ISO/IEC JTC 1
Information technology

Internet of Things (IoT)

Preliminary Report 2014

Our vision

To be the world's leading provider of high quality, globally relevant International Standards through its members and stakeholders.

Our mission

ISO develops high quality voluntary International Standards that facilitate international exchange of goods and services, support sustainable and equitable economic growth, promote innovation and protect health, safety and the environment.

Our process

Our standards are developed by experts all over the world who work on a volunteer or part-time basis. We sell International Standards to recover the costs of organizing this process and making standards widely available.

Please respect our licensing terms and copyright to ensure this system remains independent.

If you would like to contribute to the development of ISO standards, please contact the ISO Member Body in your country:

www.iso.org/iso/home/about/iso_members.htm

This document has been prepared by:

ISO/IEC JTC 1

Cover photo credit: ISO/CS, 2015

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. +41 22 749 01 11
Fax. +41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

1 Introduction and Scope

The ISO/IEC JTC 1/SWG 5 was chartered to by JTC 1 in 2012 and modified in 2013 with the following "Terms of Reference" (ToR):

1. Identify market requirements and standardization gaps for Internet of Things (IoT);
2. Encourage JTC 1 SCs and WGs to address the need for ISO/IEC standards for IoT;
3. Facilitate cooperation across JTC 1 entities;
4. Promote JTC 1 developed standards for IoT and encourage them to be recognized and utilized by industry and other standards setting organizations;
5. Facilitate the coordination of JTC 1 IoT activities with IEC, ISO, ITU and other organizations that are developing standards for IoT;
6. Periodically report results and recommendations to JTC 1/SWG on Planning;
7. Provide a written report of activities and recommendations to JTC 1 in advance of each JTC 1 plenary meeting; and
8. Study IoT reference architectures/frameworks and provide a study report. This study report should be written so it could be referenced in a possible JTC 1 New Work Item Proposal on IoT.

This report is in fulfilment of it's ToR 7 and 8 and will focus on the result of study on understanding of IoT, market requirements, standards gaps and reference architectures.

2 Background

Various outlooks exist for defining the significant opportunity for globally interconnected and networked "smart things" resulting in an IoT. The following statistics demonstrate that while the estimated volume of connected things may vary, the market impacts are projected to be quite significant.

"*Global machine-to-machine connections will rise from two billion at the end of 2011 to 12 billion at the end of 2020*." – Machina Research

Cisco Systems Inc. Chief Executive Officer John Chambers said that the Internet of Everything – connected products ranging from cars to household goods – could be a $19 trillion opportunity. Only 0.6 % of physical objects that may one day be considered part of Internet of Things are currently connected. (Source: Cisco)

"The vision of more than 50 billion connected devices will see profound changes in the way people, businesses and society interact." -Ericsson

The Internet of Everything could boost global corporate profits by 21 % by 2022, Cisco said in slides prior to Chambers's presentation. By 2020, 50 billion objects will be connected to the Internet, according to the slides. - Bloomberg

3 Activities

SWG 5 had four physical meetings and three electronic meetings as follows:

SWG 5 established Ad hoc Groups to work on the four items identified in the ToR:

1. Develop a common understanding of IoT (Ad hoc Group 1: AHG1)
2. Identify market requirements for IoT (Ad hoc Group 2: AHG2)
3. Identify standardization gaps and develop a standards roadmap for IoT (Ad hoc Group 3: AHG3)
4. Prepare a Study Report on IoT reference architectures/frameworks (Ad hoc Group 4: AHG4).

These Ad hoc Groups had 30 electronic meetings and a report of their work is included in this report.

4 What is the Internet of Things (IoT)?

SWG 5 AHG1 was formed at the 1st Meeting of ISO/IEC JTC 1/SWG 5 (IoT) in Berlin, Germany, March 6-8, 2013. It was tasked to develop a common understanding of the IoT with the following ToR:

ISO/IEC JTC 1/SWG 5 notes that IoT has diverse applications and encompasses many technical and non-technical disciplines, including, but not limited to, physical connectivity, data manipulation, application interfaces, regulatory issues, and cyber security. Therefore, SWG 5 agrees to develop a common understanding of IoT with an IoT Mind Map that would be essential to the work it has undertaken.

AHG1 started its work with a search for existing definitions for the IoT. It became clear right from the outset that the notions of IoT, Cyber Physical Systems (CPS), and Machine to Machine Communications (M2M) were quite similar. This conclusion was reached based on observing M2M standardization activities at ETSI and one M2M as well as academic research in the CPS area. Therefore, AHG1 expanded the scope of its search and identified about two dozen definitions for IoT, M2M, and CPS that were regarded as better than many others that were found. More definitions were found and added to the list of reasonable definitions later. Over the past two years, other notions such as the Industrial Internet, Internet of Everything, and Industrial IoT have been proposed that SWG 5 regards them as too similar to the IoT. Hence, SWG 5 decided to define the IoT in such a way that it would include the characteristics of all these similar notions. It is unlikely that in the long run more than one of these terms would survive.

The process of arriving at an IoT definition for ISO/IEC JTC 1 was hardly easy. Every member of SWG5 had her/his views of what the IoT was about. Each member could write down a list of traits the IoT should have and each did not have a strong objection to the traits identified by other members. However, it became clear that a long definition that would cover all these traits would not be useful and hence would not be widely adopted. It was important to develop a fairly short definition that would encompass the most important traits and characteristics of the IoT only. After almost 16 months of difficult debate (with a 4 to 5 month gap in the middle), SWG 5 agreed on the following definition for the IoT at its 4th meeting in London, England, July 29-31, 2014:

An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.

SWG 5 recognized early on that there is no way of capturing all the complexities of the IoT in a 2 to 3 line definition. Therefore, AHG1 was tasked to develop a mind map for the IoT as a tool to facilitate the work done in other ad hoc groups within SWG 5 (see the documents "IoT Mind Map", "IoT Mind Map-Technologies" and "IoT Mind Map-Application Domains" in Internet of Things Preliminary Report Annexes). Specifically, the IoT mind map serves the following purposes:

— The "Application Domains" and "Stakeholders" parts of the mind map are useful in developing market requirements for the IoT.

— The "Application Domains" and "Technologies" parts of the mind map are useful in identifying standardization gaps. In fact, AHG3, which developed a catalogue of more than 400 existing standards that are somehow related to the IoT, mapped each of those standards to one of the technologies expected to play a main role in the development of the IoT.

— The "Requirements", "Application Domains", and "Technologies" parts of the mind map are expected to guide the development of a Reference Architecture (RA) for the IoT.

SWG 5 regards the IoT mind map as a living document and expects it to be used as a reference as ISO/IEC JTC 1 embarks on developing a suite of standards for the IoT. It is a living document in the sense that it may be revised on an ongoing basis as a more complete picture emerges as to what the IoT is all about. It should be noted that taxonomies of the kind depicted by the IoT mind map are never unique. There are many ways to organize the material. Some topics may be missing, and the depth at which different technical areas have been presented is not uniform across the board. Yet, SWG 5 believes the mind map is a good representation of what the IoT is about and should serve as a good resource for the purposes listed above.

Given that the IoT mind map grew so large, to make it more user-friendly, it was decided to break it into three mind maps. The top-level mind map shows what the IoT is about. Two of the leaves in this mind map are hyperlinks to two other mind maps, one for "Application Domains" and the other one for the "IoT Technologies". The best way to use the IoT mind map is to work with its soft version along with a mind map software. This allows collapsing all subtrees of the mind map, particularly in the "IoT Technologies" mind map, and keeping only the first level children of the root node that comprise the main technologies in the IoT. One can then expand and collapse the nodes for these technologies one at a time to get a more in-depth understanding of what each technology entails as it relates to the IoT.

AHG1 also spent some time developing an "IoT Terms and Definitions" document which is mostly a collection of existing definitions from various standards. SWG 5 recognizes that development of a comprehensive terms and definitions document constitutes a major project that is beyond the scope of SWG 5.

4.1 IoT definition

AHG1 produced the following definition which was adopted by SWG 5:

"An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react."

5 Introduction to market requirements for IoT

The market requirements for the IoT is a complex topic due to the diverse views of "market." AHG2 determined that this is actually two sets of requirements, the "IoT drivers" and the "market segments". This report will focus on the overarching "market requirements."

A common definition is required to have coherent discussion. This document uses the definition from the work of AHG1:

"An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react."

5.1 What are the "IoT drivers" of "market requirements"

Various outlooks exist for defining the significant opportunity for globally interconnected and networked "smart things" resulting in the IoT. Not only are new technologies becoming available that will allow us to achieve the goal of a connected IoT, but the goals of users requires the functionality that the IoT will provide.

5.2 Technology drivers

In producing this report, the group determined that technology forecasts, which vary widely, are a reflection of the point of view of the prognosticator. For example, Cisco is looking at direct connections of objects but does not seem to account for indirect connections. An example of an indirect connection would be an RFID tag which has data which, when sensed, might trigger some autonomic activity.

5.2.1 Technology forecasts

As noted in the background section of this document, the market impacts are projected to be quite significant.

In the Gartner Hype Curve for the IoT, even though the "technology" is possible to use, it might not end up being used as initially expected due to a certain market complexity. Depending on the complexity, it may not end up to be what was initially expected. An example is with RFID adoption in the retail supply chain that has not reached the levels expected when it was at the top of the Hype Curve.

With the general consensus on the potential and significant impacts of the IoT, these projections show how technology is changing and will be one driver for the IoT.

5.2.2 Technology

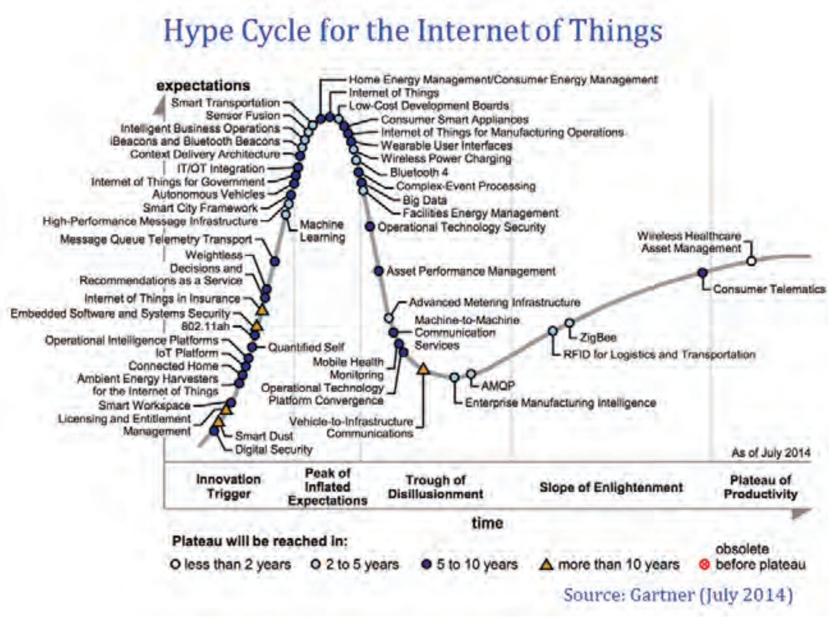

Figure 1 — Hype cycle for the Internet of Things (IoT)

Examples of technology that are considered to be part of the technology driver are:

— Low-power devices;

— Connected devices;

— Computing and distributed processing power;

— Advanced (intelligent and predictive) sensors;

— Advanced actuators.

5.3 Stakeholder requirements for IoT

To ensure that standards support the anticipated size of the IoT, AHG2 has determined that the following issues and topics need to be considered as the market requirements of the IoT:

5.3.1 Ease of use

Stakeholders want the IoT systems to be easy to use, easy to build, easy to maintain, and easy to repurpose.

5.3.1.1 Seamless connectivity — Plug and play (user level)

Stakeholders want to easily add new components to an IoT system. For the purposes of this document, we note that the use of the term device is synonymous with component.

5.3.1.1.1 Components

Stakeholders want to be able to correctly access any identified IoT component and connect any components to other components and be able to add diverse and heterogeneous devices. The concept of identification of components is crucial. It is important to be able to access the right component.

5.3.1.1.2 Communications

Stakeholders want to be able to use whatever communications network best meets the requirements for a specific task (e.g., latency, jitter, bandwidth, availability).

5.3.1.1.3 Timeliness

Stakeholders want to monitor and control physical systems with a wide range of timing requirements using the IoT.

5.3.1.1.4 Sensors and actuators

Stakeholders want to sense and act upon the physical world.

5.3.1.1.5 User experience

Stakeholders want the experience of using, managing, and building systems with the IoT to be easy and pleasant while meeting all the user needs.

5.3.1.1.6 Information fusion model of sensing object

The method of integration of multiple information and knowledge representing the same real-world sensing object into a consistent, accurate, and useful representation. It will help to fully take the usage of the IoT information resources for different application and service within an IoT system or between different information systems.

5.3.1.2 Autonomic services provisioning

Stakeholders want the IoT services to be provided by capturing, communicating and processing automatically the data of “things” based on the rules configured by operators or customized by subscribers. Autonomic services may depend on the techniques of automatic data fusion and data mining. Some “things” may be equipped with actuators to act on the surrounding environment.

5.3.2 Data management

5.3.2.1 Big data

More and more data are being created along with computing systems capable of analysing this data. Stakeholders want to leverage the amount of data available from a variety of sensors and other data generators. This provides efficient predictive analytics to manage and control networked solutions

5.3.2.2 Decision modelling and information processing

Dealing with data mining, the process of a data mining consists of data pre-processing, data mining as well as knowledge evaluating and representing.

5.3.2.3 Common data format for collaborative data processing

The mixing and mashing of data gathered by many IoT applications adds values to the collected data as a whole and to facilitate such data exchanges, the IoT applications require common data formats and application programming interfaces (APIs) so data can be accessed and combined as needed. The focus should be on semantic interoperability as syntactic interoperability can be achieved through simple translation.

5.3.2.4 Cloud service structure

Stakeholders want flexibility in how they implement and use the IoT. Stakeholders want to have access to the IoT systems anywhere. Stakeholders want to pay only for the amount of service they use. Stakeholders want to be able to quickly provision and de-provision a system.

5.3.3 Security

Stakeholders want confidence that the IoT systems cannot be used for malicious purposes by unauthorized entities. As systems built using the IoT will meet a variety of goals, different levels of security will be needed (and different levels of confidence).

5.3.4 Privacy/confidentiality

Stakeholders want confidence that their personal and business information is kept confidential.

5.3.5 Regulation

Stakeholders want IoT systems to be compliant with all relevant regulations and solutions based on common global architectures while supportive of regional requirements.

5.3.5.1 Health and safety

Stakeholders want to leverage new sensing technology to improve health and safety of individuals and of the community, this includes better monitoring of an individual's health conditions, improved communication with their medical providers/doctors, and providing data about emergency situations. This has to be done in a manner which meets relevant regulations (of particular concern is the confidentiality of private information).

5.3.5.2 Environmental protection

Stakeholders want to use the increased interaction with the physical world to better monitor and act upon our environment and reduce the negative environmental impact, following local regulations as required.

5.3.5.3 Technical regulations/regional/global — (2.4 GHz band example)

Stakeholders want to be sure that all aspects in global technical regulation of wireless technology in the IoT is being observed by all SDO's in the IoT - and that an equal and non-discriminating access to the shared worldwide wireless spectrum is ensured to foster the development of the IoT systems herein.

Real-time access, in particular is an issue in the IoT wireless environments and here -as an example- that some newer developments in standardization lead to problems in medium access in advanced automation industry environments (Integrated Industries/Integrated Internet).

Especially graceful degradation in combination with equal medium access of different stakeholders in namely WLAN(Wi-Fi) and Bluetooth (Mesh) 2.4 GHz worldwide frequency bands leads to potential conflicting standardization issues.

As an example the current version of ETSI EN 300328 (v1.7.1) is also used in office (mostly non-real-time requirements) and industrial environments (mostly real-time) as well, and without any known problems in the past.

With the newest release v1.8.1 there will be a potential conflict for future wireless IoT environments in 2.4 GHz as it requires non-real time media access mechanisms like Listen before talk (LBT) on a mandatory base - but now compared to v1.7.1 with – immediate-reaction to release a channel when occupied.

This "little change" to the standard emits great impact on further industrial use-cases, especially for low-power or energy harvesting based devices in the IoT.

Many potential real-time IoT use-cases will be disabled by this issue, and therefore SDO's involved in the IoT must take care on these conflicts, by balancing all requirements of the different stakeholders as well.

5.3.6 Infrastructure

Stakeholders desire interoperability regardless of the infrastructure used, e.g. wired, wireless, closed network, internet connected, etc.

5.3.7 Awareness of service

The IoT services are generally available without human intervention. However, this does not mean that humans (user of the IoT services) do not need to know the existence of the IoT service surrounding the users. When the IoT services are provided to a user, it is recommended that the user can notice the presence of the IoT services and do so in a manner consistent with the relevant regulations.

5.3.8 Accessibility and usage context

Stakeholders want the IoT systems to adapt to individual accessibility requirements and needs applicable in the sector involved. This approach can enable optimum accessibility and usability for diverse users in diverse contexts. It should be recognized not only that needs *are* diverse but that they can vary over time and needs of one user may conflict with those of another and that requirements for a user in one context may be different from requirements of that user in another so that only an approach of adapting to a user's needs in that context at that time can deliver optimum usability for all users.

This requirement applies to systems having direct human user interface and systems carrying data that is used in or has implications for accessibility in directly or indirectly connected systems. Where a human interface to an IoT system involves Information and Communication Technologies (as will commonly be the case) consideration might be given to using "ISO/IEC/TR 29138-1:2009, *Information technology — Accessibility considerations for people with disabilities — Part 1: User needs summary*" as a starting point for determining appropriate user needs.

5.3.9 Cohesive set of standards across all standards domains

Stakeholders desire a common set of standards that allows widespread adoption of the IoT from the various communities promoting IoT, including ISO/IEC, IEEE, IIC, One M2M, etc.

5.3.10 Distributed IT and communications management, e.g. software defined structures and virtualized systems management (e.g. SDN/NFV)

5.3.11 Cross domain/vertical routing management (e.g. one to many distribution flows across the applications domains)

5.3.12 Governance of IoT

Governance's objective is to take a balanced approach in various activities of the organization to achieve enterprise objectives, requiring balancing the risks and resources. The IoT potentially impacts upon almost all aspect of business currently touched by the Internet. Uncontrolled deployment may lead to many risks like invasion of privacy and exposure of proprietary information from businesses. Governance plays an important role in looking at stakeholder's context and needs, setting the direction and monitoring performance and compliance against these needs and objectives, a clear need in the evolving area of the IoT.

Governance of IT (and the IoT) can help to convert the enterprise goals to IT and the IoT goals, followed by the selection of appropriate enablers like policies, frameworks, organization structure, services, infrastructure that support these goals and meeting governance objectives of meeting stakeholders needs and expectations. With the broad impact of the IoT, governance of IT needs to take the IoT into account.

5.4 Summary of the market requirements for IoT

While specific market segments may have some unique requirements for the IoT, the most important considerations applying to all markets are identified above. The market for IoT will be driven by the availability of: low cost; low/sustainable power; interconnected objects, people, systems and information resources; and of the desire to use the functionality provided by a collection of interconnected devices that can be configured into systems and modified as needed.

A reference architecture for the IoT will provide a strong reflection of the technology and stakeholder requirements for the market requirements for the IoT.

6 Standardization gaps

AHG3 was tasked with looking at the standards world and defining where the gaps in standardization lie. AHG3 decided that the only way to examine the standards world for gaps was to try to collect information about existing standards. A template was created to request information from as many standards groups as possible.

Once the input from the various standards groups was collated, over 400 standards had been identified. Because of AHG3's feeling that this data was incomplete, a means to identify the gaps in the standards world was problematic. A document comparing the list of standards to the mind map created by AHG1 was created.

7 Study of reference architectures

A number of standards organisations have worked on creating an architecture in the area of the IoT. There are some application domain specific architectures and some more generic reference architectures. Additionally, a number of fora and consortia have been active in proposing architectures for the IoT, some international research projects have also worked on such developments.

A single IoT reference architecture suitable for all bodies is not an achievable goal so AHG4 identified a number of the IoT reference architectures and began an analysis of the common and domain specific requirements, and also identified differences in the reference architectures studied (i.e. limitations, suitability for different applications). Finally, AHG4 tried to draw some conclusions on the potential impact of these activities for JTC 1; while there is a possibility of defining a generic conceptual model, logical and physical models are likely to diverge and be domain or application specific. The whole report is endorsed by the SWG 5 and the complete report is referenced in Internet of Things Preliminary Report Annexes.

7.1 Requirements for IoT reference architecture

IoT is emerging as a major horizontal activity which will impact the work of many JTC 1 SCs. There is an urgent need for the development of a generic reference architecture which can help ensure a consistent approach to IoT standardization throughout JTC 1.

It is desirable for a committee under JTC 1 to be able to develop the generic standards required for IoT while the specialized work would still be done in the relevant SC, for example security aspects and requirements would be developed in SC27.

8 Conclusions

SWG 5 concludes that the IoT is here now, not just a university challenge and that standardization will be an important part of the needs. The tremendous number of standards identified by AHG3, along with the recognition that this is only a fraction of the number, highlights what an important part that JTC 1 has to play.

Creating a reference architecture and providing a gateway for standards developed in the various JTC 1 committees will provide a massive benefit to the industry. The information collected and created should be made available in the easiest available method if not published as standards.

International Organization
for Standardization

ISO Central Secretariat
Ch. de Blandonnet 8
CP 401
CH – 1214 Vernier, Genève
Switzerland

iso.org

International Electrotechnical
Commission

IEC Central Office
3, rue de Varembé
P.O. Box 131
CH – 1211 Genève 20
Switzerland

iec.ch