ITU-T, ISI, etc.) For that reason, it is necessary to map the standards to the protocols provided for the different layers in the ISO communication, as proposed by the AIOTI (given in Figure 4 provided by the WG 03). As more real-world applications will be operated on top of standardised IoT infrastructure, this needs to be considered in future IoT standards.

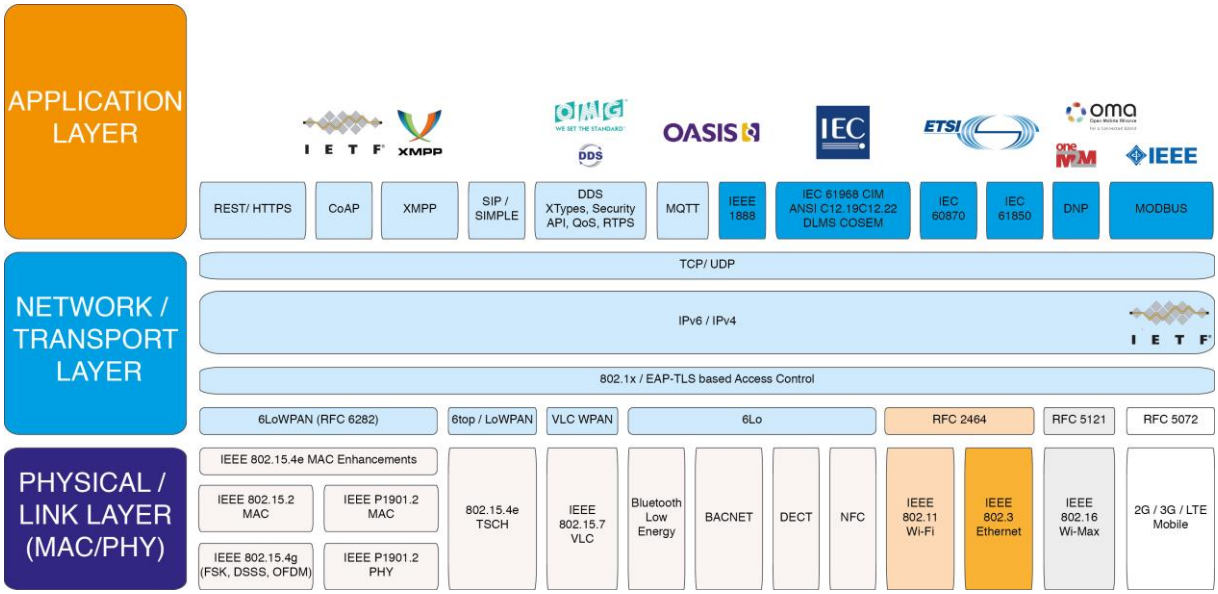

***Figure 4**. Mapping of the different standards to the protocol layer stacks*

2.1.2 In China

IoT activities have a great importance in China, too. In the following, a description of the initiatives and the projects is given.

2.1.2.1 Initiatives

Here now follows, a description of the organisational structures:

***Table 4**. IoT Initiatives in China*

Body	Description	Activities
CCSA China Communications Standards Association	It is a non-profit organisation, comprising: - 11 Technical Committees (TCs) - 9 Special Task Groups (STGs) The members are from: - operators, internet service providers, manufacturers, standardisation and R&D institutes, design units, universities, societies, etc. CCSA is a partner of both 3GPP and OneM2M.	CCSA is the main working platform for the development of ICT industry and national standards in China.

AII Alliance of Industrial Internet of Things Innovation	Is an open, cross-sector, non-profit and social organisation	The AII is working on a platform to ensure communication and cooperation for technology and standards. Their goal is the construction of a technology and standards-oriented framework for the industry. They also promote the development of the key technical standards. Furthermore, the AII promotes their standards to establish them as national or industry standards. It also encourages international cooperation towards the development of standards for the industrial internet.

2.1.2.2 Testbeds

In the following table, a description of eight testbeds in China is given.

***Table 5**. IoT testbeds in China*

	Description
China Telecom	China Telecom is a core network of the CNGI project with heavy investments in IoT infrastructure in China. It aims to have nationwide narrow-band IoT (NB-IoT) coverage and has already released the enterprise standard "NB-IoT equipment v1.0". This standard includes ITS, logistics, security monitoring, public utilities, intelligent manufacturing, modern agriculture, smart street lighting, video monitoring, intelligent financial POS information, waste management, smart manhole covers, and auto-parking. Over 400 NB-IoT base stations have already been installed covering the entire city of Yingtan in Jiangxi province.
China Mobile	China Mobile is a core network of the CNGI project and runs the OneNET open cloud platform which offers PaaS and SaaS. It offers a variety of network access protocols and accesses to networked devices, smart homes, smart cars, and wearable devices. China Mobile offers intelligent parking including online parking queries, online booking, reverse searches, and online payments. They have conducted NB-IoT and eMTC trials in Hangzhou, Shanghai, Guangzhou, and Fuzhou and now have 5000 stations. As of 2015, they have over 65 million IoT terminals registered with China Mobile.
China Unicom	China Unicom is a core network of the CNGI project and will launch NB-IoT LSPs in at least six cities for testing purposes.

	Their IoT-service platform and NB-IoT private network is supporting smart cities construction, smart meters, smart parking, environmental monitoring, and intelligent manufacturing in Shanghai. Over 3000 base stations are being built in 2017.
State Grid	State Grid will experience IPv6-sensors deployment with a minimum transmission speed of 250kbps. That will permit power transmission monitoring and, with the help of Mobile IP technology, power line monitoring together with mobile meter reading.
Yingtan Smart City	Yingtan Smart City has built a global coverage of NB-IoT business network, with 135 NB-IoT base stations. Several IoT business have been deployed, including smart cities management, smart street lights, smart parking, smart logistics and smart agriculture.
IoT Platform in BUPT	The IoT platform in BUPT includes both an Android-based gateway and Cloud service. It is an open platform - easy to extend to new scenarios - supports RESTful architecture and heterogeneous devices (IP and non-IP), and represents data in XML/JSON. An example of its use is the smart classroom where it is possible to control the lights and environmental controls as well as to monitor the number of students and what devices they have with them. New functions can easily be added while old functions can easily be updated. Cloud-computing allows for the possibility of Big Data Analysis too.
IoT Testing Platform in Southeast University	The IoT testing platform includes 200 sensor nodes. The users are able to remotely control nodes (both malicious and legitimate), realis and the base stations for testing purposes. The protocols to be tested can be downloaded remotely as well. The performance metrics include throughput, loss rate, delay, average path, average energy consumption and scalability of network, etc.
Mobike	Mobike is created by Beijing Mobike Technology Co., Ltd., which is a fully station-less bicycle-sharing system currently deployed in Beijing, Shanghai, Guangzhou, Shenzhen, Chengdu, Ningbo, Xiamen, Foshan, Zhuhai and Wuhan. It is the world's largest bicycle operator, and recently made Shanghai the world's largest bike-share city. Mobike works with China mobile, Vodafone, Ericsson, Qualcomm, and Huawei to create a seamless mobile networking system. It is also the first one to use NB-IoT in the real case.

2.1.3 Analysis of interoperability requirements

In order to reach IoT interoperability, the key idea is to consider it across those important layers of the hardware/software stack:

- Networking layer
- Device layer
- Middleware and service layer
- Data and semantic layer

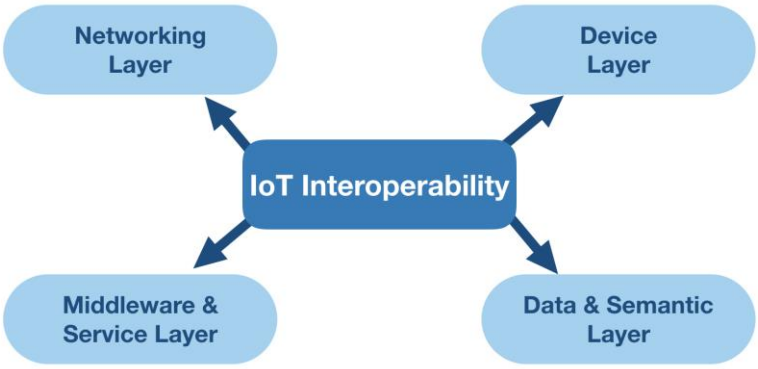

***Figure 5**. IoT Interoperability layers*

2.1.3.1 Networking Layer

IoT devices and applications are heterogeneous, multi-vendors, multi-services and largely distributed. As a consequence, the risk of non-interoperability is extremely high. Thus, it is vital to guarantee that network components will interoperate to fully unleash the value of the IoT. Interoperability requires interworking standards with less complexity and must be achieved amongst the various element of the IoT.

At the networking layer, different protocols can be used, e.g. 6LowPAN, TCP/HTTP, UDP/CoAP. In addition, communication between devices and a local gateway can be based on universal plug and play (UPnP) or DLNA. Furthermore, the use of buses running the MQTT protocol can also be used to implement asynchronous communications between entities.

The most promising solution for interoperability, on which to achieve agreement, is IPv6, with its specific version for constrained devices, 6LoWPAN, even though its adoption is currently slow.

2.1.3.2 Device Layer

The unification, convergence and accessibility of the platforms require Device-to-Device (D2D) communication. Different communication protocols are used at the device layer, and each device has to be defined, standardised and certified (Wi-Fi Alliance, WiMAX).

2.1.3.3 Middleware and Service Layer

The middleware provides general and specific abstractions to help build up IoT systems. It should be able to receive data from multiple types of sensors and support the semantic modelling. To accelerate the development of new services with other standards, inevitably requires a common access API library. For instance, the API provided by the onePOWER platform is more generic, thereby ensuring more flexibility. To facilitate the application implementation, and thus to support the uptake of the standards, the API bindings for relevant programming languages should be defined as part of the standard.

2.1.3.4 Data and Semantic Layer

Semantic interoperability can be achieved through commonly agreed information models (e.g., defined with ontologies) of the terms used as part of the interfaces and exchanged data.

This is why it is recommended to use standardised models and message formats for representing data. In fact, when interworking nodes, residing in two different service provider domains, exchange messages, the data format and payload data size of the messages must be interoperable and conform to the one used by each Service Provider. Therefore, a negotiation process regarding data format and/or data size should be considered essential.

2.2 Available funding for IoT interop projects

In Europe:

From the Work Programme Leadership in Enabling and Industrial Technologies by Information and Communication Technologies:

IoT is supported for 2014-2015 in ICT-30-2015: Internet of Things and Platforms for Connected Smart Objects, with:

- ICT30.a: €48M.
- ICT30.b: €1M.

IoT is supported for 2016-2017 in ICT-04-2017: Smart Anything Everywhere Initiative, with €26.5M

IoT is supported for 2018-2020 in ICT-27-2018-2020: Internet of Things, with €1.5M

In China:

The key IoT players in China are Huawei, the largest and leading player in IoT, and the most active application and implementation areas at the moment are:

- Wuxi – leading IoT location
- Shenzhen

By 2015, the IoT industry in China had reached 750 billion RMB (€101 billion) with 29.3% year-on-year growth rate. This accounted for 31% of the total global volume.

By 2020, the overall IoT industry in China is predicted to reach 1.8 trillion RMB (€243.5 billion).

A series of policies and Action Plans have been released since March 2011 when the "12th Five Year Plan on IoT" to boost the IoT development in China was officially released.

The original plan covered 9 key development sectors: smart industries, smart agriculture, smart logistics, smart traffic, smart grid, smart environmental protection, smart security, smart healthcare, and smart home.

In April 2011, the MoF and MIIT jointly released special funding for IoT development. During 2011 to 2014, the following projects were funded: 110, 149, 122 and 101.

The cumulative funding throughout these 4 years was over 2 billion RMB. Each project could be funded for ~ 3-5 million RMB.

In 2013, several Chinese ministries jointly committed and published the document: “IoT Development Special Action Plans (2013-2015)” which included 10 specific Action Plans. Within the series of supporting policies and Action Plans, were Pilots of national IoT key application demonstration projects and areas that were implemented during 2014-2016.

3 ANALYSIS OF THE INTEROPERABILITY SITUATION BETWEEN CHINA AND EU

3.1 Definition of the strengths of the Chinese and EU models

3.1.1 Situation in China

Recently, China's IoT application development (explained in [5]) has been widely applied in many fields and areas such as:

- Industrial manufacturing, to reduce the cost, save energy and reduce emissions;
- Agriculture, to reduce the personnel costs and improve the overall economic benefits;
- Energy conservation and environment protection, especially for large industrial parks;
- Health care, community and public safety, public services, to be able to expand in time and space;
- Urban management, pipe network monitoring and intelligent transportation;
- Network structure (the release of the international standard IUT-T Y.2086 led by CAICT was completed in 2015).

Huawei's LTE-M system, which features low power consumption, low cost, low data rate and wide coverage, meets the needs of M2M applications and is now in the experimental stage for business deployment. Both China Mobile and China Telecom are vigorously promoting the construction of M2M platforms. At present, both provide full network operation support and have launched a range of IoT products in transportation, health care, environmental protection, logistics, water supply and other fields. Studies on the optimisation of the existing networks and the M2M narrowband networks represent the current focus of activity. China is promoting standardisation work for network optimisation, including terminal triggering, low power consumption and wide-area coverage, as well as detecting and resolving network congestion.

The Chinese government attaches importance to the IPv4 addresses shortage, towards which the international attention gravitates, and the transition from IPv4 to IPv6 has become consensus. The Chinese government and research institutions devote a lot of effort to broad research and in-depth practice, aiming at the realisation of an advanced deployment as soon as possible. In addition, they are racing to gain a commanding position in the market before large-scale IPv6 industrialisation takes hold.

In accordance with the National Strategically Emerging Industries Development Planning in the 13th Five-Year Plan and the National Information Planning in the 13th Five-Year Plan, to facilitate the healthy development of the new generation of information technology, China will increase its investments in information infrastructure construction. During the 13th Five-Year Plan, new generation Internet and other network infrastructure will be deployed and applied in succession. That will give a great impetus to the development of IPv6.

Generally, IPv6 is gaining momentum in its deployment in China. However, due to various objective reasons, even though government bodies have given high-level support, the progress of its promotion and penetration have not lived up to expectation; with relatively few applications still in the industrial Internet. It has to be noticed that the slowness of IPv6 deployment, puts increasing pressure on the

availability of IP addresses that are so vital for IoT applications. It is therefore expected that IoT development and deployment will accelerate the transition to IPv6 with serious efforts to enforce the policy implementation.

3.1.2 Situation in the EU

Europe is in an excellent position to become a global leader in IoT as stated by the European Commission [6]. The main strengths of the European ICT are in Business-to-Business (B2B) software and services, embedded systems and in particular in the application of ICT to complex system-level solutions in various industrial and societal domains. Leveraging on traditional European industrial and social system strengths by augmenting solutions with ICT in, for example, Smart Grids, transportation and logistics, cyber-physical systems, eHealth, active & healthy aging, and digital inclusion is necessary for European industry.

3.2 Potential challenges related to the integration of EU/Chinese test platforms

Cyber security for IoT has become a new challenge that must be given close attention. At present, there are an increasing number of IoT devices that have loopholes, covering an ever wider and broader range. This is true for sensors, cameras and other items, across the whole range of industrial devices used for manufacturing, control, operation, maintenance and logistics, some of which are part of critical infrastructure. All of those need strict security regulation and control to avoid interruption to key services.

Therefore, in the process of IoT industrialisation, technicians should underline the study of secure coding and secure design. At the same time, we call on the government bodies to formulate relevant policies and standards to prevent any vulnerabilities that might become opportunities for IoT attacks.

4 PRELIMINARY OPPORTUNITIES AND GUIDELINES FOR INTEGRATION BETWEEN EU AND CHINA

4.1 Proposed model

4.1.1 Standards and Policy

Regarding interoperability, IoT technological implementations should ideally rely on a commonly agreed basis. So, international standards are needed to allow worldwide use of products and solutions. The standardisation of a reference architecture model for IoT is also needed to achieve the goal of compatibility and interoperability across industrial domains. This reference architecture model (like the one proposed by the European research project FI-WARE) will be the base of domain-specific refinements and extensions. Thus, it will be possible to mainly address common open platforms that support the needed communication and data capturing services. These common open platforms can be shared by multiple application providers.

For IoT standardisation, it is of huge importance to have relevant players from all the most important industrial domains involved. If IoT standards are defined only from the viewpoint of a single domain (e.g. telecommunications domain), they will not match the needs and requirements of other domains, leading to contradicting solutions for the IoT goal of interoperability across industrial domains.

We encourage the development of international standards, innovation cooperation, research and publications. This will act as a reference and will push enterprises even individuals to participate in cooperative projects between EU and China.

4.1.2 Technical cooperation

Twinning activities should be encouraged between China and Europe by carrying out technical cooperation in strategic sectors on key product development. This can be done by defining joint projects and by exchanging technical staff and industry researchers, to take full advantage of the available knowledge in both regions.

4.1.3 Legal and policy

This includes all the legal and regulatory aspects. The single digital market is an objective that can be realised. IoT services can have many societal benefits but they are often blocked by the regulatory framework still in place. A balanced view between the benefits of new technological developments and associated risks and potential issues is needed. Trust, security and privacy are important aspects of IoT which have to be guaranteed in order to achieve wide acceptance in the society, as are consumer protection, autonomy, functioning competition and choice.

4.2 Action plan

As a first step, we will organise workshops with some interop projects (F-interop, Fed4FIRE), where we can discuss further some good IoT interoperability practices. In such events, we can profit from experiences in both the research and the industry fields. We will focus our attention on the data interoperability and the protocols/standards challenges. Many other issues will be tackled: e.g. How to build a reference model and IoT architectural framework? How to encourage the technical and standards cooperation?

CONCLUSION

This report is the first version of the Interop Guidelines for IoT. A second version is expected in one year (M24 of the project). However, an overview of IoT activities and requirements for interoperability already allows us to make the following observations:

- Interoperability is a key topic of concern for IoT research, standards and industrial communities.
- Guidelines are welcome and expected to help addressing collectively interoperability between China and Europe.
- To push forward IoT integration, all parties must work together (research, industry, etc.)
- Security is a very important challenge to consider when federation is taking place.

After having presented a comprehensive summary of the variety of ongoing IoT applications and projects between EU and China, the need of interoperability can be easily identified. The development of international standards is becoming crucial to ensure interoperability among different vendors, markets, industry sectors and countries.

To speed up the standardisation process, and encourage research on the topic, workshops between China and Europe can be a key activity. In fact, thanks to these workshops it will be possible to boost the interest of the research community and to get industries to push on the standardisation bodies. Both are crucial factors to speed up the development of the standards, needed to guarantee the interoperability of the huge heterogeneity intrinsic to the IoT.

REFERENCES

[1] Na Yi, Rahim Tafazolli, Christopher Hemmens, Cédric Crettaz, Xiaohong Huang, Amira Bradai, Outline of the Pilot Concept and Identification of Ongoing IoT and 5G Large Scale Pilots between Europe and China, EXCITING Project.

[2] AIOTI Working Groups: https://aioti.eu/working-groups/

[3] Latif Ladid, EU-China 5G – IoT Exciting Opportunities and Challenges.

[4] Integration, interconnection, and interoperability of IoT systems,

[5] China Academy of Information and Communication Technology (CAICT), European Commission – DG CONNECT, EU-China Joint White Paper on the Internet of Things, January 2016

[6] CONNECT Advisory Forum, Internet of things, the next revolution