ISO/IEC JTC 1/WG 7
Working Group on Sensor Networks

Document Number:	N089
Date:	2010-09-06
Replace:	
Document Type:	Working Draft Text
Document Title:	1st Working Draft of ISO/IEC WD 29182-1, Information technology — Sensor Networks: Sensor Network Reference Architecture (SNRA) — Part 1: General overview and requirements
Document Source:	Project Editor
Document Status:	As per the JTC 1/WG 7 USA recommendation 1, this document is circulated to JTC 1 NBs and WG 7 members for comment.
Action ID:	COM
Due Date:	2010-11-15
No. of Pages:	18

ISO/IEC JTC 1/WG 7 Convenor:
Dr. Yongjin Kim, Modacom Co., Ltd (Email: cap@modacom.co.kr)
ISO/IEC JTC 1/WG 7 Secretariat:
Ms. Jooran Lee, Korean Standards Association (Email: jooran@kisi.or.kr)

ISO/IEC JTC 1/WG 7 N 089

Date: 2010-09-06

ISO/IEC WD 29182-1

ISO/IEC JTC 1/WG 7

Secretariat: KSA

Information technology — Sensor Networks: Sensor Network Reference Architecture (SNRA) — Part 1: General overview and requirements

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International standard
Document subtype: if applicable
Document stage: (20) Preparation
Document language: E

Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Symbols (and abbreviated terms) 1
5 Overview of sensor networks 2
6 Characteristics of sensor networks 3
6.1 Overview 3
6.2 Dynamic provisioning of service 4
6.3 Application inter-working 4
6.4 Types of user 4
6.5 Extension of Internet 4
6.6 Data gathering and pre-processing 5
6.7 Association with location information 5
6.8 Collaborative information processing 5
6.9 Intra-sensor-network communication 5
6.10 Power efficiency and operating lifetime 5
6.11 Dynamic network topology 6
6.12 Robustness, reliability and maintainability 6
6.13 User oriented applications 6
7 General requirements for sensor networks 6
7.1 Overview 6
7.2 Communications 7
7.3 Deployment and coverage 7
7.4 Heterogeneity 7
7.5 Mobility support 7
7.6 Observation of the environment 7
7.7 Power and energy management 7
7.8 QoS support 7
7.9 Robustness 8
7.10 Scalability 8
7.11 Security and privacy 8
7.12 Sensor network management 8
7.13 Network formation 8
7.14 Sensor node capability discovery 8
7.15 Service discovery 8
7.16 Power efficiency 8
7.17 Addressing mechanisms – ITU-T Y.2221 (2009) 8
7.18 ID design – ITU-T Y.2221 (2009) 9
7.19 Secure control messages – ITU-T Y.2221 (2009) 9
7.20 Lightweight Routing – ITU-T Y.2221 (2009) 9
Bibliography 11

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29182-1 was prepared by Working Group ISO/IEC JTC 1/WG 7, Working Group on Sensor Network.

ISO/IEC 29182 consists of the following parts, under the general title *Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA)*:

— *Part 1: General overview and requirements*

— *Part 2: Vocabulary/Terminology*

— *Part 3: Reference architecture views*

— *Part 4: Entity models*

— *Part 5: Interface definitions*

— *Part 6: Application profiles*

— *Part 7: Interoperability guidelines*

Introduction

There are a number of sensor network applications, with a variety of sophisticated functionalities such as burglar alarming, fire alarming, structural health monitoring and meteorological information gathering. Recently sensor network applications are being evolved by new technologies such as wireless sensor networking, context-based processing, global standards, open service environment, nationwide integration, etc. The aim of Sensor Network Reference Architecture (SNRA) is to give an overall understanding that can support this variety of sensor network applications and services.

ISO/IEC 29182 standards comprise of seven parts.

Part 1 provides the general overview and the requirements identified for reference architecture.

Part 2 part provides the definitions of all the terminology and vocabulary used in the sensor network reference architecture.

Part 3 provides the reference architecture views, e.g., business, operational, systems, technical as well as different presentation of the architecture, e.g., functional, logical, etc.

Part 4 provides the description of entity models, e.g., system, subsystem, component models, with their interfaces, functional descriptions, and how they are used in the reference architecture and for implementation.

Part 5 provides detailed, supportive information on the interfaces among the entity models in the reference architecture. The interface definitions include the data/information descriptions, system level specifications, and so on.

Part 6 provides the application profiles that are derived from studies of use cases, scenarios, etc., for sensor network based applications and services.

Part 7 provides the design principles for interoperability based on the reference architecture which is developed with interoperability requirements.

These International Standards can be used by sensor network designers, software developers and service providers to meet customer requirements and the organization’s own requirements for interoperability.

Information technology — Sensor Networks: Sensor Network Reference Architecture (SNRA) — Part 1: General overview and requirements

1 Scope

This International Standard provides a general overview and the requirements identified for the Sensor Network Reference Architecture (SNRA).

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 29182-2, *Information technology – Sensor Network: Sensor Network Reference Architecture (SNRA) – Part 2: Vocabulary/Terminology*

ISO/IEC 29182-3 *Information technology – Sensor Network: Sensor Network Reference Architecture (SNRA) – Part 3: Reference architecture views*

ISO/IEC 29182-4 *Information technology – Sensor Network: Sensor Network Reference Architecture (SNRA) – Part 4: Entity models*

ISO/IEC 29182-5 *Information technology – Sensor Network: Sensor Network Reference Architecture (SNRA) – Part 5: Interface definitions*

ITU-T Recommendation F.744, *Service description and requirements for ubiquitous sensor network middleware (2009)*

ITU-T Recommendation Y.2221, *Requirements for support of Ubiquitous Sensor Network (USN) applications and services in NGN environment (2009)*

3 Terms and definitions

For the purposes of this document, the terms and definitions are given in ISO/IEC 29182-2 and ITU-T Y.2221 (2009).

4 Symbols (and abbreviated terms)

ID Identifier
ICT Information Communication Technology
NGN Next Generation Network
USN Ubiquitous Sensor Network

5 Overview of sensor networks

Sensor network is a system of spatially distributed sensor nodes interacting with each other and, depending on applications, interacting with ICT infrastructures, in order to acquire, process, transfer, and provide information from the physical world and optionally react.

The overall architecture and a set of components involved in realizing various sensor network services are shown in Figure 1. Sensor network gathers environmental information and gateway connects sensor network to backbone network. Date gathered by sensor network is delivered to destination through backbone network. For example, sensor networks can be established by wireless or wired networking technologies; a sensor network can be connected via various access networks (if necessary) to a backbone network like the Internet, NGN or mobile communication network. And finally various sensor network applications may require application-layer technologies such as integrated service, sensory information description and presentation, etc. From the data point of view, data can be captured by sensor nodes and transferred to application through backbone. However, in some cases sensor networks may not need to be connected to the “Rest of the world.” Here “Rest of the world” includes IT companies, service providers, and end-users. In this case, all services are provided inside sensor networks.

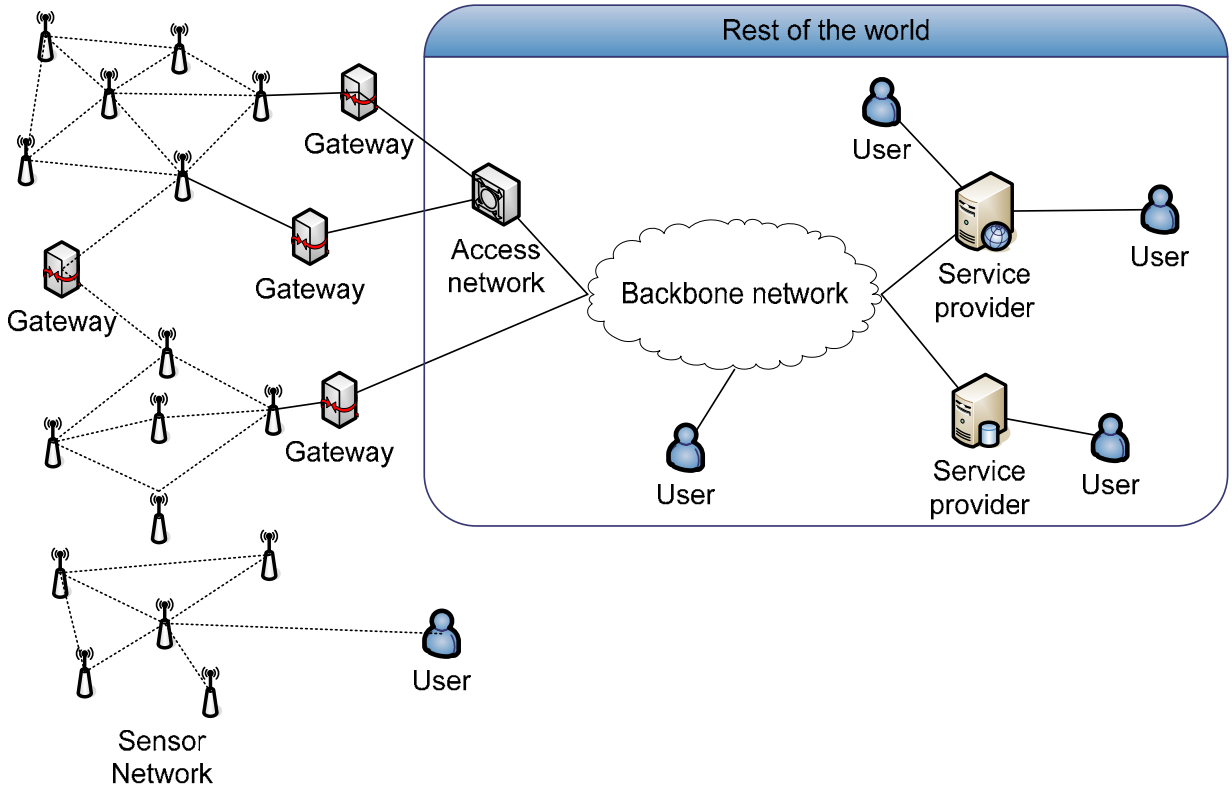

Figure 1 – Overall architecture for sensor network

Figure 2 illustrated a sensor node which consists of: (1) node hardware including different types of sensors; (2) service and basic node functions; and (3) application software modules. Sensor network has the three primary interfaces: (1) interface between service layer and node hardware; (2) interface between service layer and application layer; and (3) interface between sensor network and the “Rest of the world”. The sensor nodes in the network and the gateway (there may be more than one gateway node) connected to “Rest of the World” communicate and collaborate with each other to support the needs of “Rest of the World.” Interfaces for sensor nodes and gateway nodes can be implemented as a middleware. ITU-T F.744 (2009) describes services of ubiquitous sensor network (USN) middleware and defines the requirements for middleware.

Detailed architecture, entity models and interfaces of sensor network are discussed in ISO/IEC 29182-Parts 3,4 and 5.

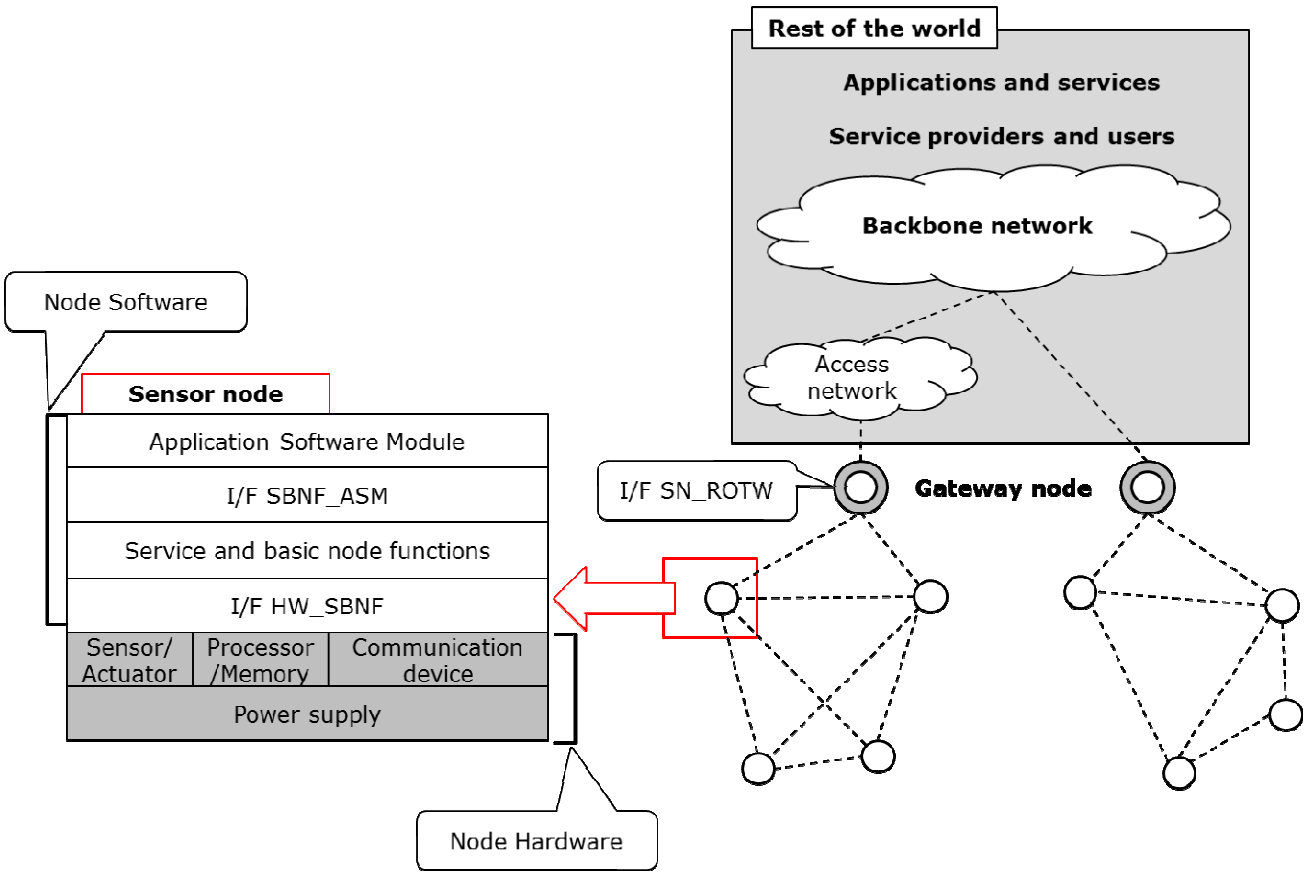

Figure 2 – Overall architecture for sensor network (from the view of sensor node)

A typical node hardware may consists of five main components as follows:

- **Processor** transforms the data and can execute code for other functionalities.
- **Memory** stores programs and intermediate data; usually, different types of memory are used for program and data. Memory may reside in processor as a component of processor.
- **Sensors and actuators** are the interface to the physical environment, i.e., devices that can measure or change the external environment.
- **Communication device** enables a sensor node to send or receive information over a wireless or wired link.
- **Power supply** is a battery, mains power or a type of energy harvesting, such as a solar cell that provides the required energy for the sensor to operate.

6 Characteristics of sensor networks

6.1 Overview

The emerging wired or wireless sensor networks have many unique characteristics. Especially there are many differences between them and traditional wired or wireless networks. Compared with the traditional networks, not only do emerging sensor networks perform data transmission but also perform data acquisition, data

processing, data aggregation, data management, networking management, resource management, automation (sense and actuate), and many other functions and services. The emerging sensor network can connect with existing infrastructures such as database, repository, and other systems through IT backbone and Internet; thus become part of systems of systems (SoS) that provides benefits to home and business.

6.2 Dynamic provisioning of service

To satisfy the different requirements of services for the different users, a sensor network may dynamically process certain sensor data. In comparison, many of the traditional sensor networks (or sensors-on-the-network) have been installed for specific application purposes where consumer service models are not considered. The examples of those include structures monitoring, street light control, agriculture monitoring and management, military surveillance, city facilities management, home utility control, and flood and fire monitoring. In contrast, as an information service infrastructure to improve the quality of life, the sensor networks can incorporate various technologies such as sensor data gathering from various data sources. The example of data source include sensor nodes themselves, other service providers, and private enterprises with functions including data filtering, data mining, context-aware decision making, estimation and forecasting. Moreover, the type of services provided may depend on users' service requirements and expectations. Therefore, it may be challenging for the designer of traditional sensors-on-the-network to pre-determine the application and service features, relevant functions and a wide variety of users. As in the example below, some users may ask for weather information from the weather information services, but due to their different needs, they have different service requirements demanding the different levels of services:

- Fishermen may request on-demand and periodic weather information for fishing;
- Tourists may request periodic and warning/alarming information of the nature's condition for a few days, a week, or a month by a service subscription;
- Crewmen of a ship may request long-term weather forecasting information;
- National disaster centre may request the whole weather information to observe the natural phenomena of an area and detect emergency situations.

6.3 Application inter-working

The emerging sensor network capabilities and functions may allow the a sensor network to be developed benefiting multiple business partnerships whose business areas have been traditionally mutually exclusive, for example, auto industry, private safety and emergency monitoring services industry. Another general example is that a sensor network service provider may need to interoperate with other sensor network service providers to obtain sensor data, processed results, or information to improve the service quality. In comparison, there are many kinds of traditional sensor network applications where these applications usually operate in a mutually exclusive manner, for examples, industrial automation, various types of monitoring and control applications, civil engineering, intelligent building, home automation.

6.4 Types of user

The emerging sensor networks and their applications and services may allow arbitrary and evolving number and grouping of consumers and business partners. For example, weather information may be provided to arbitrary consumers such as tourists and fishermen as well as business partners such as airlines, shipping companies and travel agencies. Predefined users, i.e. business partners, by contracts or agreements may result in B2B-type sensor network services. Arbitrary consumers by service subscription result in B2C-type sensor network services. In comparison, the traditional sensor network applications typically have a dedicated group of users.

6.5 Extension of Internet

The emerging sensor networks may be regarded as an extension of Internet towards the physical world, so-called Internet of Things, connecting physical world with users which cannot simply be regarded as a communication network. Sensors may start to process sensor data and produce information which may be

routed to a user. Here user might be a human or machine. In most cases, the human user does not stand in the foreground. Sensor nodes detect and monitor environment conditions, i.e. the physical world, and/or other physical beings. The raw data from the sensor observation, including detecting and monitoring, is then transformed into different formats of data and information by various types of processing. These data and information are routed to different users according to their requests. In comparison, the traditional sensor networks usually provide predefined linear data processing.

6.6 Data gathering and pre-processing

Usually, the main objective of an emerging sensor network implementation is to gather and pre-process sensor data. Therefore, intelligence on the sensor node may be necessary. And a sensor network may be designed to ensure that all the information is available for the tasks given. Moreover, the communication and data links in the sensor network system have to be reliable and robust. If one of the links is terminated, the sensor network may self-organize and find other ways to route the data or information to the gateway as no human intervention is available to fix the broken link by rearranging or reconfiguring the sensor network.

6.7 Association with location information

For many emerging sensor network applications, sensor data may be associated with sensor's location information. For certain applications producing the location information of a sensor may be one of the most important services provided by a sensor network. The sensor network may offer a service to provide the sensor node location information by a type of localization process, e.g., triangulation or data routing latencies. For certain cases, sensors or sensor nodes in a network have the ability to determine their own location, especially for mobile sensor nodes, e.g., on-board GPS receiver.

6.8 Collaborative information processing

In emerging sensor network applications, the sensor nodes may collaborate to solve complex sensing problems, such as measurement, detection, classification, and tracking in physical world. The data from a sensor may have to be pre-processed and refined at the sensor node or at another sensor node. Depending on applications, intermediary data, such as features or estimated parameters, may need to be extracted from raw sensor data during the pre-processing. The results from this pre-processing may be shared among the sensor nodes in the sensor network. Once shared, the intermediary data from multiple sensor nodes can be transformed into context data and situation information by data fusion.

6.9 Intra-sensor-network communication

Sensor nodes may communicate with each other without an existing communication infrastructure. For this reason, a multi-hop capability and clustering algorithms may be required. Efficient data communications among the sensor nodes are one of the important traits for the measure of performance which is affected by bandwidth and latency. For example, different applications dictate different requirements on latency time. For, example an alarm message has to be routed through a large network in less than a few seconds; for other applications a minute or an hour may be acceptable. Therefore, designing a flexible sensor network for different applications can carefully select data routing schemes and communication protocols that support both types of applications. The design can also consider the cost-effectiveness in developing and operating such a sensor network.

6.10 Power efficiency and operating lifetime

In sensor networks, some devices are powered by main power line but most are battery-operated or use energy harvesting mechanisms and therefore have limited power. In addition, sensor nodes have the characteristics of small devices, limited memory sizes, low speed processors, low bandwidth, high loss rates, etc.; which may lead to specific requirements to mitigate the effect of such limitations. For example, implementation of such sensor nodes may have efficient code, sleep mode, etc.

In the theft prevention system, for example, its batteries may need to be large enough in order to operate sensor nodes and networks for two or three months. In other applications, sophisticated energy management algorithms may needed to maintain the same energy level in all sensor nodes in a network so that the life time

of each sensor node and network can be predicted for maintenance. The wireless sensor network power budget requirements are influenced by power consumption on average and on frequency of peaks per given time period, low overall cost of installation and maintenance, data rate, transmission bandwidth, and communication range. For wireless sensor networks, low data rate, narrow transmission bandwidth, and short communication range (when not using wireless relays to extend the range) are typical.

6.11 Dynamic network topology

The topology of the wireless sensor network is rarely fixed. An emerging sensory network may adapt to the availability of communication links between sensor nodes, to the changing positions of objects to which sensor nodes are attached (e.g., mobility), to energy levels (e.g., node drop out as battery runs out) and roles of sensor nodes. Applications where all the nodes are fixed are relatively easy to handle. In contrast, applications where nodes move within the network can be more difficult to manage. The routing and communication protocols may be very fast and flexible, yet energy efficient. This flexibility in the sensor network topology may not affect networks' performance when sensor nodes enter or leave the network, e.g., the self-healing and self-organizing nature of sensor networks.

6.12 Robustness, reliability and maintainability

A wireless sensor network may operate for a long period of time without maintenance. For wireless sensor network's operations, no operator is typically available to resolve any problem. Maintenance and problem solution capabilities may be restricted to remote maintenance and resolution operations. Thus, the sensor networks may be desired to have basic functions such as self-maintenance, self-organization, redundancy and failure tolerance. Absence of these functions may seriously limit applicability of a sensor network.

6.13 User oriented applications

Functions and services provided by sensor networks may be quite diverse in many applications and in various market segments. This diversity can be managed by developing an application profile to define an application's requirements and operation concepts for each sensor network application. In developing the application profile, usually a better end-user satisfaction is achieved if the developer focuses on the end-user of the system, typically the human users.

For example, the application profile for a subway station security monitoring network may define types of sensor to be deployed (detectors for explosive, poisonous gas, etc.), typical deployment locations, quantity of sensor nodes, information publish mode, function and parameter set, etc. And the application profile should address how the sensor network for the security monitoring system can benefit those people who use subway stations in case of emergency.

7 General requirements for sensor networks

7.1 Overview

In this clause, general requirements for sensor networks are explored. ITU-T Y.2221 (2009) defines requirements for support of USN[1] applications and services in NGN environment. In ITU-T Y.2221 (2009), requirements for USN applications and services are given from the outside NGN point of view as well as NGN point of view. This International Standard refers to ITU-T Y.2221 (2009) for defining general requirements for sensor networks.

The general requirements are considered to be general for all types of sensor network applications, and are used to define functional requirements of sensor network reference architecture.

[1] ITU-T Y.2221 (2009) defines ubiquitous sensor network (USN) as "A conceptual network built over existing physical networks which makes use of sensed data and provides knowledge services to anyone, anywhere and at anytime, and where the information is generated by using context awareness"

7.2 Communications

Sensor networks shall provide communications capabilities between individual sensor nodes. Also sensor network may have communication capability between sensor nodes and a gateway and between a gateway and another gateway.

NOTE: Sensor network communication can be performed by either wired or wireless connections, or a combination of both connections. The communication ranges can vary from short to long distances depending on applied communication protocol, situations and applications. The data rate can vary from low to high data rates.

7.3 Deployment and coverage

A sensor network shall provide information on deployment and coverage for its prospective application.

NOTE: Application's requirements for deployment and coverage are one of the most important requirements for system implementation.

7.4 Heterogeneity

Sensor network application may consist of several different types of networks. Heterogeneous sensor networks supporting an application or applications shall have interoperability among the sensor networks.

NOTE: An application may consist of several different networks. The standards for the interconnection of different networks for interoperability should be established.

7.5 Mobility support

A sensor network with mobile sensor nodes shall support sensor node mobility within the sensor network and shall support the mobility of its sensor node to another sensor network. Also, a sensor network shall accept the transition of a sensor node from another sensor network.

NOTE: Although not all applications have mobile sensor nodes, supporting mobility is very important for some applications such as the applications in Intelligent Transportation System.

7.6 Observation of the environment

Sensor network applications use data which is observed by sensor nodes. Therefore, sensor nodes may observe the environmental data, e.g., temperature, brightness, humidity, motion or vibration.

7.7 Power and energy management

Sensor networks with battery powered devices, e.g., sensor nodes, gateway, etc., may require a power and energy management scheme.

NOTE: Sensor network applications mainly powered by batteries need power/energy management to optimize the sensor network's operation life time.

7.8 QoS support

Mission-critical applications and services should be carefully managed. QoS may be a key technical issue in some scenarios. For example, emergency notification of fire in national treasure monitoring system must be delivered by time-critical and reliable way. Sensor network applications have different QoS requirements, such as data accuracy, reliability, latency, etc.

NOTE: Applications have different QoS requirements, such as data accuracy, reliability, latency, etc.

7.9 Robustness

Sensor networks shall provide and maintain operational robustness. A sensor network should be able to keep working when some sensor nodes die or leave the sensor network.

NOTE: A sensor network should be able to keep working when some sensor nodes die or leave the sensor network.

7.10 Scalability

Sensor networks shall adapt dynamically to provide scalability for various sensor network applications.

7.11 Security and privacy

Sensor networks shall ensure network security and user privacy. In general, sensor network applications highly require strong security and privacy, as the sensed data are very sensitive. There are various security issues which need consideration, such as protection against unauthorized use of network resources and unauthorized access to information and authentication of users.

7.12 Sensor network management

There are different types of sensor network such as IP based sensor networks or non-IP based sensor networks, and wired or wireless sensor networks can co-exist. These diverse types of sensor networks should be managed in transparent way.

7.13 Network formation

Sensor networks can have a fixed static configuration or may adapt dynamically to the addition or removal of sensor nodes, reconfiguring as necessary.

In certain circumstances, maintenance may become impractical and mechanisms such as auto-configuration and self-healing are useful to provide robustness.

In some applications, identification of sensor nodes on a sensor network may be required.

7.14 Sensor node capability discovery

In some applications, the ability to discover the capabilities or characteristics of a sensor node may be required.

7.15 Service discovery

In some applications, the ability to discover the services provided by a sensor node, gateway or sensor network may be required.

7.16 Power efficiency

In order to conserve power in sensor nodes, some applications require efficient software code and memory usage and may implement sleep modes.

7.17 Addressing mechanisms – ITU-T Y.2221 (2009)

In some applications, sensor networks may need scalable addressing mechanisms. In addition, sensor network applications and services may have a variety of traffic patterns requiring Point to Point, Multi-Point and broadcast capabilities, or a combination of these, which needs to be reflected in the addressing mechanisms.

NOTE: In clause 7.17, the term “USN applications and services” is changed to “sensor network applications and service” in this International Standard.

7.18 ID design – ITU-T Y.2221 (2009)

As sensor networks are generally deployed as a stub network in many services, IDs for sensor nodes in the network may be allocated by a coordinator in the sensor network considering the applications and service types. In other way, it could have global address like IP address, but have special naming mechanism for the services. USN applications and services have following ID design requirements:

- In some applications and services, data-aware ID or naming mechanism is recommended. (e.g. temp_etri_x36y30, wind_etri_x36y30) Application functions should support to decode the ID with local or global addresses of the sensor nodes.

- In some applications and services, geographical ID or naming mechanism is recommended. (e.g. temp_etri_x36y30, wind_etri_x36y30) Application functions should support to decode the ID with local or global addresses of the sensor nodes.

NOTE: In clause 7.18, the term “USN applications and services” is changed to “sensor network applications and service” in this International Standard.

7.19 Secure control messages – ITU-T Y.2221 (2009)

Security threats within sensor networks may be different from existing threat models in other networks. E.g. bootstrapping and Neighbor discovery may be susceptible to threats. The following requirement is placed on sensor networks:

- Control messages within sensor networks are required to be secure, in the way that security mechanism should not be overhead of low-powered sensor networks.

- Design for power conservation should not compromise security, especially in sensor network applications with strong security requirements.

NOTE: In clause 7.19, the term “USN applications” is changed to “sensor network applications” in this International Standard.

7.20 Lightweight Routing – ITU-T Y.2221 (2009)

As sensor networks have special requirements on energy saving and data-oriented communication, the following requirements are placed on sensor networks:

- Energy efficient routing schemes are required to be supported.

  NOTE: energy efficiency should not be considered in absolute terms (e.g. support of multi-path routing in case of USN application specific security and resilience requirements)

- It is required to support routing schemes for sensor nodes in sleeping mode at the most of the time.

- It can optionally support data-aware routing schemes.

- It is recommended to support efficient routing schemes for diverse data traffic patterns; MP2P, P2MP, and P2P.

Some USN applications and services are based on large scale sensor networks. To support high scalability, the following requirement is placed on sensor networks:

- Scalable routing schemes (e.g. with reduced routing state) is recommended to be supported for large size of sensor networks.

NOTE: In clause 7.20, the term “USN applications and services” is changed to “sensor network applications and service” in this International Standard.

Bibliography

[1] ISO/IEC JTC1 SGSN N149, *SGSN Technical Document Version 3*

[2] Ken Arnold, "*Tutorial T11: Wireless sensor networks – An enabling technology*," Oceans 2003.