Expert Group Position Paper on Internet-of-Thing Architecture

title
EU-China Common Views: Internet-of-Things Architecture

Date of publication	Document version:
28/10/2014	V1.0

Dissemination level		
PU	Public	**X**
PP	Restricted to other invited experts	
RE	Restricted to a group defined by the expert group	
CO	Confidential, only for members of the expert group	

Authors (organizations) :

EU-side:
- Dr. Francois Carrez (University of Surrey / Institute for Communication Systems – United Kingdom)
- Philippe Cousin (Easy Global Market – France)
- Dr.PayamBarnaghi (University of Surrey / Institute for Communication Systems – United Kingdom
- GianmarcoBaldini (JRC – EC[1])
- Prof. John Soldatos (Athens Information Technology - Greece)
- Dr. Martin Bauer (NEC Research - Germany)
- Pasi Hyttinen (VTT – Finland)

China-side:
- Haihua Li (CATR,MIIT - China)
- Yang Liu (CATR,MIIT - China)
- Xueli Zhang (CATR,MIIT - China)
- Xiaohui LI (CECT-China)
- Decheng Zhu (CECT-China)
- Jie Shen(WSN-China)

Abstract :

Based on the co-research of EU-China advisory Group on Internet of Thing (IoT), EU-China reached some common views on the IoT architecture design, that is:IoT architecture design methodology, horizontal capabilities, identification resolution, semantic, security are important aspects for IOT architecture development, which should be pay attention to. Moreover, the work and research on the IoT Reference Architecture and Modelare still in progress.EU-China advisory Group on Internet of Thing will improve the research continually, and some further actions are already planned

Keywords :

EU-China initiative, Internet of Things, Architectural Reference Model, Interoperability

[1] Disclaimer: The contents of section 2.5 (Security) are the views of the author and do not necessarily represent an official position of the European Commission)

Disclaimer

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Any liability, including liability for infringement of any proprietary rights, relating to use of information in this document is disclaimed. No license, express or implied, by estoppels or otherwise, to any intellectual property rights are granted herein. The members of the expert group do not accept any liability for actions or omissions of expert group members or third parties and disclaims any obligation to enforce the use of this document. This document is subject to change without notice.

Revision History

The following table describes the main changes done in the document since it was created.

Revision	Date	Description	Author (Organisation)
V0.1	1st Sep,2014	Creation (IoT ARM focussed)	Francois Carrez, Martin Bauer, PasiHyttinen
V0.2	30th Sep,2014	New TOC + new content	Haihua Li, Yang Liu
V0.3	21stOct, 2014	ARN update + Semantic + Security + Identification updates	Francois Carrez, PayamBarnaghi, GianmarcoBaldini, John Soldatos (resp.)
V0.4	21stOct, 2014	Abstract+ update	Haihua Li, Yang Liu
V0.5	23rd Oct, 2014	Review, Addings in section 2 and abstract, xref, acronyms	Francois Carrez
V0.6	24th Oct, 2014	Update of China's view in section 2.1	Haihua Li, Xiaohui Li, DechengZhua, Jie Shen
V0.7	26th Oct, 2014	Editorial revision	Haihua Li
V1.0	28th Oct, 2014	Chapter 2.2 Positioning with Open Source SW and DevOps	PasiHyttinen

Table of Content

1. Context of this Position Paper

The IoT architecture is being kept as the focus of global researches and attentions, for it is quite significant to promote the IoT development healthy in scale. In the worldwide there are numbers of corresponding research projects and lots of corresponding achievements we can find out.

The most noticeable work on Architectures in Europe for the IoT has been achieved by the IoT-A project, which was a 3-years project ending up late 2013. One of the main results of IoT-A was the IoT Architectural Reference Model. Many other projects from various FP7 calls have been also working on Architecture but always focussing on their own topic, while IoT-A took a holistic approach to Reference Architecture for IoT with no specific thematic in mind like Smart -City, -Agriculture, -Grid or –Heath. The result is a whole approach to architecting IoT system that can apply to any sub-field of the Internet of Thing. Section 2.1 below gives more detail about the IoT ARM work. It is worth noting that most of IoT projects from the latest FP7 call had to reuse and align as much as possible to the IoT ARM. This ended up in a very good collaboration between all IoT projects materialised in the IERC Activity Chain #1 “Architecture” work and meet-ups. Through this AC1, IoT-A received lot of constructive comments, which resulted in many improvements of the ARM.

In China, the industries, research institutions, universities, etc., carry out studies on the IoT architectures actively, such as CATR, CETC,WSN. China set up some Projects on IoT architecture research also, such as in Mega Projects III (New generation broadband wireless mobile communication network), two research items initiated separately in 2009 and 2011, that is, research item “architecture research and the overall design of UN(Ubiquitous networking) (2009ZX03004-001)” and research item “generic architecture and key technique research of IoT (2011ZX03005-005)”, lots of achievement reached on the general IoT architecture. Meanwhile, IoT architecture research on some specific application areas carry out also, such as the research on M2M, WoT, Connected Vehicle, healthcare. The general IoT architecture provides important reference for the IoT architecturedevelopment of specific application areas.

With the development of the Internet of things faster and faster, the design of the concrete system architecture has been initiated in many specific IoT areas and the deployment of IoT systems are rolling out gradually. While considering this situation, EU-China reaches some consensuses based on the previous researches on IoT architecture of both sides and points out in this paper, hope they can guide and help architects in taking the right design decisions that eventually lead to these properties to be reached.

2. Common statements

2.1. IoT ARM provides methodology for deriving IoT architectures

Because IoT can potentially encompass lots of application domains-- the smart home, the smart city, the smart grid, the functions, service model, etc. are different for different application domain. How to define the general IoT Architectural Reference Modelis a big challenge, new concepts and methods are emerging endlessly. Both side of EU-China have stated respectively some research result on this.

The IoT Architectural Reference Model (ARM)[2]is one of the major results of the IoT-A[4], the European 3-years flagship project on Architecture Framework for the IoT; it is also the outcome of an intensive collaboration work between a few tens of experts coming from leading European academia and industries. The IoT ARM is not an "Architecture" *per se* but actually aims at being used for deriving concrete IoT architectures. In other words, IoT ARM is not focused on defining "THE" architecture for the IoT, but on the contrary, on providing a number of means (models, views, perspectives, best practices, etc.) that can be used to derive a concrete IoT architecture. This sole characteristic makes it already very different to other existing initiatives.

The IoT ARMconsists of three interconnected parts:

- *The IoT Reference Model (RM):*The RM provides a set of models that are used to define certain aspects of the architectural views. One of the most important models is IoT Domain Model (DM). It defines taxonomy of IoT concepts (e.g. Physical, Virtual and Augmented Entities, Devices, Resources and Services) and a set of relationships between those concepts. It defines the IoT domain in general, a customization of this generic model w.r.t. a specific IoT application allows to generate a common understanding of that domain (like identifying the entities of interest for that application, identifying the resources, e.g. sensors, actuators etc.). The RM also provides: 1) an Information Model (IM) which is a meta-model used to describe information as handled within the system, 2) a Communication Model, 3) a Functional Model (FM) used as the foundation of the Functional View and finally 4) models for Security, Trust and Privacy.

- *The IoT Reference Architecture (RA):*Based on models part of the RM, the RA takes from the best practices in software engineering as introduced by Rozanski& Woods[3] and adapts them to the IoT field. The RA consists of a set of Views (used to represent certain structural aspects of the system) and Perspectives (that focus on quality of the system that spans different views, e.g. Security, Resilience).
  Part of the Views is the Functional View. It proposes a layered model of Functional Groups which maps to most of the concepts introduced in the DM,together with a set of essential Functional Components (and associated interfaces) that an IoT system should provide. It is worth mentioning that the FV is not exhaustively developed. The Information View, based on the IM, complements the FV and provides a more detailed view about how information is to be handled in the system (including details about the components where the information is handled) and how it flows within the system. The perspectives are mainly derived from non-functional requirements and consist of activities and related tactics. Few other views focus on other aspects of the targeted architecture: Deployment and Operation View, Physical-Entity View and Context View for instance. Worth noting that the two later ones are not covered by the RA because they are heavily application dependant. However their purposes are explained in detail in the Guidance section;

- *A set of Guidance (also called best practice):* The Guidance defines the process that based on the RA and RM will lead to the generation of the concrete IoT architectures. In particular it defines the

[2]In this document IoT ARM is understood as the Architectural Reference Model as released by the IoT-A project, or as the general name for the IoT Architectural Reference Model. The specific meaning depends on the context.

[3]See http://www.viewpoints-and-perspectives.info/home/viewpoints/context/

requirement process, introduces additional views (i.e. Physical View and Context View) that are not part of the ARM as they are extremely application dependent and explaining general how and in which order the set of architectural views (which constitute a concrete architecture according to Rozanski& Woods) should be generated. It also gives a large (but not exhaustive) list of design choices that can be used as recommendations to achieve certain system qualities.

In addition to IoT-A, there are some other viewpoints on the IoT ARM which can provide reference and guidance to the concrete IoT architecture design as well. Such as the Six-Domain IoT conceptual reference model (ISO/IEC 30141) proposed by WSN, user domain, object domain, sensing & actuating domain, service providing domain, resources interchange domain, operation and management domain are defined, and three different views of IoT reference architecture are developed, (1) a generalized IoT Systems Reference Architecture (IoT-SRA); (2) Communications Technology Reference Architecture (IoT-CRA); and (3) IoT Information Technology Reference Architecture (IoT-IRA). ISO/IEC 30141 shares some very similar ideas with IoT-A, such as the definition of physical entity and virtual entity, different descriptions about IoT from different views, but may be different ideas about the definition of concrete domain in IoT.Operation and business models are quite important points for IoT architecture development. Considering of this, CETC presented a new concept named "IoT port", which works as an IoT device pool, and provides the basic functions of register, access, management, and service encapsulation for the devices. Sevenaspect views should be considered for the architecture design from CATR's point of view, they are networking view, functional view, communication interaction view, serviceinvocation view, data view, identification and addressing view, and security view.

- Networking viewdescribes the network deployment model, and domain concepts are usually introduced based on the business model analysis.
- Functional view describes functional entities, functions of each functional entity, and the interaction procedure.
- Communication interaction view describe the information exchanged, for IoT, primitive can be defined and used to describe the information exchanges. To realized these, the mapping from primitive to protocols are required.
- Serviceinvocation view describes the mechanism for the services invoking hosted by different networking components, such as Client/Server model, REST style model.
- Data view describes the data attributes, and data processing rules. At present, semantic related technology is being introduced into IoT.
- Identification and addressing view describes the object identifier, communication identifier, application identifier with the naming, addressing, discovery mechanism.
- Security view describes the security mechanism to provide network security, information security, and privacy protection. Security has influences on the other six view, should be considered and designed while develop other six views.

2.2. Horizontalcapabilities is the basis for building "internet of things"

Due to the huge differences of IoT devices, data collected, applications, IoT architecture design should pay special attention to the horizontal application, even for some specific application system, in order to offer IoT architects a common technical grounding in order to optimize the chances of reaching interoperability. While the objective of EU-China co-research on the IoT architecture focus more on the general common capabilities which are independent of specific application domains, in order to promote the "Internet of things"not "intra-net of things" build.In that case, IoT applications would not be any longer built as stand-alone silo applications, but as inter-operable vertical applications still having a common "horizontal" grounding, such as the compliant components, protocol suites, etc.

In order to maximize the chance of reaching desired properties like interoperability and security, we reckon that lots of researches needs to be done, for instance, the IoT Forum Working Group on "Architecture and Interoperability"are considering to definition of IoT ARM profiles, each profile will focus on a specific system quality –say interoperability- and will define precisely a set of needed Components (and API) that are needed to reach the desired quality, and it will also take all related technology and design

choices.Application capabilities in difference IoT network components as well as the interaction between these application capabilities are important aspects from IoT functional view. The general strategy here is to reduce the degree of freedom of architects, to guide and help architects in taking the right design decisions that eventually lead to those properties to be reached in concrete system development case.
Despite the right design decisions taken, it is the run-time executables that, during their interoperation, both make and are Internet of Things. When the number of run-time executables increase also probability of systemic side effects rise. Now when having such system, we can ask what are the structures and parts of the system that originated (at least partially) from the IoT architecture model? What arethe structures that cause emergent positive and negative effects and should they be part of IoT architecture model and even reference model? Is interoperability, security level or other cross-cutting aspect achieved? Why it was achievedor why not?
Systemic effects are complex, unique to particular system and therefore cannot be studied without such system.
IoT architecture referencemodel cannot be influenced by all subsystems that constitutethe Internet. This is because there are too many of those and some of those are proprietary and therefore out of reach. However, there is set of systems that are within reach and gaining popularity and these are Open Source Software (OSS) systems. By selecting reasonable small set of the most popular, relevant and stable OSS implementations we can establish a set of reference systems for IoT that cover most of the Internet technologies for IoT architectures. The run-time properties of the reference systems can be used for improving reference model and architecture.
A third researchtheme could be related to deployment of IoT architecture elements and applications.Model driven approach together with set of reference systems could be first used for generating concrete reference IoT platforms and applications as IoT-A RM proposed. These model driven products could be starting points of agileDevOps[9]SW processes that customize and continuously improve products and launch them intotheir run-time environments. The basic questions here are how latest DevOps tools and methods are harnessed for IoT production, and, is there need for new tools and methods.

2.3. Identification resolution system and identification-centric addressing are developingsimultaneously

Tag-based identification applications get a rapid development in recent years. Barcode and RFID technology has been widely used in supply chain management, logistics management, asset tracking, public safety management, vehicle management, etc.The core technologies associated with the identification mainly include ID naming, addressing and discovering. In particular, the resolution system for addressing and discovering is an important component for IoT architecture.

A variety of identification technologies are used in EU and China, including IPv6, RFID identifiers, Digital Object Identifiers (DOI) and more. These identification technologies are usually associated with naming and addressing technologies (such as DNS for Internet-addresses and ONS for RFID), which are also deployed in the scope of practical applications in both China and EU. As part of the identification technologies, several schemes for the efficient discovery of IoT resources are deployed. A review of naming, addressing and discovery technologies for IoT, with emphasis on their deployment in EU and China is provided at [2]. In addition to the practical deployment of these technologies both China and EUhas launched a lot of research initiatives on IoT ID related technologies. For example, based on a National Founding project from NDRC, China Academy of Telecommunication Research (CATR), ETIRI, China Internet Network Information Center (CNNIC) and GS1 China developed a public IoT ID Service Platform together.In EU, many FP7 R&D projects of the IERC clusterhave produced a wide range of identification solutions, including solutions that can discover IoT resources stemming from diverse IoT system and using different identification schemes. Relevant projects includeiCore, OpenIoT, IoT@Work and more. Despite these research efforts there is still a number of important research challenges, including: (A) The need to ensure the semantic interoperability across IoT applications that leverage different identifiers; (B) The need to provide scalable deployment and address performance constraints; (C) Security challenges associated with the authorized, authenticated and encrypted access to IoT naming and discovery services, but also with the avoidance of cache poisoning and

denial of service; (D) The need to take into account objects' mobility during the discovery of IoT resources. Several of these challenges require the homogenization of the representation of IoT resources, as well as the semantic unification of diverse IoT systems and services.

In-line with the need for the above-mentioned unification, the FP7 IoT-A project introduced the new concept of "ID layer" was first proposed in the IoT-A project as the centre of the firstconvergence point in the communication stack. Leveraging on uniforminterfaces provided by the network layer, the ID Layer allows for a common resolutionframework for the IoT. Also, security, authentication, and high-end services will exploit this layerfor providing uniform addressing to the many different devices and technologies in IoTnetworks. Similar ideas also appeared in China during thestudy of the future network architecture, emphasizing the importance of Data ID addressing in the network layer aspect.Such an ID Layer could provide virtualized IoT-system and identification technology agnostic functionalities for IoT addressing and discovery of IoT resources. In this context, the design of this layer could also cope with several of the above-listed IoT identification challenges (such as the security and interoperability challenges). Some IERC project has also provided proof-of-concept implementations of selected functionalities of the IoT-A ID Layer, as part of their efforts to adopt, implement and comply with the ARM. Most of these implementations have focused on the specification and implementation of semantic gluing layer across diverse identification systems, thereby enabling the identification and use of objects that are originally represented on the basis of different identifiers. As ARM can be used to derive IoT architecture, we expect different specifications and implementations of the ID Layer to emerge as part of practical applications. Note also that the ID Layer of the ARM is also in-line with on-going standardization efforts (such as OneM2M), which emphasize the unification of the structure of various object as a means of expressing and using their identity in a common standards-based way.

Overall, the identification of IoT resources is closely related to several other topics addressed in the present paper, such as the implementation of semantic interoperability solutions for sharing resourcesacross different IoT deployments and the ever important security and privacy functionalities.

2.4. Semantic plays key role for resource sharing and intelligent processing

As the essential technology help in automated processing and sharing for IoT resource, semantic technologieshave received asignificant attention.Semantics can be applied to describe sensors, RFID readers, collected data, network capabilities,and the semantic annotationsimprove the way thatthe IoT resourcescan found and used.

From IoT architecture perspective, semanticannotations influence several components, for instance, the sensor node should send out collected data along with the semantic descriptions, the data processing components cananalyseand combine heterogeneous data using semantic annotations and applications can find suitable IoT data or devices and use them (if permitted) by querying the semantic data and finding and discovering relevant resources according to different criteria.The semantic annotations and interoperability between various sources using common metadata will encourage the creation of an open market for the IoT data and device sharing and use.

Both EU-China realize the importance of semantic technologies for the IoT, and are making efforts to improve the semantic technology and linked-data research. In recent years there have been several research efforts that have received contributions from the EU projects. This includes W3C SSN Ontology [3], the IoT-A information model that included IoT resources, services and entity descriptions based on semantic models [5], IoT.est service description model [6] and linked-data models for describing the IoT data and external resources among several other research works [7] and domain specific semantic models for applications such as Smart Cities (e.g. CityPulse linked-data model [8]), China has initiated the research item in Mega Project IIIand the IoT semanticspecificationsarebeing developed.

But semantictechnologies could becomplex and resource consuming for the constrained environments in the IoT; common semantic mechanism should be designed as well as the domain specific semantic. Most of the current work on the semantic technologies has focused on defining the schema models and ontologies

to describe the IoT resources, services and real world entities. While the later are very important, the research community needs to define a set of common attributes and concepts that are defined and describes using common schema models (e.g. id, time, location, type). This common model can promote interoperability between various platforms and providers. Obviously additional attributes to describe more detailed features such as quality, operational and network attributes can be included in the model as pluggable modules. Another important aspect of using semantic technologies is providing tools and mechanisms to generate, publish, test, query and use the semantically annotated data. Providing efficient tools and APIs that can ease publishing and using the sematic data will allow wider adaption and use of the underlying models. Using linked-data approach to include external descriptions and common ontologies and knowledge-bases is also an effective approach to interlink different resources and to take advantage of large datasets that are available on the Web.

Semantic annotations are intermediary and internal descriptions. Their goal is to ease access to data and to provide interoperability across different providers and various platforms; however they should be simple enough to be easily used, optimised to be suitable for resource constrained environments and/or very large-scale data annotation. They should support stream annotations, as well as devices, entity and service descriptions and there should be tools and mechanisms available to publish, store, index, query and access these semantic and process them in order to extract actionable-information from large data sources, or to be able to find relevant devices and services in a distributed IoT framework. However the complexity of the semantic annotations should be transparent and kept away from the end-users and consumers of the data and services.

2.5. Security and privacy protection require special attentions for IoT architecture

The interplay between IoT and privacy, data protection and security is a long-debated subject. IoT connected objects can generate an enormous amount of data, some of which actually constitute personal data. Issues related to the adequate level of security of IoT devices, ensuring transparency and users' choice in an environment where sometimes there is no user interface, safeguarding the privacy of individuals are relevant for discussion. Recent trends in Big Data can also influence how individual's data is used by business entities.

The European Commission's proposal for the new Data Protection Regulation, currently being discussed in the European Parliament and the European Council, will apply to IoT applications whenever there will be an impact on data subject privacy and personal data will be processed. The EC's proposal reinforces in various ways the obligations of the data controllers by imposing accountability, privacy by design, privacy impact assessment, and security breach notification. At the same time, the proposal strengthens data subjects' rights, especially with regard to consent, information, access and deletion rights. All these novelties will have to be appropriately addressed in order to guarantee a sustainable evolution and a successful deployment of IoT in Europe.Some main areas of work and the related challenges, which are investigated by the research and industry community in Europe, are security of *cyber-physical system, Device authentication, Support for Scalability, IoT and Critical Infrastructures, Physical availability of devices*. Various projects financed by the European Commission through the Framework Program 7 and Horizon 2020 are researching solutions to mitigate the challenges identified above. Some examples of the thematic areas are described below:

- **Usage control policies.** Usage control policies consist of authorizations and obligations specified as Event-Condition-Action (ECA) enforcement rules. These rules use as a reference a set of inter-related design models representing different aspects of the IoT system, and are used as input for the runtime components in the framework. The framework defined in the FP7 project iCore defines policies consisting of a collection of metamodels for specification of a computer system structure, information, behaviour, context, identities, organizational roles, and security rules. These metamodels provide the foundation for security engineering tooling add-ons and metamodel extensions to address requirements of governance, security and privacy. The framework adopts a

generic design language to represent the architecture of a distributed system across application domains and levels of abstraction including refinement relations support inspired in the Interaction System Design Language (ISDL).

- **Secure Setup and Configuration**. Existing operational credential bootstrapping and key management protocols require the existence of some initial credentials as a starting point. Also key pre-distribution protocols, e.g. applied in wireless sensor networks, assume the configuration of some initial credential information before operation. The FP7 project called RERUM will take approaches to initially bootstrap credentials on the IoT objects, and how to use them to update operational keys, and analyze their applicability on the desired Smart City applications. To avoid any incidents during network bootstrapping, RERUM will take into account existing bootstrapping protocols (such as EAP, PANA, 802.1x, CoAP, and 6LoWPAN) and will define mechanisms to optimize the process, enhance the security to minimize attacks for the desired Smart City applications.
- **Trust and Reputation systems**. The FP7 project called COMPOSE has designed a framework, which manages reputation of virtual objects represented by service objects, services, applications, and users. Through the monitoring of various reputation dimensions such as popularity, user feedback, service compliance to its promised behavior, its quality of service, or its security properties (such as defined by policies or contracts) appropriate reputation values are accumulated. This accumulated reputation is used in a trust metric to compute trust values for the respective COMPOSE entities. Access control modules and enforcement monitors in the respective security architecture use these trust values to grant resource access or prevent the execution of particular processing steps.

Technology and solution research onthe IoT security and privacy protection are one of the objectives in many projects in China. Benchmark and evaluation methods for IoT system are especially emphasized and promoted. In 2012, NDRC financed the test service on the IoT security, it includes perception equipment security test service, system level security test and risk evaluation service, information securityvulnerabilities and patch advisory services, integrated security managementServices.In order to guidance the device R&D and system reliable operation, the requirements on the IoT information system security level protection, the IoT terminal operating system security, the perception layer protocol security of IoT, etc. are being analyzed and clarified.

The approaches/solutions for security and privacy protection may be used stand-alone or in combination with existing technologies (e.g., biometrics, ToR, OAuth 2.0) to provide a comprehensive framework. Beyond the purely research and technological work, we are also addressed the following aspects to support a reliable and secure IoT:

1. Even if we are successful in identifying successful security and privacy solutions in IoT, we must also highlight that without policy or standardization support, any research solution risks being non-effective and the research work wasted.

2. IoT is going to be pervasive in many different domains with different operational and technical requirements and various contexts. The deployment of technical solutions to ensure anonymization or access control can be quite different in each specific context. Research activities should also focus on the deployment and organizational aspects.

3. It is widely acknowledged that in order to make inroads into establishing influence and effective controls over IoT's overall direction some form of global governance is needed as soon as practically possible. Without IoT governance the adoption of an IoT supporting the IERC definition will be challenging due to the breadth of legacy application solutions, technologies and stakeholder interests. There is a very real potential for IoT fragmentation if adequate time and efforts are not invested in the process of establishing IoT governance without taking great care and paying sufficient respect to major influencing sectors. To gain a unified cross platform and application domain IoT will require governance. The earlier a start can be made the more chance IoT has of being built upon broad accessibility.

3. Further actions

3.1. Further study and cooperation on IoT architecture

The objective of the IoT Forum Working Group on “Architecture and Interoperability” is –beyond sustaining the ARM- to define and specify specific “ARM-profile” dedicated to essential properties like semantic interoperability and security. In the context of the EU-China initiative it is very important that Chinese partners (like CATR which has signed a MOU with the forum few years back) eventually join the Forum and get actively involved in the profile definition. Beyond profile definition it is also very important to specify in the deep details horizontal components (e.g. Identification related functions).IoT Forum Working Group is a good cooperation platform; EU-China will keep collaboration and promote the IoT architecture research.
The IoT architecture is one of the importance discussion topics for the EU-China advisory Group on Internet of Thing (IoT), the EU-China advisory Group will carry on the relevant researchandinformation exchange. Currentlythis paper shows the core common understanding and agreements of EU-China on the IoT architecture, in the future, the IoT architecture white paper will be considered, and this paper will form base of the white paper.

3.2. Interoperability activities

Based on the test environment between EU-China, further interoperability test are under consideration, such as, semantic Interoperability test on some specific application areas.

4. References

[1] http://en.wikipedia.org/wiki/Identifier

[2] John Soldatos and Ge Yuming (eds.) «EU-China Joint White Paper on Internet-of-Thing Identification», position paper by The European Research Cluster on the Internetof-Things (IERC) and the China Academy of Telecommunication Research (CATR), October 2014.

[3] Compton, M., et al. (2012), "The SSN Ontology of the W3C Semantic Sensor Network Incubator Group", Journalof Web Semantics.

[4] F. Carrez, *ed.* IoT-A Deliverable D1.5 "Final Architecture Reference Model for the IoT V3" Downloadable at https://dl.dropboxusercontent.com/u/23123988/D1.5%20%2020130715%20VERYFINAL.pdf

[5] De, S., et al. (2012), "An Internet of Things Platform for Real-World and Digital Objects", Journal of ScalableComputing: Practice and Experience, vol. 13, no.1, 2012.

[6] W Wang et al, Knowledge representation in the internet of things: semantic modelling and its applications, Automatika–Journal for Control, Measurement, Electronics, Computing and Communications, volume 54, issue 4, 2013

[7] Barnaghi, P., Mirko Presser, M. &Moessner, K., (2010), "Publishing Linked Sensor Data", In Proceedings of the 3rd International Workshop on Semantic Sensor Networks (SSN), November 2010.

[8] S. Kolozali, D. Puschmann, A. Karapantelakis, H. Liang, D. Kümper, T. Iggena, M. I. Ali, F. Gao, Deliverable D.3.1: "Semantic Data Stream Annotation for Automated Processing", September 2014.

[9] http://en.wikipedia.org/wiki/DevOps

Appendix A: Acronyms

Acronym	Defined as
6LoWPAN	IPv6 over Low-power wireless Personal Area Networks
API	Application Programming Interface
ARM	Architectural Reference Model
CATR	China Academy of Telecommunication Research of MIIT
CETC	China Electronics Technology Group Corporation
CNNIC	China Internet Network Information Center
CoAP	Constrained Application Protocol
COMPOSE	Collaborative Open Market to Place Objects at your Service
DM	Domain Model (IoT ARM)
DNS	Domain Name System
DOI	Digital Object Identifiers
EAP	Extensible Authentication Protocol
EC	European Commission
ECA	Event-Condition-Action
ETIRI	Electronic Technology Information Research Institute
EU	European Union
FV	IoT Functional View (IoT ARM)
FP7	the EU's Seventh Framework Programme for Research
iCore	Internet Connected Objects for Reconfigurable Ecosystems (FP7 project)
IERC	European Research Cluster on the Internet of Things
IM	Information Model (IoT ARM)
IoT	Internet-of-Things
IoT-A	Internet of Thing – Architecture (FP7 project)
ISDL	Interaction System Design Language
M2M	Machine to Machine
ONS	Object Naming Service
PANA	Protocol for carrying Authentication for Network Access
RFID	Radio Frequency Identification
SSN	Semantic Sensor Networks
ToR	The Onion Router (anonymity enabling software)
W3C	World Wide Web Consortium
WoT	Web-of-Things
WSN	Wuxi SensingNet Industrialization Research Institute