INTERNATIONAL STANDARD

ISO/IEC 29182-1

First edition
2013-06-01

Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) —

Part 1: General overview and requirements

Technologies de l'information — Réseaux de capteurs: Architecture de référence pour réseaux de capteurs —

Partie 1: Vue d'ensemble et exigences

Reference number
ISO/IEC 29182-1:2013(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national 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 and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29182-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

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 and terminology*

— *Part 3: Reference architecture views*

— *Part 4: Entity models*

— *Part 5: Interface definitions*

— *Part 7: Interoperability guidelines*

The following part is under preparation:

— *Part 6: Applications*

Introduction

A wide range of applications has been proposed for sensor networks. In practice, however, sensor networks have been built and deployed for a relatively small number of applications. This is partly due to the lack of a business case for certain applications and partly due to technical challenges in building a non-trivial sensor network of reasonable complexity. The main reason for this impediment is multi-disciplinary expertise – such as sensors, communications and networking, signal processing, electronics, computing, and cyber security –is required to design a sensor network. Presently, the design process is so complex that one can leverage little from one sensor network design to another. It appears as if one has to start from almost scratch every time one wishes to design and deploy a sensor network. Yet, upon closer inspection, there are many commonalities in instantiations of sensor networks that realize various applications. These commonalities include similarities in the choice of network architecture and the entities/functional blocks that are used in the architecture.

The purpose of the ISO/IEC 29182 series is to

— provide guidance to facilitate the design and development of sensor networks,

— improve interoperability of sensor networks, and

— make sensor networks plug-and-play, so that it becomes fairly easy to add/remove sensor nodes to/from an existing sensor network.

The ISO/IEC 29182 series can be used by sensor network designers, software developers, and service providers to meet customer requirements, including any applicable interoperability requirements.

The ISO/IEC 29182 series are comprised of seven parts. Brief descriptions of these parts are given next.

Part 1 provides a general overview and the requirements for the sensor network reference architecture.

Part 2 provides definitions for the terminology and vocabulary used in the reference architecture.

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

Part 4 categorizes the entities comprising the reference architecture into two classes of physical and functional entities and presents models for the entities.

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

Part 6 provides detailed information on the development of International Standardized Profiles.

Part 7 provides design principles for the reference architecture that take the interoperability requirements into account.

There are no requirements for compliance in ISO/IEC 29182-1 to ISO/IEC 29182-7. Users should ensure that the sensor nodes, and the related sensor network, are compliant with the application or deployment governing body.

Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) —

Part 1: General overview and requirements

1 Scope

This part of ISO/IEC 29182 provides a general overview of the characteristics of a sensor network and the organization of the entities that comprise such a network. It also describes the general requirements that are identified for sensor networks.

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 networks: Sensor Network Reference Architecture (SNRA) — Part 2: Vocabulary and terminology*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29182-2 apply.

4 Conventions

In this part of ISO/IEC 29182:

The keywords “is required to” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords “is recommended” indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords “can optionally” and “may” indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor’s implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

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 (Information and Communication Technology) infrastructures, in order to acquire, process, and provide information about the physical world and optionally react to such information.

This clause describes sensor networks from a communication perspective and a service provisioning perspective. Figures 1, 2 and 3 illustrate from a communication perspective the overall architecture and logical arrangements of components in three classes of sensor networks. The sensor networks shown in Figures 1, 2 and 3 gather information about their physical surroundings and deliver this information to the

sensor network user(s), and any of the communications links may be implemented using wired or wireless technologies: there is no constraint in principle on mixing communications technologies within a network.

Figure 1 depicts a standalone sensor network that operates on its own and is isolated from other networks. This type of sensor network may be regarded as an ad hoc sensor network.

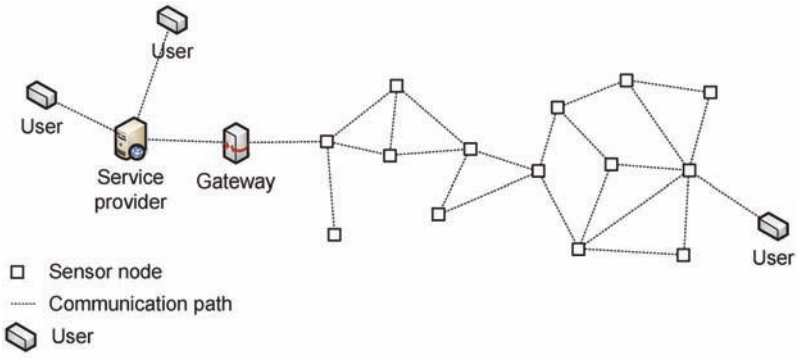

Figure 1 — Standalone sensor network

Figure 2 depicts the case where multiple sensor networks, two in the case of this figure, are interconnected via a gateway. Gateways can play various roles in a sensor network, as shown in Figures 1 and 2 and shortly in Figure 3.

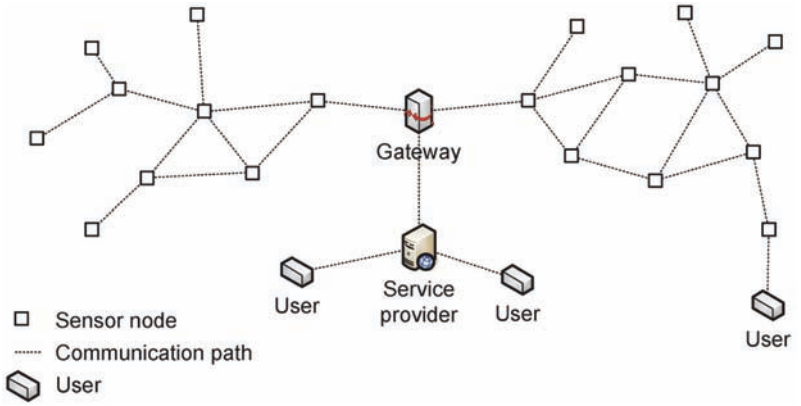

Figure 2 — Interconnected sensor networks

Figure 3 depicts sensor networks, two in the case of this figure, which are connected to a backbone network or other entities. In this case, gateways provide sensor networks with connectivity to other networks possibly through access networks.

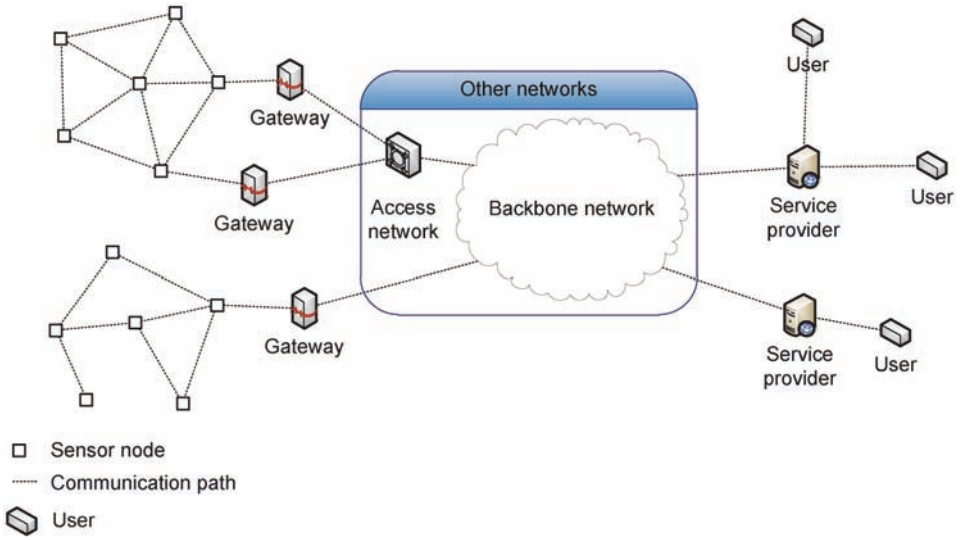

Figure 3 — Sensor networks connected to other networks

Sensor network applications may require application-layer technologies such as data processing (data integration, data filtering), sensor information description and presentation. Data are acquired by sensor nodes and either processed within the sensor network (e.g. sensor nodes in the sensor network) or by service providers connected to the sensor networks, as in Figure 1 and Figure 2. Alternatively it can be transferred, through a backbone network, to applications and other entities such as service providers, as in Figure 3.

As for service provisioning, sensor network services may be provided either by a sensor node directly or by a service provider. Users may request services, without an intermediary, from an arbitrary or a designated sensor node, as in the case of the users on the right side of Figure 1 and 2 or from a service provider, as in the case of the users on the left side of Figure 1, the middle part of Figure 2 and the right side of Figure 3. A service provider gathers sensor data either from sensor networks directly or through a backbone network and facilitates the negotiation of the service to be provided. In some cases, a user that requests services from a sensor node may be integrated with that sensor node.

6 Characteristics of sensor networks

6.1 General

Wired or wireless sensor networks have unique characteristics which differentiate them from traditional data networks. Sensor networks not only perform data transmission but also perform data acquisition, data processing, data aggregation, data management, network management, resource management, automation (sensing and actuation), and other functions and services.

Clause 6 identifies the unique characteristics of sensor networks which differentiate from traditional networks.

6.2 Service provisioning for individual requirements

Sensor network applications and services allow arbitrary and evolving types and grouping of users. For example, weather information may be provided to consumers such as tourists and fishermen as well as business partners such as airlines, shipping companies and travel agencies. Functions and services provided by sensor networks may be quite diverse supporting many applications, market segments and types of users.

Users' service requirements and expectations may be diverse and change depending on circumstances. Users may ask for weather information from a service providing such information, however they may have different requirements depending on their circumstances and applications.

A tourist is content with getting summary weather information once or twice a day for the short period of his/her vacation.

A fisherman, on the other hand, may need periodic weather updates throughout the day as well as warnings for inclement weather conditions as soon as they become available. He would need such weather information for the duration of the fishing season.

The crewmen of a ship travelling on high seas may request extended weather forecasts for the duration of their trip.

A national centre for the study of the climate and weather patterns would need very detailed weather-related information from a wide array of sensors at high sampling rates. Such information is particularly important for prediction of emerging dangerous weather conditions and natural disasters.

6.3 Data gathering and pre-processing

Sensor nodes gather data from the physical world and pre-process the sensed data (e.g. through data integration or filtering) and then supply sensor network services to the user, either directly from the sensor node or via a service provider.

6.4 Collaborative information processing

In some sensor network applications, the sensor nodes may collaborate to solve complex sensing problems such as the detection, classification and tracking of objects in the physical world. The data from a sensor may be pre-processed and refined at the sensor node acquiring the sensed data or at another sensor node. Depending on the application, intermediate data, such as features or estimated parameters, may be extracted from the sensed 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 intermediate data from multiple sensor nodes can be transformed into context data and situation information by data fusion.

6.5 Maintenance-free operation

Sensor networks may have to operate for a long period of time without maintenance or technical support to resolve problems. Provision of remote diagnostics and resolution may be required.

6.6 Dynamic network topology

The topology of a wireless sensor network is rarely fixed. A sensor network may have to adapt to the availability of communication links between sensor nodes, to the changing positions of sensor nodes due to mobility, to energy levels (e.g. a node may drop out as its battery runs out) and to the changing of the roles of sensor nodes (e.g. when a sensor node becomes to take the roles of a sensor network gateway). Implementations where sensor nodes move within the network require routing and communication protocols that are flexible and quick to response to changes. Sensor network topologies have to be capable of handling sensor nodes leaving or joining the network without unmanaged degradation of sensor network performance. Some sensor network topologies are self-healing and self-organizing.

6.7 Energy efficiency and operating lifetime

Energy management 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. Energy harvesting technologies may help with energy management and extending network lifetime.

6.8 Self-adaptation

Sensor networks may self-adapt to accommodate changing conditions, to support robustness and reliability and to optimize resource management and sensor node functionality.

7 General requirements for sensor networks

7.1 Connectivity to other networks

In some sensor networks, it is required to connect sensor networks to other networks, as shown in Figure 3. This is achieved through use of gateway(s).

7.2 Deployment and coverage

A sensor network is typically required to observe and acquire information about the physical world over some pre-determined area in the 3D space called the coverage area of the sensor network.

Sensor networks may be deployed upon the requirements of sensor network applications..

7.3 Support of heterogeneous sensor networks

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

Therefore, it may support interoperability among heterogeneous sensor networks.

NOTE A sensor network application may rely on different sub-networks of a heterogeneous sensor network.

7.4 Sensor node mobility support

A sensor network with mobile sensor nodes can optionally support node mobility within the network and from one network to another.

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

7.5 Power and energy management

Sensor networks with battery powered devices (e.g. sensor nodes or gateways) may require power and energy management schemes.

There are many ways to reduce energy consumption in sensor nodes including using low-power (potentially lower speed) processors, limiting the communication range and bandwidth of radio links, limiting the local storage capacity, using efficient data processing algorithms, and having sensors go into sleep mode according to a schedule. It may also be possible to increase the battery life available to a sensor node through some means of energy harvesting. The operational lifetime may be maximized by distributing the processing tasks among the nodes to balance energy usage and energy availability in such a way that no node dies significantly earlier than the others, even if such redistribution results in an increase in the overall power consumed by the entire network.

NOTE Sensor network applications mainly powered by batteries need power/energy management to maximize the sensor network's operating lifetime.

7.6 QoS support

Mission-critical applications and services should be carefully managed. QoS (Quality of Service) 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 and latency.

A sensor network may support QoS upon the requirements of sensor network applications.

7.7 Dynamic adaptation

7.7.1 Dynamic topology

Sensor networks may have a static topology or may adapt dynamically to the addition or departure of sensor nodes and reconfigure as needed.

Therefore dynamic topology of a sensor network may be supported.

7.7.2 Self-organization and self-healing

A sensor network can optionally support self-organization and self-healing.

Self-organization and self-healing are attributes of wireless sensor networks and they are closely related to dynamic network topology. Self-organization is the capability of the sensor network to form a network graph without the need for any human intervention. The network graph specifies which sensor nodes any given sensor node communicates with. Self-healing, on the other hand, is the network capability to recuperate from failures of sensor nodes or communication links. Sensor nodes may fail due to their batteries running out, hardware failures, or a node simply leaving the network. A communication link can break due to worsening channel propagation conditions due to the two nodes communicating over the link getting far away from each other, shadowing, multipath fading, or RF interference. Once the network self-organizes or heals, then the necessary communications can take place and the sensor network can do its job at an acceptable level of performance.

7.8 Context-awareness

A sensor network may provide context-awareness. Context-awareness is the capability that allows a sensor network to paint a coherent picture of parts of the physical world the sensor network is observing and measuring. For example, there may be a number of sensors attached to the body of a firefighter that enters a burning building. The sensors measure physiological health signs of the firefighter, such as heart rate, breathing rate and body temperature. Other sensors on the firefighter – possibly in conjunction with other sensors in the building – determine firefighter's location and his gait and whether he is walking, crawling, or motionless. These sensor measurements together provide the necessary context and paint a good picture of the firefighter's status and whether he is in need of help. Typically, context information is used as the basis for taking actions in response to the situation at hand, possibly through the use of actuators.

7.9 Scalability

A sensor network may support scalability. There are many ways in which a sensor 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.

7.10 Privacy

A sensor network is recommended to ensure user privacy. In general, sensor network applications require privacy protection, as the sensed data may be sensitive and may be or contain personal information. User information should be protected, and the users should be notified of any occurrence of violation of privacy policies in the network that are set by the users. A privacy risk/impact assessment shall be conducted in order to identify privacy risks related to the proposed sensor network initiative and to identify appropriate privacy safeguards.

7.11 Security

A sensor network may support various security mechanisms. There are many security considerations associated with sensor networks. Examples include malicious acts to disrupt network operations, protection against unauthorized use of network resources, unauthorized access to information, user authentication and accounting. Organizations should also identify and adopt relevant security standards such as ISO/IEC 27002.

7.12 Sensor network management

Sensor networks are often complicated. For example, the network may operate in a centralized or distributed manner. It may use the IP (Internet Protocol) protocol or not. It may be wired, wireless, or a combination of the two. The various aspects of sensor network operation are recommended to be managed in a transparent way.

Also, a sensor node may be managed through sensor network management (e.g. resource management of a sensor node, and task management of a sensor node).

7.13 Discovery capabilities

7.13.1 Sensor node discovery

Sensor nodes may have the capability to detect presence of other nodes. This capability is used for network formation and to support a dynamic network topology, as described in Clause 7.7.1.

7.13.2 Sensor node capability discovery

Sensor nodes may have the capability to not only detect presence of other nodes, but also their capabilities, such as remaining battery power, computational resources and communication capabilities.

7.13.3 Service discovery

In some applications, it is required to find a provider of accommodation and/or activities required by a user or a sensor network.

A service may be provided by a sensor node or by a sensor network (e.g. through a service provider). A sensor node may provide sensor node level services (e.g. identification service, locating service and data acquisition service) and a sensor network may provide more comprehensive services (e.g. air pollution monitoring, tracking and tracing of containers, and temperature monitoring for fresh goods).

7.14 Routing in sensor networks

Energy-efficient routing schemes are highly desirable in resource-constrained, ad hoc sensor networks.

Some sensor network applications and services require large-scale network deployment. To support scalability in such networks, use of scalable routing schemes is required.

Bibliography

[1] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

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

[3] ITU-T Y.2221, *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment*

ICS 35.110
Price based on 8 pages