An Evolutionary Way to Standardize the Internet of Things

Subin Shen[1] and Marco Carugi[2]

[1]*School of Computer, Nanjing University of Posts and Telecommunications, Nanjing, China*
[2]*Study Group 13, International Telecommunication Union, Telecommunication Standardization Section, Geneva, Switzerland*
sbshen@njupt.edu.cn, marco.carugi@gmail.com

Received: October 17, 2014;
Accepted: November 10, 2014

Abstract

The current situation of technology separation among the different application domains of the Internet of Things (IoT) results in a market separation per application domain. This issue hinders the technical innovation and investments in the IoT business. In order to solve the issue, it is necessary to standardize common technologies of the IoT across the different application domains. This paper argues that a key direction of the future standardization of the IoT, in addition to standardizing specific technologies, is building over a standardized new architecture reference model for the IoT. Based on the analysis of existing key activities concerning the standardization of OSI, NGN and IoT from a functional architecture perspective, it suggests that the IoT standardization work be progressed in an evolutionary way in order to enable the integration of existing technologies, and focus on the interactions among functional entities or deployable components of the IoT to impose minimum constraints on future technical innovations. Topics discussed in the paper include characteristic capabilities of the IoT, ways of integrating the cloud computing technologies in the IoT perspective, and challenges faced by the IoT standardization work.

Journal of ICT, Vol. 2, 87–108.
doi: 10.13052/jicts2245-800X.222

Keywords: architecture reference model, functional entity, interaction, Internet of Things, Next Generation Network, Open System Interconnection, standardization.

1 Background

The International Telecommunication Union (ITU) had identified in its Internet Reports 2005 on the Internet of Things (IoT) that "a new dimension has been added to the world of information and communication technologies (ICTs): from *anytime*, *anyplace* connectivity for *anyone*," to "connectivity for *anything*" [1]. The evolution from anytime and anyplace to anything connectivity is a development goal of ICTs in the near future.

Now, there seems to be a long way to reach this goal. Even though the IoT technologies have been applied in various application domains, the IoT has not been developed in the view of a global information infrastructure. There is no standardized IoT architecture for global support of the different application domains. From the industrial point of view, the technologies of the IoT are segmented by the different application domains, so that the market of the IoT is also divided by the different application domains. This situation hinders the investment and development of IoT technologies and applications. In this sense, significant advances of the IoT standardization are essential and urgent for the development of IoT technologies and applications.

It has to be admitted that the IoT is indeed a very complex subject of the information and communication technologies. And the standardization of the IoT is then a very complex work too. There are different perspectives and opinions about the IoT standardization work: some focus on the specific technologies of the IoT in order to make the IoT of practical value, such as the work on machine-to-machine communications (M2M) done by the European Telecommunications Standards Institute (ETSI, www.etsi.org); others focus on a standardization process starting with the IoT requirements and capabilities and moving then to the IoT architecture, such as the work on IoT architecture reference model done by the IoT-A (Internet of Things – Architecture) project (www.iot-a.eu) co-funded by the European Commission within the Seventh Framework Programme (2007–2013).

In our opinion, in addition to the standardization of the specific technologies of the IoT, it is necessary to standardize a new architecture reference model (ARM) for the IoT, as the existing reference models are not suitable for the IoT. This paper assumes that the Open System Interconnection (OSI) basic reference model (BRM) [2], the Next Generation Network (NGN) BRM [3]

and the NGN functional architecture [4] are the key existing reference models over which the new ARM for the IoT can be developed.

The standardized IoT ARM should enable the integration of existing technologies and support the unique requirements of the IoT applications.

In order to enable the integration of existing technologies, it is suggested that the standardized IoT ARM builds over the OSI BRM, the NGN BRM and the NGN functional architecture, and the standardization work focuses on the interactions among the IoT functional entities or deployable components in order to impose minimum constraints on future technical innovations.

In order to support the unique requirements of the IoT applications, the characteristic requirements and corresponding characteristics capabilities of the IoT should be analyzed at first. Then, the ARM of the IoT can be standardized building on existing reference models and the characteristic capabilities of the IoT.

The contents of this paper are arranged as follows.

- In Section 2, the evolution of the standardization requirements in an architecture perspective is presented based on the analysis of the interactions in the OSI BRM, NGN BRM and NGN functional architecture, and the interactions which are required to be standardized in the IoT are then described.
- In Section 3, some characteristic capabilities of the IoT are introduced.
- Section 4 presents the evolution of the ARM based on the analysis of the frameworks of OSI BRM, NGN BRM, and NGN functional architecture, and a proposed framework of the IoT ARM for IoT standardization is then discussed.
- In Section 5, ways of integrating the cloud computing technologies in the IoT perspective are discussed.
- Section 6 discusses some existing activities (outside the ITU-T) related to the standardization of the IoT.
- In Section 7, challenges faced by the IoT standardization work are analyzed.
- In Section 8, some suggestions for the future standardization of the IoT are given.
- The conclusion of this paper is given in Section 9.

2 The Evolution of the Standardization Requirements

The analysis of the requirements for the standardization of the architecture reference model is the first step in the standardization activity. The

standardization requirements had evolved from those of the OSI BRM to those of the NGN BRM from the perspective of the interactions.

The OSI BRM aims to "*qualify standards for the exchange of information among systems*" [2]. The exchange of information can be termed as interactions, and the systems can be regarded as the computing systems. So the OSI BRM is required to guide the standardization of the interactions among computing systems. The interactions in the OSI BRM are illustrated in Figure 1, where the standardized interactions are represented by solid arrows and other interactions are represented by dashed arrows. The application process is "*an element within a real open system which performs the information processing for a particular application"*.

The OSI BRM is a logical reference model that does not consider the implementation and deployment aspects (i.e. specific service access points for each functional layer, the functional components in each functional layer, etc.), so it is not suitable to guide directly the standardization of the technologies for implementation and deployment.

The NGN BRM takes into account the requirements concerning the adoption of existing transport and service technologies and the separation between service system (service functions) and transport system (transport functions). So, as illustrated in Figure 2, the NGN functional architecture is required to standardize the interactions among multiple service systems, among multiple transport systems and between service system and transport system of the same NGN. It should be noted that, in Figure 2, an application is "*a structured set of capabilities, which provide value-added functionality supported by one or more services"* [5].

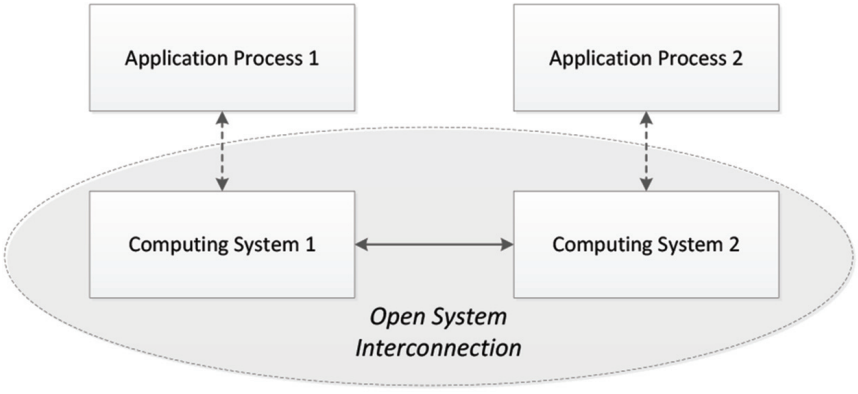

Figure 1 Interactions in the OSI BRM

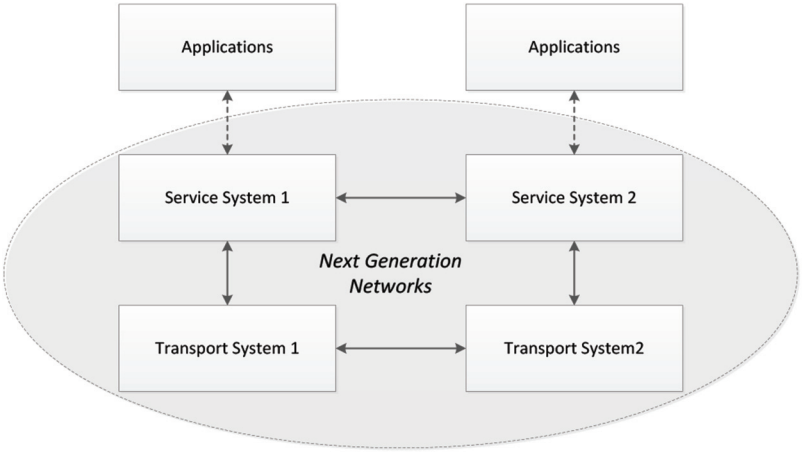

Figure 2 Interactions in the NGN BRM

The separation of service system from transport system results in independent service provisioning in NGN, so that a competitive environment is promoted in order to speed up the provisioning of diversified NGN services [4]. In this sense, the standardization requirements have evolved from the information exchange in OSI BRM to the service provisioning in NGN BRM.

Concerning the IoT, the interactions are extended to the interactions between computing system and IoT devices; in these interactions the exchanged information is constrained to the information collected by the devices and the information controlling the devices. Here the IoT devices refer to the devices connected to the IoT. As the messages exchanged between computing system and IoT devices are no longer transparent in terms of information meaning, it is required to identify and process the meaning of the information exchanged from the application perspective. These content-aware interactions between computing system and IoT devices can be classified into local interactions and remote interactions.

The local interactions are illustrated in Figure 3. This type of interactions may be initiated by the local computing system or the local related applications. As far as the technologies related with this type of interactions, existing technologies can be used, such as those developed for wireless sensor networks. This is the basic interaction type to be standardized in the IoT.

The remote interactions are illustrated in Figure 4. This type of interaction is decomposed into the local interactions between IoT devices and local

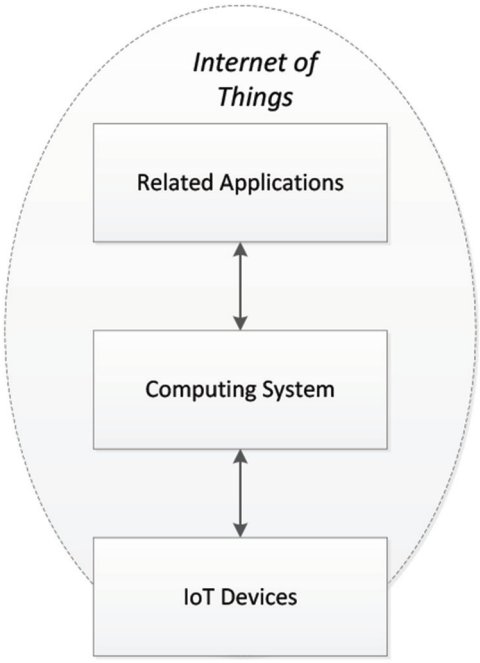

Figure 3 Local interactions in the IoT

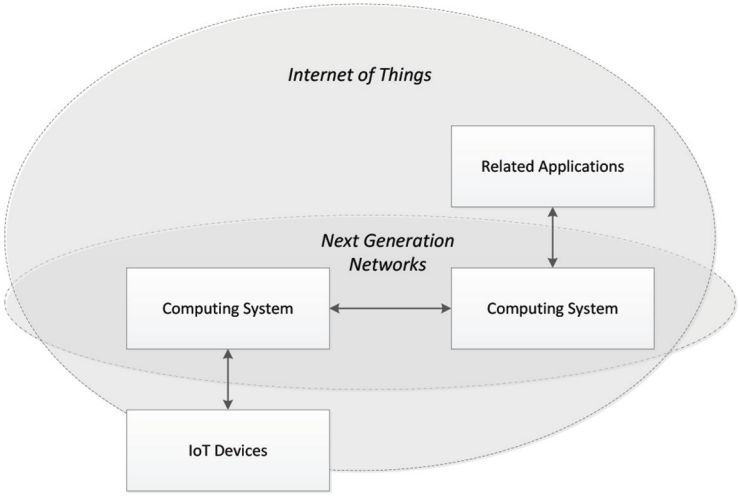

Figure 4 Remote interactions in the IoT

computing system, and the interactions between local computing system and remote computing system as described in the NGN specifications and their necessary extensions to be specified in IoT related standards. NOTE - It is assumed here that the IoT is implemented building over the NGN.

This type of interactions is a complex part of the IoT standardization, requireing to integrate IoT technical standards and NGN technical standards.

Based on the above analysis, a global view of the interactions in the IoT is proposed as illustrated in Figure 5, where the computing system is decomposed into transport system and service system as defined in the NGN specifications. The standardization of the different interactions shown in the figure (between IoT devices and transport system, between transport system and service system, between service system and related applications, among different transport systems and among different service systems) is required.

Although the IoT devices in Figure 5 are illustrated as directly connected to the transport system, the IoT devices need to interact with the service system and even related applications based on the requirements of IoT applications. An IoT device can be also regarded as a specific computing system that is required to automatically interact with the transport system, the service system and related applications, possibly resulting in automatic service provisioning.

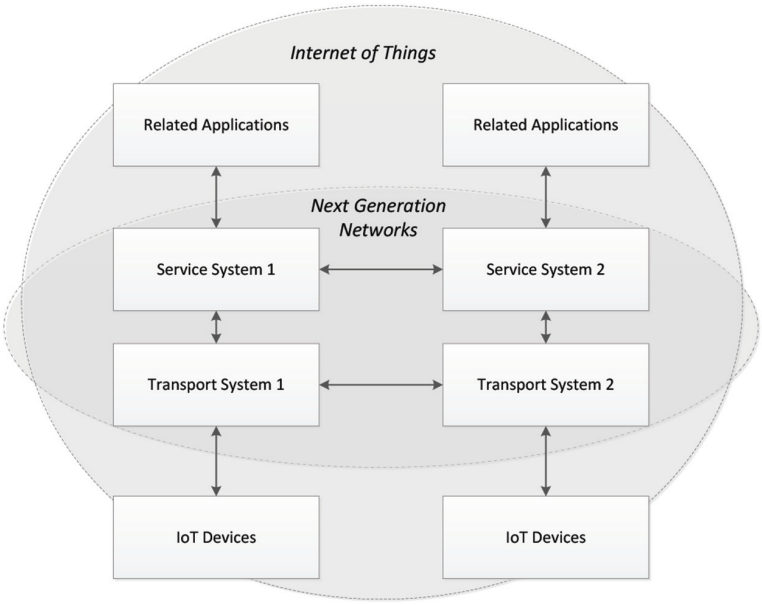

Figure 5 A global view of the interactions in the IoT

Also, the IoT devices exchange data with the related applications, and these interactions belong to a content-aware type of information exchange.

In IoT, the standardization requirements have then evolved from a content-transparent information exchange as assumed in the OSI BRM, and the traditional service provisioning as assumed in the NGN BRM, to a content-aware information exchange and the automatic service provisioning as required by the IoT applications. In this sense, the IoT requires a new set of characteristic capabilities and a new standardized architecture reference model to fulfill its characteristic requirements.

3 Characteristic Capabilities of the IoT

According to the characteristic requirements of the IoT, the standardization work of the IoT involves a new set of characteristic capabilities.

Building on some characteristic requirements identified in ITU-T studies [10,11], significant examples of these characteristic capabilities of the IoT are, in our opinion, the capabilities for support of autonomic operations, location based operations and data operations.

The capabilities for support of autonomic operations include the capability for autonomic service provision and that one for autonomic networking. The first one involves the abilities of automatic capture, transfer and analysis of data of things, as well as the automatic provision of services based on predefined rules or policies. The second one involves the abilities of networking parameter self-configuration, self-healing connectivity with the IoT, networking performance self-optimization, and networking entity self-protection.

The capabilities for support of location based operations include the capability for location based and context aware services, and that one for location based communication. The first one involves the abilities of automatic provision of services based on location information and related context. The second one involves the abilities of location identification and communication initiation.

Among the capabilities for support of data operations, the capability for semantic based data operations, the capability for virtual storage and virtual processing, and the capability for data management security can be identified. The capability for semantic based data operations involves the abilities of semantic based annotation, query, storage, transfer, and aggregation of data of things in order to fulfill the requirements of IoT applications. The capability for virtual storage and virtual processing involves the abilities of providing storage and processing resources in a dynamic and scalable way. The capability for

data management security involves the abilities of providing secure, trusted and privacy protected data management.

4 The Evolution of the ARM

The ARM of the IoT can be seen as an evolution of existing reference models. In this paper we consider the OSI BRM, the NGN BRM and the NGN functional architecture as the key existing reference models.

The OSI BRM is independent from implementations and deployments, and was standardized from a logical perspective. The OSI basic reference model consists of four basic elements: "open systems" that are pertinent to OSI, "application-entities" that exist within the OSI environment, "associations" that connect the application-entities and permit them to exchange information, and "physical media for OSI" that provide the means for the transfer of information between open systems [2].

The NGN BRM was adopted in the NGN functional architecture [4]. The NGN functional architecture is defined as "*a set of functional entities and the reference points between them used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions*" [4]. Although the reference points are sufficient to guide the standardization of the local interactions between service system and transport system, it is our opinion that functional entities and reference points are not sufficient for satisfying the requirements of remote interactions, such as the remote service provisioning requirements. The reason of such limitation is that the architecture of a system consists of its functional entities and the interactions among them, and a reference point refers to "*a conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities*" [4]. Functional entities and reference points cannot cover all interactions among the various functional entities, such as the interactions among functional entities connected through networks (in fact, for these functional entities, the associations - in OSI BRM's terms - among these functional entities should be also considered besides the reference points).

Although each functional entity can be specified by its capabilities and its reference points with other functional entities, a functional architecture would require specification of the functional entities, the reference points and the associations among the reference points.

The NGN functional architecture specified in [4] has evolved from the OSI BRM by taking into account requirements and capabilities from the

implementation and deployment perspectives, with separation of the service functions from the transport functions. The OSI BRM is however still used in the modeling of the NGN as a supporting model of communication.

The NGN functional architecture includes NGN functional entities and NGN components [4]. The definition of functional entity in [4] is "*an entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.*" Although a definition of component (NGN component) is not given in [4], based on the content of clause 10 of [4] and the above definition of functional entity, the components can be regarded as the "groupings of functional entities which are used to describe practical, physical implementations." In this sense, "component" is a concept that is used in deployment models.

From the above analysis, it can be concluded that [4] contains both the specifications of functional model of NGN and deployment model of NGN. The functional model of NGN is specified from a logical point of view, and the deployment model of NGN is specified from a deployment point of view.

Figure 6 illustrates the framework of the "NGN ARM" consisting of OSI BRM as communication model, NGN functional model and NGN deployment model.

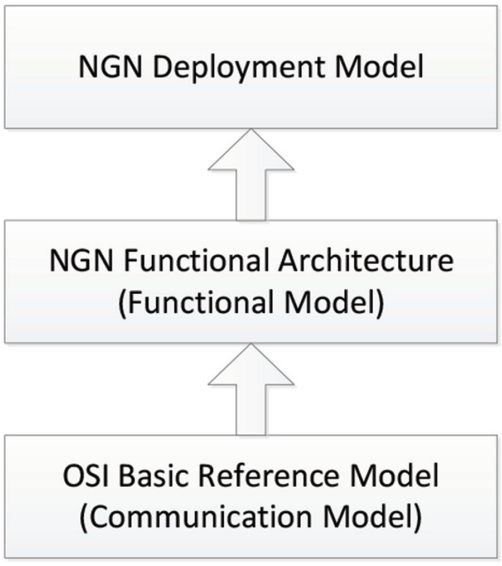

Figure 6 Framework of the NGN ARM

As the standardization requirements of the IoT include the standardization of content-aware interactions and automatic service provisioning, the only supporting model of communication is not sufficient for the ARM of the IoT. Three additional models are identified for the standardization of the ARM of the IoT: the information model, the security & privacy model, and the IoT concept and requirement model. A framework of the IoT ARM is proposed and is illustrated in Figure 7.

The technical scope of the IoT covers different aspects of ICTs, such as computing, control and communication technologies. In order to define correctly and reasonably the scope of the IoT standardization, the establishment of an IoT concept and requirement model is necessary to specify characteristics and high level requirements of the IoT from an ICT perspective.

Based on the requirements of IoT applications, the IoT is required to automatically capture and process (e.g., classify, aggregate, store, transfer and analyze) the data collected by the IoT devices, and possibly send instructions for their control according to pre-defined rules and occurrences of pre-defined events. The IoT depends on the understanding of the meaning of the captured or transferred data for correctly performing the required operations. In order to standardize the information exchange among IoT functional entities from the application perspective and support automatic operations in the IoT,

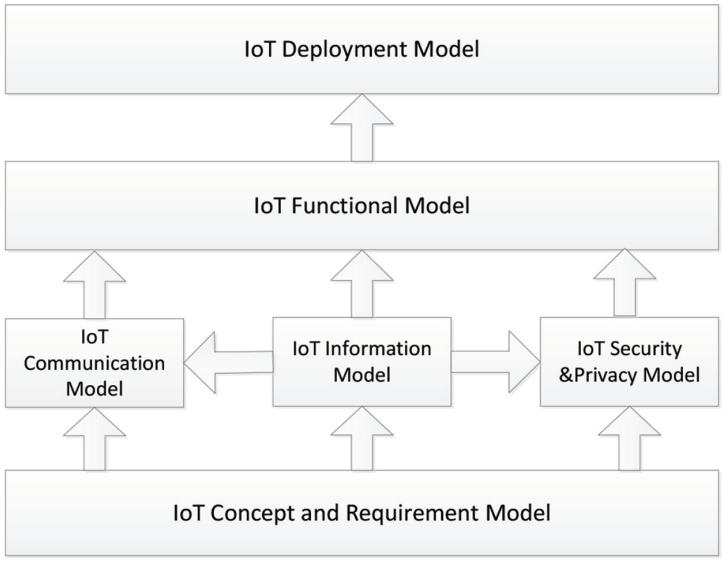

Figure 7 Proposed framework of the IoT ARM

it is necessary to establish an IoT information model specifying the IoT information entities and their relations based on the application requirements. An information model has been proposed by the IoT-A project. However, as the IoT information model involves some complex topics, such as the data models related with physical things and the semantics of physical things, more work is expected to be done in the future.

The security and privacy protection capabilities are no longer optional in the IoT. A security & privacy model is needed in order to specify the constraints of security and privacy protection distributed in the IoT information entities, and the operations to enforce and fulfill these constraints. "Concepts and solutions for privacy and security in the resolution infrastructure" of the IoT have been proposed by the IoT-A project, but these concepts and solutions are not linked to the IoT information model.

In our opinion, in order to integrate the different models of the IoT ARM, a "knowledge plane" such as that one proposed by David Clark in [6] may be needed in the IoT functional model. This means that the functional model should have the capabilities of capturing, storing, using and updating the knowledge in support of the operations required in the IoT. This knowledge could be represented in the IoT functional model according to formal descriptions contained in the information model.

In summary, the ARM has evolved from the logical model specified in the OSI BRM, and the logical and deployment oriented model specified in the NGN functional architecture, to the conceptual, logical and deployment oriented model required for the IoT. Because this paper focuses on the trend for standardizing the IoT and the standardization work concerning the IoT ARM is at an early stage, the paper does not go further into details of the IoT ARM.

5 Integration of Cloud Computing Technologies with the IoT

Based on the framework of the IoT ARM, ways of integrating other (IoT relevant) technologies in the IoT perspective can be described clearly. The integration of existing technologies with the IoT impacts in fact the content of one or more of the models identified for the standardization of the IoT ARM.

In this paper, we take the cloud computing technologies as an example of existing technologies that can be integrated with the IoT in order to support data operations and flexible service provisioning.

As mentioned earlier, the capability for virtual storage is required in the IoT to enable a dynamic and efficient usage by the IoT functional entities of all possible storage resources, within the IoT or connected to the IoT, for storage of the data of things. Similarly, the capability for virtual processing is required in the IoT to enable a dynamic and efficient usage by the IoT functional components of all possible processing resources, within the IoT or connected to the IoT, for processing the data of things.

These two capabilities of the IoT can be implemented based on cloud computing technologies. These capabilities can be also supported in the IoT service platform that can then integrate its services with cloud computing oriented services.

The capability for support of "Things as a Service" is an example of additional capabilities which can be provided in the IoT via the integration of cloud computing technologies with the IoT. This capability involves the abilities of publishing interfaces of virtual things as services, and linking virtual things with physical things in order to implement functionalities of sensing and actuating things by the invocation of corresponding services.

6 Some Existing Activities (Outside the ITU-T) Concerning the Standardization of the IoT

Several relevant efforts concerning the standardization of the IoT have been progressed and/or are in progress besides that one conducted within the Internet of Things Global Standard Initiative (IoT-GSI) administrated by the ITU-T (www.itu.int/en/ITU-T/gsi/iot). This paper simply concentrates on two of these efforts, the "Smart Machine-to-Machine communications (SmartM2M)" ETSI (www.etsi.org) Technical Committee (continuation of the previous "M2M" Technical Committee) and the IoT-A project (www.iot-a.eu).

ETSI has published technical specifications concerning the M2M functional architecture, respectively in 2011 and 2013.

The ETSI "M2M service capabilities functional architecture framework" published in 2011, illustrated in Figure 8, provides a network-independent architecture framework for M2M [7]. It adopts the principle of separation between service functions and transport functions as specified in the NGN functional architecture [4], and focuses on the service layer aspects.

The ETSI "M2M service capabilities functional architecture framework" published in 2013, illustrated in Figure 9, extends the previous framework in some deployment aspects [8].

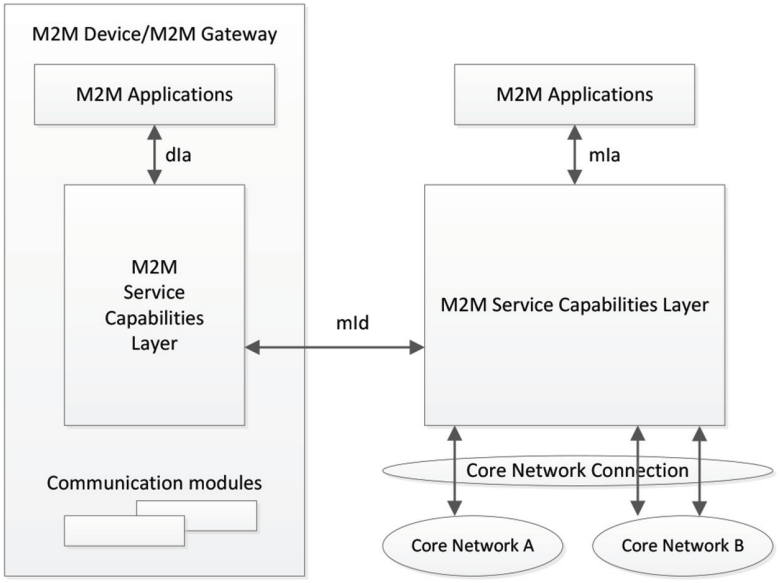

Figure 8 ETSI M2M service capabilities functional architecture framework published in 2011

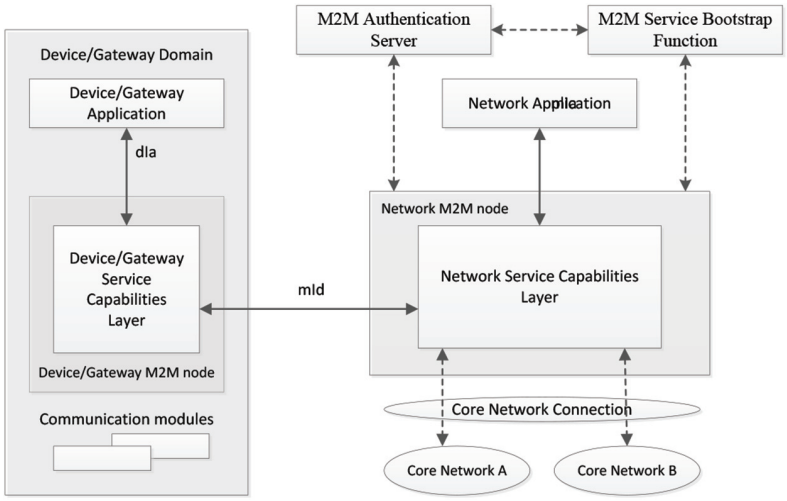

Figure 9 ETSI M2M service capabilities functional architecture framework published in 2013

It can be realized that the ETSI architecture framework published in 2013 has introduced the concept of node ("Device/Gateway M2M node" and "Network M2M node") in order to emphasize the deployment aspects of the architecture framework, although a clear distinction is not made there between functional aspects and deployment aspects. As already anticipated, functional model and deployment model serve different purposes, and their specifications should be addressed in a distinct way.

The IoT-A project has done a lot of studies on the IoT ARM. The IoT-A ideas and methodology concerning the study of the IoT ARM are - in our opinion - very valuable for further research and standardization activities concerning the IoT ARM. The IoT ARM has been decomposed into IoT domain model, IoT information model, IoT functional model, IoT communication model, and IoT trust, security & privacy model. The framework of the IoT ARM defined by the IoT-A project [9]is illustrated in Figure 10.

In this framework, differently from the proposed framework of the IoT ARM shown in Figure 7, either the communication model or the trust, security & privacy model do not support the IoT functional model, they are simply included within the IoT functional model. This approach may be satisfactory from a research point of view, but may have some limitations from a technical standardization point of view.

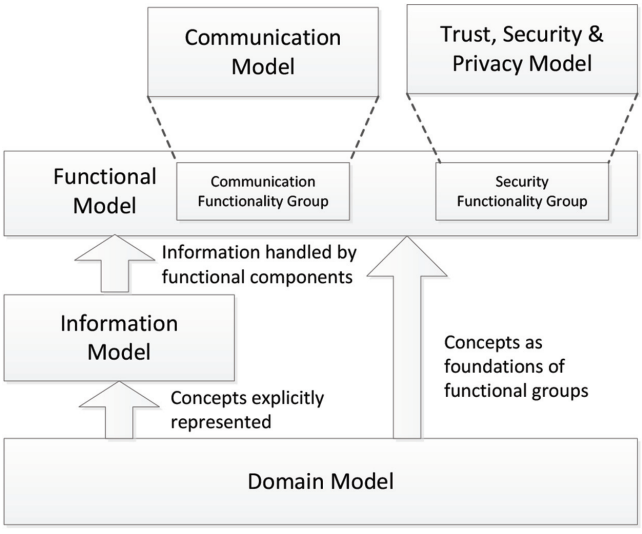

Figure 10 Framework of the IoT ARM defined by the IoT-A project

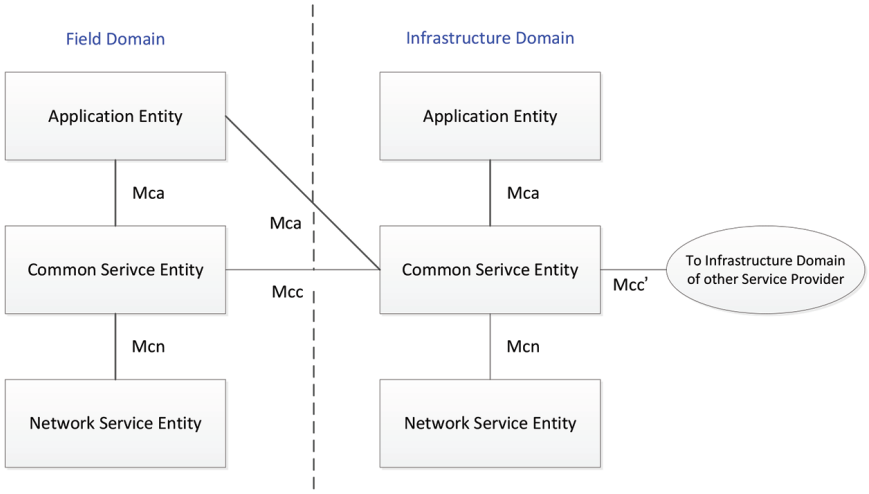

Figure 11 oneM2M functional architecture

As a relatively new effort concerning the standardization of the IoT, it is worthwhile to mention here also oneM2M, a global standards partnership for Machine to Machine Communications and the Internet of Things. As reported in the official website of the oneM2M organization (www.onem2m.org), "the purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide." In summary, oneM2M focuses on the standardization of a common M2M Service Layer that constitutes a part of the IoT architecture.

Among its initial developments, oneM2M is progressing a functional architecture specification: Figure 11 illustrates the oneM2M Functional Architecture [12].

As far as the entities in Figure 11 are concerned: an Application Entity represents an instantiation of Application logic for end-to-end M2M solutions; a Common Services Entity represents an instantiation of a set of "common service functions" of the M2M environments; a Network Services Entity provides services from the underlying network to the Common Service Entities.

As far as the reference points in Figure 11 are concerned, they represent the reference points for M2M communications between relevant entities within a M2M Service Provider or among different M2M Service Providers.

7 Challenges in IoT Standardization

Many IoT technologies are still under development, and a large scale adoption of a given technology usually depends also on the availability of related standards. More globally, the availability of IoT standards of general applicability will be key to the large scale adoption of IoT solutions.

The IoT standardization work faces numerous challenges and this paper only highlights few significant challenging areas: autonomic capabilities, data operations and privacy protection. The availability of IoT standards of general applicability in these three areas involves the development of a standardized ARM of the IoT, as well as the standardization of specific technologies of the IoT.

The autonomic capabilities include capabilities not only for automatic operations, but also for other operations such as self-configuring, self-healing, self-optimizing and self-protecting operations. The implementation of these capabilities depends on the application of the autonomic computing theory, which is currently still a research topic. A challenge faced in the standardization of autonomic capabilities is then how to specify reasonable standards without constraining the technical innovations on autonomic capabilities in the future.

Data operations include not only the data operations for the IoT management and control, but also the data operations for IoT application support and service provision. A challenge faced in the standardization of data operations is how to specify standards for data operations which are independent of the different application domains.

In order to protect the IoT from harmful attacks, it is expected that every IoT user and every IoT device are somehow identified. How to marry identification requirements with proper privacy protection, and consequently how to specify adequate standards, is a real challenge in the standardization of the IoT.

8 Suggestions About the Future Standardization of the IoT

Based on the above analysis and discussions, some principles for the standardization of the IoT have been derived [13]. The following suggestions are given for consideration in the future standardization of the IoT in addition to the standardization of specific technologies.

Suggestion 1: The standardization of the IoT should focus on the interactions among functional entities from a functional perspective and among deployable components from a deployment perspective. This would simplify

the standardization work and impose minimum constraints on future technical innovations.

According to the concept of standardization of the IoT based on the interactions among computing systems (assuming here that a related application can also be regarded as a computing system, so the interactions among computing systems include the interactions between related applications and computing system), and the interactions between computing system and IoT devices, the standardization of the IoT should focus on the capabilities related to the interactions. Some capabilities that are not related to the interactions, such as, for example, the capability for internal storage, should not be the focus of the IoT standardization work.

As an example of this suggestion to focus on interaction aspects, let's consider the capabilities for support of semantics in the IoT. If the related standardization work would focus on interaction aspects such as the exchange formats of semantically described data and the service provision using semantics, this would reduce the standardization work complexity and still leave space for future technical innovations via the research studies on semantics.

Suggestion 2: The standardization of the IoT should also focus on the standardization of the IoT ARM, taking into consideration the various models (i.e., according to the proposed framework of the IoT ARM described earlier, IoT concept and requirement model, IoT information model, IoT communication model, IoT security & privacy model, IoT functional model and IoT deployment model).

It is suggested that the standardization of the IoT ARM be specified at both logical and physical level. The physical level refers here to the deployment oriented level, and the logical lever refers to the deployment independent level. If possible, it is recommended that the logical level specifications be separated from the physical level specifications in order to simplify the technical specifications and provide stability and long term applicability of the logical level specifications.

In order to guide correctly the future IoT standardization work, it is suggested that the standardized IoT ARM be verified in its correctness and completeness. Verifying the IoT ARM is a complex task, but it is worth doing, including for the promotion of technical innovations. In this sense, it is very critical to attract both industry experts and academic experts in the standardization effort concerning the IoT ARM.

Based on this principle of correctness and completeness verification, with specific reference to the work carried out by the ITU-T IoT-GSI, the IoT

standardization work on the IoT ARM should build over the specifications concerning IoT requirements [10,11] and IoT functional framework and capabilities (study currently in progress).

Suggestion 3: The standardization of the IoT should also focus on appropriate work concerning the deployment of the IoT in various application domains (e.g. e-health, intelligent transport systems, smart energy, smart cities), and the integration of IoT relevant technologies (e.g. cloud computing, software defined networking, web services, service delivery platform, data storage, data mining and other big data technologies), in order to strengthen the direct applicability and value of the IoT standards in the industry.

9 Conclusion

Based on the analysis of existing key activities concerning the standardization of OSI, NGN and IoT from a functional architecture perspective, a global view of the interactions in the IoT and a framework of the IoT ARM have been proposed. Also, an evolutionary way to define standard architecture reference models from OSI and NGN to IoT has been analyzed.

Based on these proposals and analysis, it is suggested that, in addition to the standardization of specific technologies, the future standardization of the IoT focuses on the architecture reference model of the IoT, as a guidance for the whole standardization process, and on the interactions among functional entities or deployable components of the IoT, in order to simplify the standardization work and impose minimum constraints on future technical innovations. It is also suggested to progress the IoT standardization work concerning the deployment of the IoT in specific application domains as well as the integration of IoT relevant technologies, in order to strengthen applicability and value of the IoT standards.

Considering that the IoT builds on existing information and communication systems, the IoT standardization work should be conducted in an evolutionary way in order to enable the integration, at the greatest possible extent, of existing information and communication technologies.

References

[1] International Telecommunication Union (ITU), “ITU Internet Reports 2005: The Internet of Things”, 2005.

[2] ITU-T Recommendation X.200 |ISO/IEC 7498-1:1994, “Information technology – Open Systems Interconnection – Basic Reference Model: The basic model”, 1994.

[3] ITU-T Recommendation Y.2011, "General principles and general reference model for Next Generation Networks", 2004.
[4] ITU-T Recommendation Y.2012, "Functional requirements and architecture of the NGN", 2010.
[5] ITU-T Recommendation Y.101, "Global Information Infrastructure terminology: Terms and definitions", 2000.
[6] D. Clark, C. Partridge, J. Ramming and J. Wroclawski. "A knowledge plane for the Internet". Proceedings of ACM SIGCOMM2003, August 2003, pp. 3-10, 2003.
[7] ETSI TS 102 690 v1.1.1, "Machine-to-Machine communications (M2M); Functional architecture", 2011.
[8] ETSI TS 102 690 v1.2.1, "Machine-to-Machine communications (M2M); Functional architecture", 2013.
[9] IoT-A Deliverable D1.4, "Converged architectural reference model for the IoT v2.0", 2012. http://www.iot-a.eu/public/public-documents/documents-1 (visited on 2014-02-26)
[10] ITU-T Recommendation Y.2060, "Overview of the Internet of Things", 2012.
[11] ITU-T Recommendation Y.2066, "Common requirements of the Internet of Things", 2014.
[12] oneM2M, oneM2M-TS-0001 - V-2014-08, "oneM2M Functional Architecture Baseline Draft", 2014-08-01.
[13] S. Shen, M. Carugi, "Standardizing the Internet of Things in an Evolutionary Way", Kaleidoscope 2014.

Biographies

Subin SHEN received the bachelor's, master's and PhD degrees in computer science and engineering from the Southeast University (SEU), Nanjing, China.

He is a professor in the School of Computer and the School of Software at the Nanjing University of Posts and Telecommunications (NUPT), China. His research interests include computer networks, telecommunication networks, the Internet of Things, cloud computing, big data, and future networks. He is one of editors of Recommendation Y.2066 "Common requirements of Internet of Things", Draft Recommendation "IoT functional framework and capabilities", and Draft Recommendation "IoT application support models" of International Telecommunication Union, Telecommunication Standardization Sector (ITU-T). He is a member of the Institute of Electrical and Electronics Engineers (IEEE), Association for Computing Machinery (ACM), China Computer Federation (CCF), and China Institute of Communications (CIC).

Marco Carugi Rapporteur for Question 2 of Study Group 13, International Telecommunication Union, Telecommunication Standardization Section, Geneva, Switzerland

Marco Carugi is currently Independent Consultant on advanced telecommunication technologies and associated standardization. During his professional career, he has worked as Telecommunication Engineer in the Solvay group, as Research Engineer in Orange Labs, as Senior Advisor in the Nortel Networks CTO division and as Senior Expert in the Technology Strategy department of ZTE R&D.

He is active in standardization since 1997, leading the development of numerous standards specifications and holding numerous leadership positions, including ITU-T SG13 vice-chair, Rapporteur for ITU-T Questions and ad-hoc groups, OIF Board member, IETF Provider Provisioned VPN working group co-chair. Currently, he is Rapporteur for Question 2 - "Requirements for NGN evolution and its capabilities including support of IoT and SDN" - inside ITU-T SG13 (Future networks), acts as SG13 Mentor and leads the development of technical specifications on requirements, capabilities and services for IoT/M2M in the ITU-T Internet of Things Global Standards Initiative.

Future Networks, SDP, SDN and Cloud Computing are other technical areas in which he is involved at present.

Marco holds an Electronic Engineering degree in Telecommunications from the University of Pisa in Italy, a M.S. in Engineering and Management of Telecommunication Networks from the National Institute of Telecommunications (INT) in France and a Master in International Business Development from the ESSEC Business School in Paris.