ISO/IEC JTC 1 N 9069

2008-05-15

ISO/IEC JTC 1
Information Technology

Document Type:	**Other Document(Defined)**
Document Title:	**Technical Requirements for Sensor Networks and Standardization Items for consideration at the 1st SGSN Meeting, 26-27 June.**
Document Source:	**SGSN Convenor**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for information**
Action ID:	**Information**
Due Date:	
No. of Pages:	**14**

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC JTC 1
Study Group on Sensor Networks

Document Number:	SGSN N010
Date:	2008-05-15
Replace:	
Document Type:	National Body Contribution
Document Title:	Technical Requirements for Sensor Networks and Standardization Items
Document Source:	National Body of Korea
Document Status:	For consideration at the 1st SGSN Meeting, 26-27 June.
Action ID:	FYI
Due Date;	
No. of Pages:	13

SGSN Convenor: Dr. Yongjin Kim, Modacom Co., Ltd (Email: cap@modacom.co.kr)
SGSN Secretary: Ms. Jooran Lee, Korean Standards Association (Email: jooran@kisi.or.kr)

Technical Requirements for Sensor Networks and Standardization Items

Ho-In Jeon

(jeon1394@korenet.net)

Professor, Dept. Electronic Engineering, Kyung-Won University

1. Introduction

This contribution presents technical requirements and relevant standardization items related to wired/wireless sensor networks. Sensor networks together with appropriate sensors installed in target positions are found to have tremendous application areas. However, there is no doubt that u-City would be the greatest market for the sensor networks.

u-City is a city which can provide the residents of the city with safe, convenient, healthy, and wealthy life by installing broadband information infrastructure as well as wireless sensor networks all over the city for the delivery of sensory data, by collecting these data in the uMC and processing them for the provisioning of context-aware services, and thus by being able to provide public services including u-ITS, u-Facility management services, u-Environment management services, and u-disaster protection services in real time, and then by finding new life quality-enhancing services out of which some profits can be produced, such that the residents, when they carry their u-terminals equipped with context-awareness, can entertain all the u-services even when they are not aware of. Figure 1 shows the basic concept of u-City from the point of broadband backbone network, wireless sensor networks, and the services that can be implemented on the top of the information infrastructure.

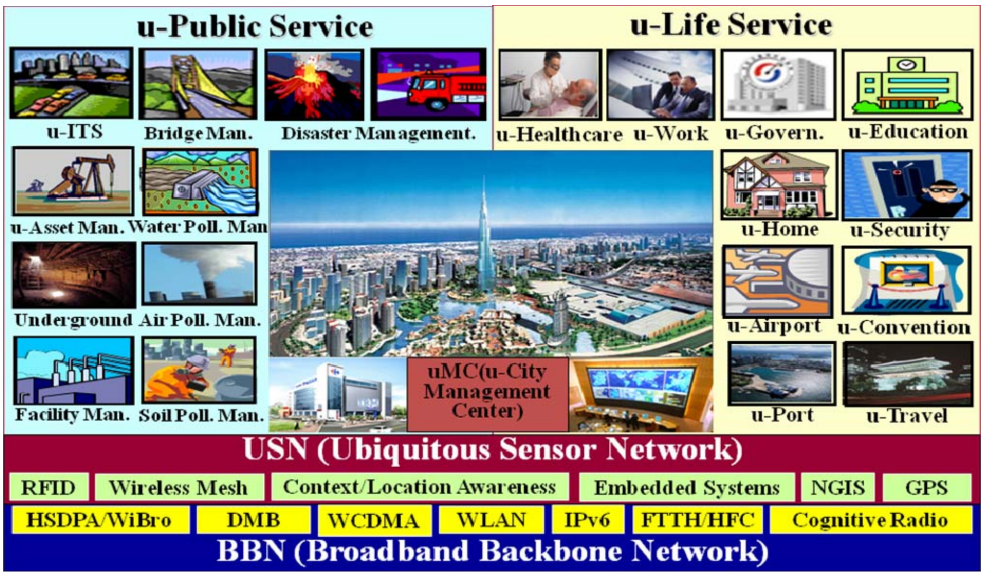

Fig. 1 Conceptual perspectives of u-City

2. Applications Areas of Sensor Networks

The application area of sensor networks can reach from ITS to home automation and AMR(Automatic Meter Reading). The following is the list of applications that sensor networks are used, if it is not the exhaustive one:

- Intelligent Transportation
  - ATIS (Advanced Travelers Information System)
  - ATMS (Advanced Traffic Management System)
  - APTS (Advanced Public Transportation System)
  - CVO (Commercial Vehicle Operation System)
  - AVHS (Advanced Vehicle & Highway Information System)
  - Aircraft Management
  - Fleet Management
- Facility Management
  - Building Management
  - Bridge Management
  - Tunnel Management
  - Underground Facility Management
- Asset Management Assistance
  - Touch/Pressure Sensors (e.g. Art Works, Windows and Doors)
  - Audio and Video Surveillance
  - Smoke and Gas Sensors
  - Structural Integrity/Health Monitoring (Bridges, Tunnels and Highways)
- Building/Home Automation
  - Temperature/Humidity, Heating, Ventilation and Air-Conditioning monitoring and controls
  - Light Sensor and Remote Light Switch
  - Remote Dimmer Control
  - Occupancy/Activity Sensor
  - Damper/Fan/Valve controls
- Defense/Homeland Security
  - Battlefield Monitoring
  - C/B/N Threat Detection
  - Subway/Rail/Bus Monitoring

  - Infrastructure Monitoring
- Industrial
  - Machine Condition Monitoring
  - Inventory Tracking and Surveillance
  - Supply Chain Management
  - Process Monitoring
  - Temperature/Pressure/Flow monitoring
- Agricultural
  - Crop Disease Management
  - Nutrient Management
  - Microclimate Monitoring
- Retail
  - Inventory Management
  - Alarms/Building Security
- Healthcare
  - Hospital Personnel and Equipment Tracking
  - Inventory Tracking
  - Patient Monitoring/Management
- Research
  - Habitat Monitoring
  - Remote Ecological Sensor Network (e.g. endangered species of plants)
- Environment Observation and Forecasting System
  - Weather
  - Environmental Pollution Including Air and Water
  - Seismic sensing
- Automatic Meter Readings
  - Gas/Water/Electricity
- Active Tags
  - Personnel tracking (e.g. coal mine security)
- Ship/Airplane monitoring and control

It is important to note that sensors used for the applications listed above are in fixed positions for the case of environment management systems. However, the sensors for the ITS applications are freely moving at a speed of from 10 Km/hour to faster than 100 Km/hour, in which OBE(On-Board Equipment) is the moving sensor, while RSE(Road Side Equipment) is the infrastructure that are installed to deliver the traffic information to the Gateway over either single hop or multi-hop routes. Some applications like home automations are working in a mixed mode: AMR collects data from fixed sensors while the mobile remote control terminal the residents of the house carry are moving at a speed like 10 Km/hour.

On the other hand, the scale of the sensor network that the home automation application requires is not larger than 100 meters, while that of ITS application needs to cover over several kilometers. The former case can be implemented by using a single network which is defined to have only one gateway with only one NID(Network ID). However, the latter case may require multiple networks with multiple gateways, with multiple NIDs, that are connected through Internet. The technical requirements for the latter case would be more complicated than the former.

It will be more complicated if a u-City implementer of a local government wants to provide a seamless connectivity between home automation application and ITS. In other words, if we consider the case when the home owner with his mobile terminal controlling the home appliances wants to go outside and entertain the ITS services with the same terminal, then the technical requirements cannot be simply listed for each of the applications. Section 3 describes technical requirements of sensor networks, even though it may be impossible to specify all the requirements that can cover all the applications.

3. Technical Requirements of Sensor Networks

From the point of functionalities that wireless sensor networks shall provide, the following is the list of the requirements that the sensor networks need to fulfill to be standardized under the ISO/IEC JTC1 umbrella.

3.1 Sensor Network Topology

The sensor network that is used for the various applications shall support all types of logical topologies including star, tree, and mesh. The star topology is the simplest sensor network with perfect power saving capabilities, least delivery latency, and no waste of address space. However, it suffers from the greatest installation costs with the limited support of device mobility due to the fact that the mobile devices have to re-associate as it moves from one gateway to others.

Mesh networks have the capability to provide (1) extension of network coverage without increasing transmission power or receiver sensitivity, (2) enhanced reliability via route redundancy, (3) Easier network configuration, and (4) longer device battery life. The mesh network, however, has drawbacks of propagation delays over the multiple paths, and additional memories needed to store routing table information. Nevertheless, the sensor network that is to be standardized shall support low power-consuming mesh network topology. The network configuration can be, of course, static or dynamic.

3.2 Bit Rate

The bit rate is categorized as link bit rate, aggregated bit rate (multi-channel or common channel), and End-to-end bit rate (multi-hop). The link bit rate is determined by PHY specifications, and the aggregated bit rate is the sum of link bit rate for each single channel radio. Finally, the end-to-end bit rate is bounded by the aggregated bit rate.

The bit rate that needs to be supported for u-City services is at least 4 Mbps at one radio PHY-SAP for the useful applications of ITS services and voice data delivery, as well as environment management service at the graceful sensor network architecture .

3.3 RF Range

The RF range for the wireless sensor network is mostly determined by its PHY specification. For the case of u-City applications, the RF range shall be 50 meters long, while it can be negotiated from the power-saving aspects. From the communication point of view, the longer RF range would be always preferred than the shorter one because the cost factor of the total installation cost for the specific services could be important.

However, this is not always true when the small form factor with small battery size will require very little power consumption. For example, a small wrist watch that an old lady is wearing for u-healthcare service may not be able to have long-enough RF-range for the sake of power saving purpose. In other words, she wants to keep the small size battery for 2 years. This is the issue of sensor network design in terms of the power consumptions and the battery life.

3.4 Power Consumptions

The wireless sensor nodes must perform the sensor data gathering functions while supporting a battery life of months or years without intervention. Therefore very efficient power-saving modes are desirable, in particular for devices that transmit sporadically.

When the star topology is engaged, the power-saving can be achieved easily because the overall sensor network is allowed to work under the beacon mode. However, mesh network topology that requires multi-hop communications may not be able to provide energy-efficient operation unless smart way of avoiding beacon conflicts is adopted. If the beacon conflicts cannot be avoided, the entire network shall work under non-beacon mode and thus the intermediate nodes of the mesh network have to wake up all the time. Therefore, the synchronization mechanism over the entire network is crucial from the power consumption point of view.

3-5 Data Reliability

For the static sensor node, the link packet loss rate shall be less than 1% for the stable operaion of sensor networks, while end-to-end packet loss rate is application specific. This link packet loss requirement can be alleviated because of the ARQ (Automatic Repeat reQuest) protocol.

For the dynamic topology of the sensor network in which devices are moving at a speed up to 100 Km/h, the engagement of ARQ mechanism is not acceptable. In the case of mobile devices, FEC (Forward Error Correction) as well as ARQ will improve the data reliability. Since FEC adds another complexity to the chip, there is again the compromise between link packet loss rate and power consumptions.

3-6 Propagation Delay

The star topology of a sensor network does not impose any propagation delay, because the communications take place between coordinator and sensor nodes. However, the mesh topology requires multi-hop communications with some communication overheads of hidden node problems and exposed node problems. Maximal end-to-end latency for the sensor network of mesh topology shall not exceed 50ms.

3-6 WAN Connectivity

The Gateway device of sensor networks establishes WAN connectivity for any sensor network. Therefore, the Gateway device shall have both WAN interface and sensor network interface. Regardless of sensor network type (non IP or IP-based), each gateway shall have different network ID(NID) that specifies the sensor network, and NAT (Network address Translation) functions. The sensor network gateway shall not prevent the sensor nodes from being to move from one sensor network to the other.

3-7 Message Flow

The sensor network shall support unicast, multicast, and broadcast. The multicast requires a smart way of grouping, while it has to accommodate reliable broadcasting such that flooding does not cause the deterioration in the performance of the entire network.

3-8 Device Mobility

Device mobility is a mandatory feature related to Intra-SN mobility. Even though roaming or handover functionality requires high computation power, it is good to have it for the better mobility services. Nodes shall be capable of reliable communications when in the move, at least for tracking. It is admitted that limited communication performance (e.g. data rate) can be tolerated in such cases. The considered applications may involve pedestrian, industrial vehicle and optionally high speed vehicle mobility.

Inter-SN mobility is also important for the u-City services, since the entire sensor network may move from one point to others. Examples may be that a moving man wearing a cellular phone with headset profile forms a sensor network having its own NID. Even if this fulfilment of the requirement is extremely challenging at this point of time, it is desirable to have the Inter-SN mobility.

3-9 Network Size

In most cases, home network systems do not contain more than 500 home appliances, while commercial applications such as parking lot systems may include more than 10,000 nodes up to 65,000 nodes. Since u-City services cover from home network to u-ITS services, the size of the network may vary from tens to thousands nodes. Therefore, the network expandability in network density, network size and hop numbers shall be supported. The addressing mode of the sensor network influences the maximum network size and proper addressing modes. The maximum number of hops that the sensor network shall provide can be up to 65,000, without any waste of address space.

3-10 Complexity

The complexity has the relation with unit complexity, system complexity, etc. The sensor node with high chip complexity consumes more power than that with lower complexity. In most cases, chips with faster clock rate consume more power with higher computing power. For sensor nodes, power consumption is one of the most important factors in deploying the wireless sensor networks. Complexity should be minimized to enable mass commercial adoption for a variety of cost sensitive products.

3-11 Network Management

In wireless sensor networks we need to assume that any sensor node may fail to work properly, due to either power failure or link failure. This mal-functioning situation has to be fixed as soon as possible in order for the sensor network to do the right thing for the u-City public services. The amendment of the mal-functioning network can be achieved by network management functionality. Network Management includes: Self-organization; Self-healing; Dynamic routing adaptive to environment; Continuum of distributed to centralized management; and Traffic Priority Control. An idea of SNMP used in IP-based network may be accommodated for the sensor network management purposes.

3-12 Ease of Deployment

Ease of planning, installation, and use for the sensor network is crucial for the easy deployment of the network for the u-City implementations. Consider the case where CO-detecting sensors have been installed in a subway station and the sensed data have been collected using appropriate sensor networks. Suppose, after a while, that new toxic gas such as SO_3 has been detected in the subway station. In this situation, the whole sensor network should have been selected in such a way that the deployment of new sensor and the sensor network that is going to be used for the delivery of the sensory data shall be made easy.

The best case would be that the overall topology of the sensor network should not be modified at all, and the sensors with wireless communication modules are autonomously growing. Wired sensor network will never be able to defeat the advantages of wireless sensor network, even though DOS attack is the fundamental limitation that every wireless network is suffering from.

3-13 Single Association Point without Limitation on the Maximum Number of Children

Most sensor network applications are built with routers installed as the infrastructure. When a new device comes into the network, there always is a node that will allow the new joining of the device, providing the new device with a new logical short address. This node is called the association point of the sensor network, as shown in Fig. 2.

The wireless sensor node designated by "Association Point" is the device that allocates the logical address to every incoming family member's device. If there is any limitation on the number of logical addresses that the association point can allocate, then the new family member would not be able to join in the home network, and the whole home network services cannot be provided. Therefore, the single association point should not impose any limitations in allocating a new logical address. In other words, the association point shall not have any limitations on the maximum number of children to be associated. In this case, the logical addresses to be allocated are systematic, and thus tree routing may have to be given up.

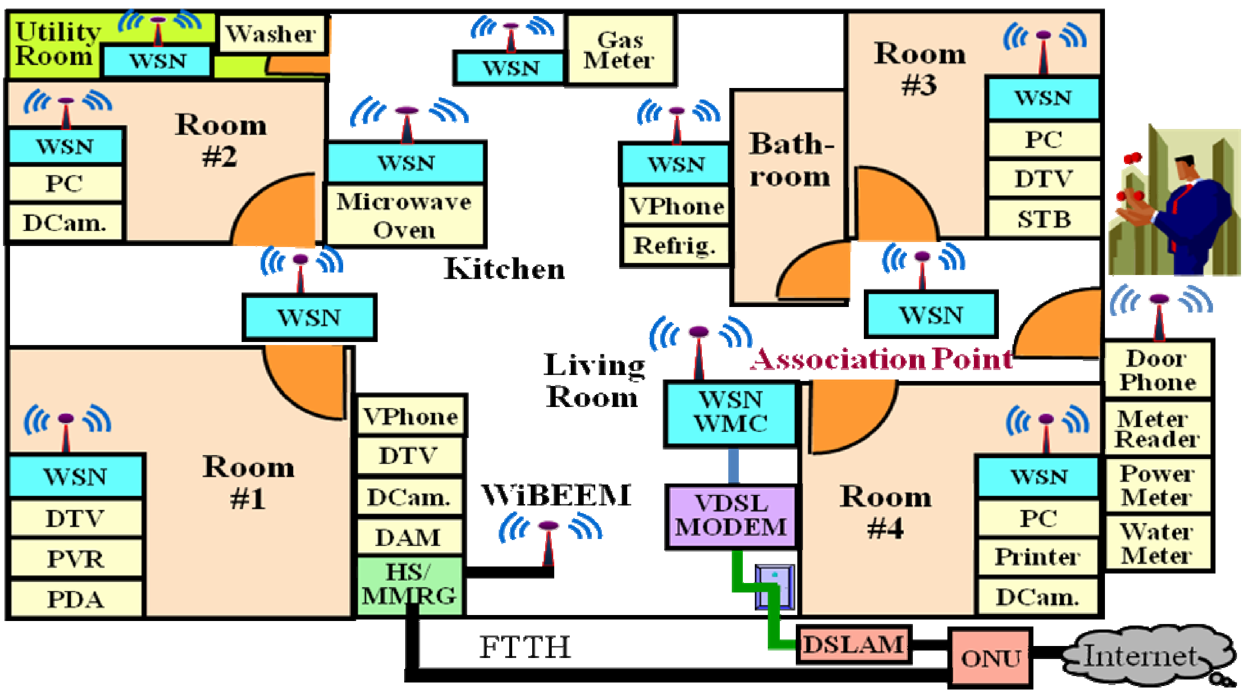

Figure 2 Wireless Sensor Network Infrastructure for Home Network Services

3-14 Fast Association of New Device with the allowance of Dynamic Topology

The ITS service that u-City builders want to provide requires fast-moving vehicles to join in the sensor network and to communicate with the routable devices. This shall allow the OBU of the vehicle to receive the traffic information anywhere the driver wants to know. One single sensor network cannot cover the entire service area of ITS. In other words, more than one segments of sensor networks must be engaged to cover the entire ITS services. Even when the position of the sensor node is dynamically changing, it shall allow fast association of new devices to be able to provide reliable ITS services.

3-15 Fast Routing

Since the device mobility is supported, slow and fast, the supportability of fast routing is important to provide. Because of the large coverage of the service area, tree routing cannot be used due to the limited depth of the network. Consequently, non-systematic addressing has to be used in this case and the routing algorithm such as RIP (Routing Information Protocol) should be adopted. The routing can be proactive, reactive, and hybrid. Whatever the case is, the routing algorithm should be fast enough to track all the moving devices.

3-16 Fast Discovery of Device and Services

When a new device enters into the network area, it should be discovered as soon as possible. At the same time, services that the device provides shall be discovered. A smart way of discovering devices and services shall be used to provide this functionality. It is important to note that heavy traffic taking place to discover the device and services shall be avoided.

3-17 Disassociation Notifications

When a device that has joined already in the network leaves the network, it shall notify the disassociation to the network such that any attributes of the devices, e.g., logical address, shall be reused for the avoidance of waste of address space. The protocol of the sensor network shall en developed in such a way that the disassociation is notified without any burden of the resources.

3-18 QoS Support

Different traffics generated from different nodes have different priorities. The QoS should be supported based on the predetermined policy depending on the different priority. The backoff time may vary depending upon the different priority of users or access category of the traffic. Another way to provide prioritized QoS would be to allocate a time slot in which lower priority traffic are blocked.

The parameterized QoS can be provided based on the resource reservation of the bandwidth. The question is whether the complexity of the protocol provides any burden of the sensor network or not. This would be another compromise issue between enhanced functionalities and power consumptions.

3-19 Hidden Node Problem

Hidden node problems can be serious when a great amount of traffic is generated continuously. There is a way of solving this problem by abandoning the bandwidth of the resource, with inevitable deterioration of the network performance. The packet size can be designed to be short enough such that the hidden node problem can be ignored. However, his will cause the u-City services limited to some extent. There should be some trade-offs between effect of hidden node problem and the level of services.

3-20 Exposed Node Problem

Exposed node problem also causes a degradation of the network performance, while it does not cause a serious network problem. Especially, delay-sensitive traffic cannot live with this problem. It would be good to have a solution for this problem.

3-21 Robustness to External Interference Sources

Every wireless communication system is vulnerable to external interference source. Shorter-range wireless network tends to be the victims of longer-range wireless systems, even though they follow the conformance of the standards. A way of providing robustness to the external interference source shall be provided.

4. Standardization Items for Each Layer

4-1 PHY Layer

PHY layer requires high speed mobility of sensors and devices, if we consider the application area to be u-City services. In this case, mobile terminals are regarded as the sensor nodes. Low-power consuming MODEM shall be adopted for the sensor network. Moreover, it shall be robust to the Doppler shift of the RF signals because we need to support high speed mobility.

PHY layer also requires high speed data transmission capability upto 4 Mbps using low power consuming MODEM. The concept of channel bonding may be used for the enhancement of data rate.

The high speed mobility support may also require FEC(Forward Error Correction) capability in the MODEM. The modulation mechanism could be QPSK, while OFDM would provide better fading characteristics with more power consumptions.

4-2 MAC Layer

MAC layer requires synchronous way of controlling the inactive period of the nodes. This requirement may need a new superframe structure in such a way that multiple beacons shall be transmitted to allow the synchronization. For the case of transmitting multiple beacons, In many cases, it also requires synchronous medium access mechanism for the efficient handling of delay-sensitive traffic.

Error Control: Efficient FEC in energy consumption and computation power. and ARQ

The QoS is also an important topic for the wireless sensor network. Low power-consuming mesh network are also affected by the MAC protocol. So, services shall be predetermined before MAC specification is determined.

4-3 NWK Layer

NWK layer performs addressing and routing. For the efficient communication capability, the addressing mode must be selected in such a way that addressing mode should not waste the address space in a rapid way. This address space saving can also be useful when it can provide a device mobility at the NWK layer. Sometimes, an efficient routing algorithm such as tree routing may be given up. High speed routing for the large scale sensor network may also be standardized for the u-City services. Energy-efficient routing is an important topic for the high-performance sensor network specifications.

4-4 APP Layer

APP layer should take care of ASDU(Application Service Data Unit). Therefore, the data representation or format of the sensory data will be extremely important. Moreover, data encapsulation mechanism will be crucial for the safe delivery of the ASDU. The mechanism of generating bonding table between controller and objects to be controlled is a good topic for standardization.

4-5 Security Suite

The security suite for the safe delivery is very crucial. For secure communications of sensor data, complicated encryption algorithm together with nice network security is required as well as key management mechanisms. Encryption keeps unauthorized users from understanding messages and injecting false messages into the system.

Security Services include: Authentication ensures that a principal’s identity or data origin is genuine; Access Control ensures that only authorized principals can gain access to protected resources; Data Confidentiality ensures that only authorized principals can understand the protected data (privacy); Data Integrity ensures that no modification of data has been performed by unauthorized principals; and Non-repudiation Ensures that a principal cannot be denied from performing some action on the data (e.g., authoring, sending, receiving)

However, the communication bandwidth is always limited in the sensor network which consequently constrains the effectiveness of the secure communication capability. The trade-off between limited communication bandwidth and the level of secure communications must be well-defined.

Whatever the case is, the security suite shall be selected after protocols and algorithms running on PHY, MAC, NWK layers, and Routing mechanism are determined.

5. Conclusions

It is interesting to note that ITS is the most important service that most u-City construction administrators want to provide. So, the local government will invest their money in installing the wireless infrastructure for the ITS services. And then the u-City construction administrator would add more services, on the top of ITS infrastructure, including environment management, disaster protection, and facility management services. Since the sensory data are going to be delivered over the ITS infrastructure, the specification of overall sensor networks shall conform the requirements of the ITS infrastructure. This is what we call interoperability between services. The technical requirements and standardizations relevant to them should be specified even though it may not be easy to implement.

In this contribution, we listed some requirements of wireless sensor networks. In order to have successful deployment of the wireless sensor network over the tremendous number of u-Cities, some of these requirements shall be met for a technology to be standardized under ISO/IEC JTC1 umbrella.