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

Document Number:	N137
Date:	2011-01-19
Replace:	
Document Type:	Working Draft Text
Document Title:	Pre-2nd Working Draft of ISO/IEC 29182-1, Information technology — Sensor Networks: Sensor Network Reference Architecture (SNRA) — Part 1: General overview and requirements
Document Source:	Project Editor
Document Status:	This document is circulated for comments by WG 7 members (1 month period). This document and comments received will be considered at the 3rd JTC 1/WG 7 meeting in Sophia Antipolis.
Action ID:	COM
Due Date:	2011-02-20
No. of Pages:	19

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 137

Date: 2011-01-15

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

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 Networks.

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, 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 provides the definitions of all the terminology and vocabulary used in the sensor network reference architecture.

Part 3 presents the reference architecture from various viewpoints, such as business, operational, systems, technical, functional, and logical.

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

Part 5 provides detailed information on the interfaces among various entities in the reference architecture.

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 the reference architecture that take the interoperability requirements into account.

These International Standards can be used by sensor network designers, software developers and service providers to meet customer requirements and anay applicable interoperability requirements.

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

1 Scope

This International Standard provides a general overview of 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*

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

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)

B2B Business-to-Business
B2C Business-to-Consumer
ID Identifier
ICT Information and Communication Technologies
IP Internet Protocol
MP2P Multi-Point to Point
NGN Next Generation Network
P2MP Point to Multi-Point
P2P Point to Point
QoS Quality of Service
USN Ubiquitous Sensor Network

5 Overview of sensor networks

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

The overall architecture and a set of components involved in realizing various sensor network services are shown in Figure 1-a and Figure1-b.

Figure-1 is the architecture of sensor network services where sensor networks are not connect to a backbone network. In this case, service users may request services to sensor networks directly. In Figure1-b, sensor networks are connected to a backbone network. A sensor network gathers environmental information and a gateway connects sensor networks to a backbone network. Data gathered by sensor networks are delivered to a destination through a 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 networks. And finally various sensor network applications may require application-layer technologies such as data processing (data integration, filtering and so on), sensor information description and presentation, etc. From the data point of view, data can be captured by sensor nodes and transferred to applications through a backbone. However, in some cases sensor networks may not be connected to the “Rest of the world”, where typically includes the Internet or its future incarnations, service providers, and users. In this case, all services are provided inside the sensor networks.

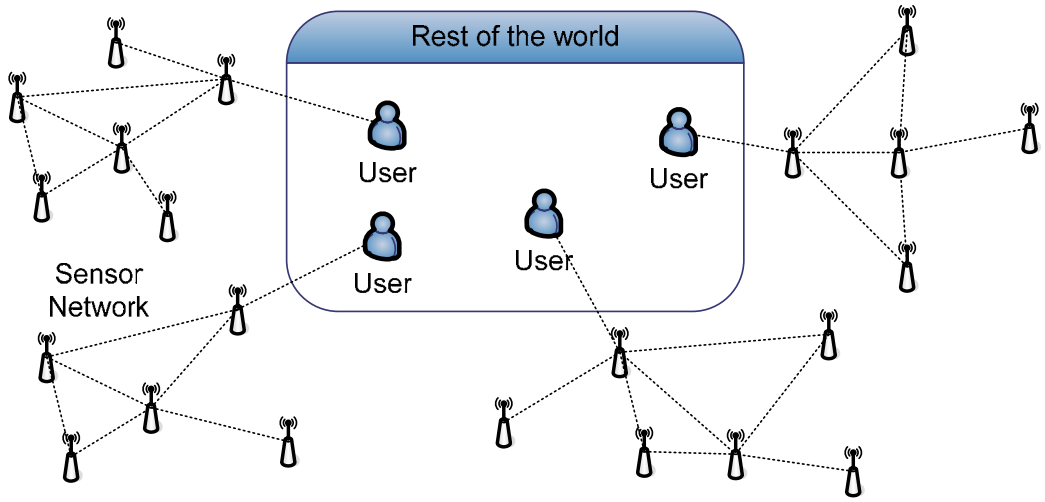

Figure 1.a – Overall architecture for sensor network service (isolated from backbone network)

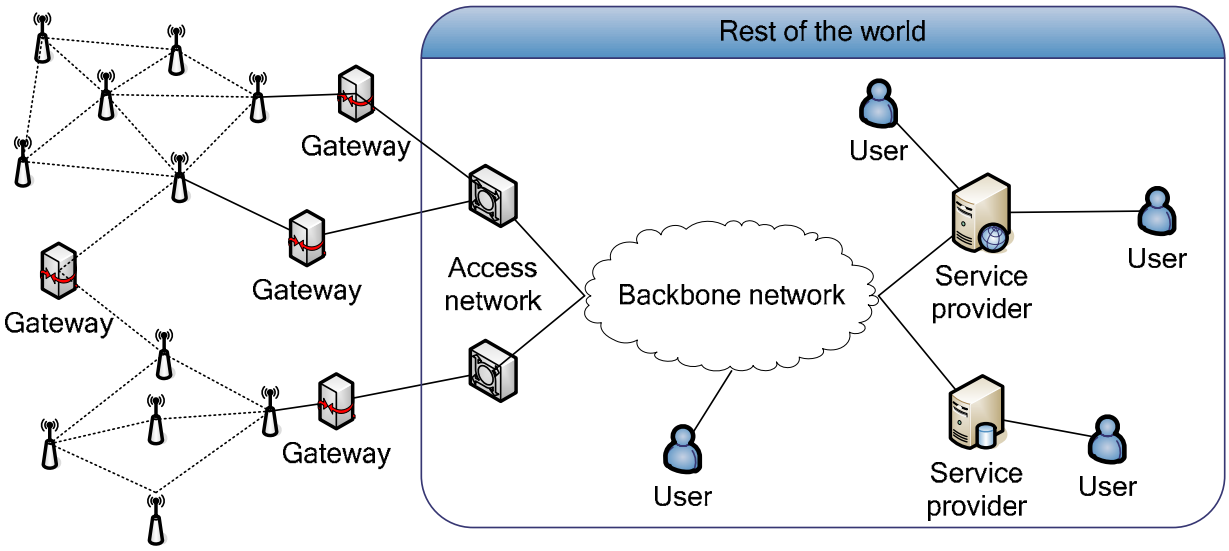

Figure 1.b – Overall architecture for sensor network service (connected to backbone network)

Figure 2 illustrates a sensor node which consists of: (1) node hardware including different types of sensors; (2) service and basic node functions; and (3) application software module. A sensor network has the three primary interfaces: (a) interface between service layer and node hardware; (b) interface between service layer and application layer; and (c) interface between sensor networks and the “Rest of the world”. Sensor nodes in the sensor network and the gateway (there may be more than one gateway nodes) 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 describes the services of ubiquitous sensor network (USN) middleware and defines the requirements for the middleware. Also, OGC 07-165 defines service model standards for integrating sensor networks into Sensor Web, i.e. make sensor networks accessible to the “Rest of the world” via middleware services.

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

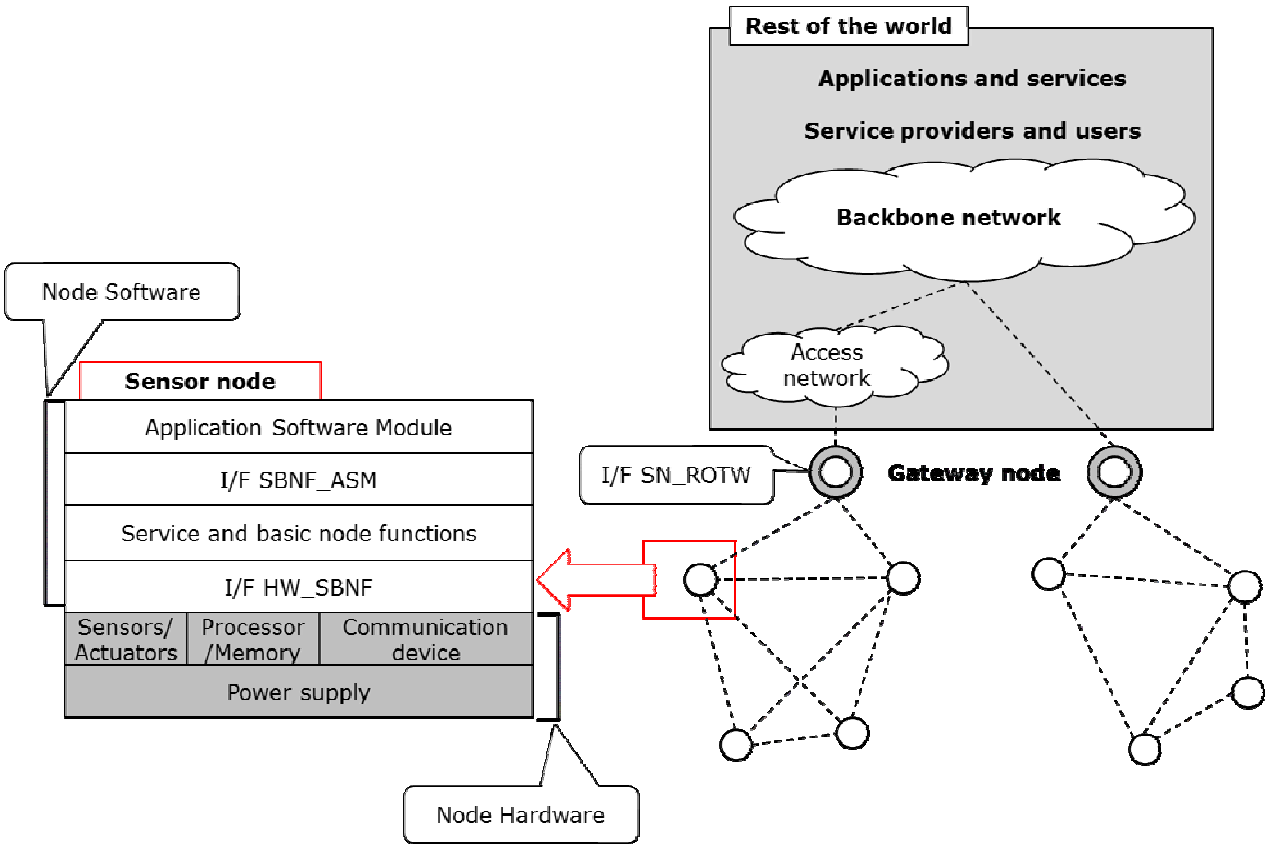

Figure 2 – Overall architecture for sensor network (from the view of sensor node)

Typical node hardware may consist 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.

Service node functions, basic node functions and application software module (ASM) are defined in ISO/IEC 29182-4.

6 Characteristics of sensor networks

6.1 Extension of the Internet

Wired/wireless sensor networks have to be regarded as an extension of the Internet towards the physical world (“Internet of Things”) connecting the physical world with users which cannot simply be regarded as a communication network. Sensors which never have been able to communicate with their environment start to process sensor data and produce information which is routed to a user. The “user” might be a man or a 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’s observation (includes detect & monitor) is then transformed into different formats of data and/or information by various types of processing. These data and information are routed to different users according to their requests.

6.2 Types of users

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 develop in B2B-type sensor network services. Arbitrary consumers by service subscription develop in B2C-type sensor network services. In comparison, the traditional sensor network applications typically have a dedicated group of users.

6.3 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 better user satisfaction is achieved if the developer focuses on the user of the system, typically the human user.

For example, the application profile for a subway station security monitoring network may define types of sensors to be deployed (detectors for explosives, poisonous gas, etc.), typical deployment locations, quantity of sensor nodes, information publish mode, function and parameter set, etc.

6.4 Application inter-working

In tradition, sensor network applications usually operate in a mutually exclusive manner, for examples, industrial automation, various types of monitoring and control applications, civil engineering, intelligent building, and home automation. However, the emerging sensor network capabilities and functions may allow a sensor network to be developed benefiting multiple business partnerships through the application inter-working whose business areas have been traditionally mutually exclusive, for example, auto industry, private safety and emergency monitoring services industry. Another general example for the application inter-working 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.

6.5 Dynamic provisioning of service

Sensor networks accommodate specific user requirements through communication and collaboration among their nodes (both sensor nodes and gateway nodes, when the sensor network is connected to the “Rest of the world”), which allows them acquiring, processing, transferring, and providing information from the physical world and optionally reacting.

Those interactions (communications and collaborations) are driven by the individual embedded sensor node and gateway node programs.

In some areas, like Ambient Intelligence and Self-Serve applications, users’ service requirements and expectations may be diverse and dynamically changing. Sensor networks are incorporated in these applications as field information service infrastructure, which may be combined with other data sources like

private enterprises with functions including data filtering, data mining, context-aware decision making, estimation and forecasting.

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.

6.6 Dynamic request control

When new multiple correspondent users want to get the various types of information (for each user's own) that is directly provided by a sensor node which is already on work, a new request methods is needed for the sensor node which has more resource limitation than the conventional devices such as PC, PDA, Smartphone, etc., which have user interfaces for managing user requests.

The dynamic request control method may be applied for the sensor network. This method is deployed with subscription, which can be accessed by correspondent user itself or administrator which receives requests from correspondent users and manages them. This make the information from a sensor used with various way by each correspondent user. For example, in the case of Shipping Container Monitoring System in which a sensor node (for instance, for temperature and humidity) applied to the container, more than one user (such as shipper, shipping company, container terminal, forwarder, etc.) can get the information from the sensor, which each user want data with its own way (for example, different sensing data, different acquisition period, etc.).

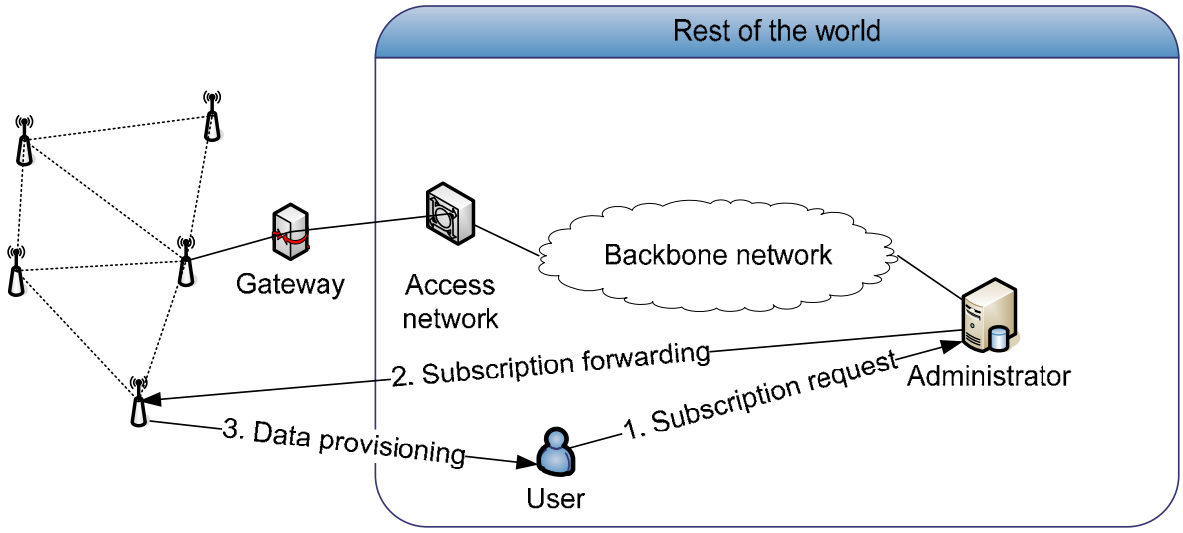

Figure 3 – Subscription model using administrator

6.7 Data gathering and pre-processing

Usually, the main objective of a sensor network implementation is to gather and pre-process sensor data. For providing sensor network services, sensor nodes gather data from the physical world and pre-process data such as integration or filtering before transferring sensor data to back-end systems (in the case of backbone network connected),

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 application, 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 Association with location information

For many emerging sensor network applications, sensor data may be associated with sensor's location information. In certain applications, the output data from sensor nodes is considerably more useful if it is accompanied with the location information for where the data was acquired. In such cases, determination of the location, commonly referred to as localization, of the sensor nodes is one of the most important services that the sensor network would have to provide.

6.10 Maintenance

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.

6.11 Intra-sensor-network communications

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. 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, the routing scheme and communication protocols used by the sensor network have to be designed with the throughput and latency required by the application taken into account. In certain cases, the design has to be sufficiently flexible to support a plethora of applications with different throughput and latency requirements

6.12 Dynamic network topology

The topology of the wireless sensor network is rarely fixed. An emerging sensor 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 flexible and changed very fast, yet energy efficient. This flexibility in the sensor network topology may not affect network performance when sensor nodes enter or leave the network, e.g., the self-healing and self-organizing nature of sensor networks.

6.13 Energy efficiency and operating lifetime

Energy efficiency is important in many sensor networks where the sensor nodes are battery-operated and it is desirable for the network to be operational for as long as possible. In certain short-lived networks, it is not

possible to change the sensor node batteries and the network would stop functioning and essentially dies when a sufficiently large number of its nodes run out of battery power.

7 General requirements for sensor networks

7.1 Communications

The communication capability among sensor nodes themselves, sensor nodes and gateway nodes, and among gateway nodes themselves, may be used for communicating both data and program.

NOTE: Sensor networks communications can be performed by either wired or wireless connections, or a combination of both connections. The communication range can vary from short to long depending on the communication protocol used, situation and application. The data rate can vary from low to high data rates.

7.2 Deployment and coverage

A sensor network shall provide information on deployment and coverage.

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

7.3 Heterogeneity

A sensor network may be heterogeneous in the sense that it may be comprised of several different, inter-connected, interoperable networks.

NOTE: A sensor network application may rely on different sub-networks of a heterogeneous sensor network. Standards for interconnection and interoperability of such sub-networks have to be developed.

7.4 Sensor node mobility support

A sensor network with mobile sensor nodes may support node mobility within the network and from one network to another. Also, a sensor network may accept the migration of a sensor node from another 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 (ITS).

7.5 Environmental monitoring

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.

7.6 Power and energy management

Sensor networks with battery powered devices, e.g., sensor nodes, gateway, etc., may require a power and energy management scheme. There are many ways to reduce energy consumption in sensor nodes, including using low-power and hence low-speed processors, limiting the communication range and transmission bandwidth of the radios used in each sensor node, limiting the storage size, using efficient data processing algorithms, having sensors go into sleep mode according to some schedule, etc. It may also be possible to increase the battery power available to a sensor node through some means of energy harvesting. The lifetime is hence maximized by redistributing the tasks that have to be done by the sensor network among its nodes in such a way that no node dies significantly earlier than the others, even if such redistribution results in an increased overall power consumed by the entire network.

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

7.7 QoS support

Mission-critical applications and services should be carefully managed. QoS may be a key technical issue in some scenarios. For example, detection and notification of fire in certain locations, e.g. a hospital nursery, is time-critical and needs to be done reliably and with low latency. Sensor network applications have different QoS requirements, such as data accuracy, reliability, latency, etc.

7.8 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 for the maximum availability.

7.9 Self-adaptation

For supporting robustness and reliability, sensor networks may self-adapt to accommodate changing conditions, and optimize resource management and the sensor node function.

7.10 Dynamic reprogramming

The goal of dynamic reprogramming consists in changing at runtime the rules that govern sensor network activities. All or only part of the nodes (sensor and gateway nodes) in a sensor network may be concerned by dynamic reprogramming.

Dynamic reprogramming may be triggered manually or automatically. Typically, if the back-end network is related to a dynamic sensor network macro-programming environment or to an automated reasoning system. In these cases, the new program is computed and communicated via the back-end network. New sensor network programs may also be computed by sensor nodes themselves, being provided by another sensor node (case of intra and inter-sensor network code mobility), or acquired directly from interacting end-users.

This is in contrast with many of the traditional sensor networks (or sensors-on-the-network), installed for specific application purposes where consumer service models are not considered.

The examples of those include structural monitoring, street light control, agricultural monitoring and management, military surveillance, city facility management, home utility control, and flood and fire monitoring."

7.11 Location information support

A 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.

7.12 Scalability

There are many ways in which a network can be scalable, including but not limited to the following: number of nodes, per area density of nodes, volume of data traffic that needs to be communicated, mobility, and multiplicity/frequency of events under surveillance.

7.13 Code mobility support

A sensor network may support code mobility to support features like dynamic reprogramming, dynamic reorganization, dynamic resource optimization, as well as to support the implementation of QoS, scalability, security, self-healing, and other quality attribute policies. Code may move within the same sensor network

(intramobility) and to another sensor network (inter-mobility). Also, a sensor network shall accept the transition of a sensor node code from another sensor network.

A sensor network may support dynamic reprogramming (through code mobility) to support dynamic adaptation to changes in user requirements. Dynamic reprogramming may concern all or part of sensor nodes.

NOTE: In contrast with 7.4, in these applications sensor nodes are not necessarily mobile (although could be), but the sensor node code is mobile for optimization reasons, or to accommodate specific end-user needs.

7.14 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 malicious acts to disrupt the operation of the sensor network, protection against unauthorized use of network resources and unauthorized access to information and authentication of users. Also, the privacy of users and user information should be protected, for example the possibility of a violation of privacy by sensor networks should be informed to users and uses shall be able to decide the privacy policy.

7.15 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.

7.16 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.

7.17 Sensor node capability discovery

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

7.18 Service discovery

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

7.19 Addressing mechanisms – ITU-T Y.2221

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 this clause, the term “USN applications and services” of ITU-T Y.2221 is changed to “sensor network applications and service”.

7.20 ID design – ITU-T Y.2221

As sensor networks are generally deployed as stub networks, i.e. networks that have no knowledge of other networks and send their nonlocal traffic to other networks through a few known paths, IDs for sensor nodes in the network may be allocated by a coordinator in the sensor network considering the application and service

types. Alternatively, the nodes could have IP-like global addresses along with special naming mechanisms for the network services. Sensor network applications and services have following ID design requirements:

- In some applications and services, data-aware ID or naming mechanism is recommended (for example, temp_x36y30 for temperature data at the sensor node x36y30, wind_x36y30 for wind data at the sensor node 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 (for example, lat36.13n_long127.59e for the location of 36.13 degrees of north latitude and 127.59 degrees of east longitude). Application functions should support to decode the ID with local or global addresses of the sensor nodes.

NOTE: In this clause, the term “USN applications and services” of ITU-T Y.2221is changed to “sensor network applications and service”.

7.21 Secure control messages – ITU-T Y.2221

Security threats within sensor networks may be different from existing threat models in other networks. For example, bootstrapping and neighbor discovery may be susceptible to threats. The following requirement is placed on sensor networks:

- Control messages in sensor networks are required to be secure and should not be perceived as a burden or overhead even in low-power sensor networks.

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

NOTE: In this clause, the term “USN applications” of ITU-T Y.2221 is changed to “sensor network applications”.

7.22 Lightweight Routing – ITU-T Y.2221

As sensor networks may have special requirements on energy efficiency and data-oriented communications, the following requirements may have to be placed on the routing protocol used by the network:

- 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 sensor network 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 sensor network 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 this clause, the term “USN applications and services” of ITU-T Y.2221 is changed to “sensor network applications and service”.

Bibliography

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

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

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

[4] ISO/IEC 29182-6 *Information technology – Sensor Network: Sensor Network Reference Architecture (SNRA) – Part 6: Application profiles*

[5] ISO/IEC 29182-7 *Information technology – Sensor Network: Sensor Network Reference Architecture (SNRA) – Part 7: Interoperability guidelines*

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

[7] OGC 07-165, OGC Sensor Web Enablement: Overview and High Level Architecture (http://portal.opengeospatial.org/files/?artifact_id=25562)

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

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