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

Document Number:	N008
Date:	2010-02-01
Replace:	N004
Document Type:	Working Draft Text
Document Title:	ISO/IEC 29182 Information technology — Sensor Networks — Reference architecture for sensor network applications and services
Document Source:	Project Editor
Document Status:	To be considered at the 1st JTC 1/WG 7 meeting (8-12 March 2010, London, UK).
Action ID:	FYI
Due Date:	
No. of Pages:	24

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)

Reference number of working document: **ISO/IEC JTC 1/WG 7 N 008**

Date: 2010-02-01

Reference number of document: **ISO/IEC 29182**

Committee identification: ISO/IEC JTC 1/WG 7

Secretariat: KATS

Information technology — Sensor Networks — Reference architecture for sensor network applications and services

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.

Technical Committee ISO/IEC JTC 1, Working group 7, *Sensor Networks,* prepared ISO/IEC 29182

Introduction

There have been a number of sensor network applications so far, such as burglar alarming, fire alarming, structural health monitoring, meteorological information gathering, etc. But sensor network applications are being evolved by new technical achievements such as wireless sensor networking, context-based processing, sensor networking solutions standardized globally, open service environment, nationwide integration of various sensor network applications, etc., which means that sensor network applications and services have to be involved with a variety of sophisticated functionalities. A reference architecture model for sensor network applications and services can give an overall understanding of various architecture instances of lots of sensor network applications/services and relationship among relevant functionalities.

Information technology — Sensor Networks — Reference architecture for sensor network applications and services

1 Scope

This International Standard specifies the reference architecture for sensor network applications and service and covers the following in network and transport layer:

- Requirements analysis of sensor network applications and services
- Identification of the network functionalities required by different sensor network applications
- Reference architecture for sensor networks functionalities supporting various sensor network applications and services
- Specification of interfaces for sensor network functionalities supporting 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 JTC1 SGSN N149, *SGSN Technical Document Version 3*

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 following terms and definitions apply.

[Contributor's Note] This clause was re-organized as alphabetical order of terms. Also, additional terms and definitions are included from SGSN-N149-Technical Document Ver.3.

3.1

actuator
A device that performs a physical response caused by an input signal

3.2

sensor
A device that observes phenomenon/phenomena, measures physical property and quantity of the observation, and converts the measurement into a signal.

Note:

- Signal can be electrical, chemical, or other types of sensor responses.
- Signal can be represented by 1-D, 2-D, 3-D, or higher dimensional data.

3.3

sensor network
A system of spatially distributed sensor nodes interacting with each other and, depending on applications, interacting with other infrastructure in order to acquire, process, transfer, and provide information extracted from the physical world.

3.4

sensor network applications
The sensor network application is a use case of sensor networks supporting a set of sensor network services for users.

Note: The services are, for example, home utility monitoring and control, industrial automation, infrastructure and environment monitoring, weather and disaster condition monitoring and emergency alert.

Note: Sensor network application implies the utilization of software and hardware that can be performed in a fully or partially automatic way and can be accessed locally or remotely.

3.5

sensor network device
The sensor network device is sensor node or sensor network gateway.

3.6

sensor network gateway
The sensor network gateway represents the bridge between the sensor network itself and the backend system.

3.7

sensor network services
A structure set of capabilities offered by the sensor nodes or sensor networks to support sensor network applications.

3.8

sensor network service management
Sensor network service situation management and execution control process, supporting flexible execution between multi-services/multi-contents in the multi-domain environment

3.9

sensor node
A device that consists of at least one sensor and zero or more actuators, and processing and networking capabilities using wired or wireless means.

4 Requirements of sensor network applications and services

Sensor network applications and services have specific characteristics with different service requirements and functional requirements from each other. However characteristics of sensor network applications and services can be distinguished into basic service model and advanced service model from the way of application model, operation process, operation domain and type of user.

4.1 Classification of service model

4.1.1 Basic service model

A basic service model has following characteristics:

Table 1 — Features of basic service model

Features	Type	Description
Application model	Pre-defined	Sensor networks are installed for specific and static purposes such as structures monitoring, street light control, agriculture monitoring and management, surveillance, facilities management, etc.
Operation process	Straightforward	Straight forward process progresses into sensing, transmitting, processing and provisioning. Sensor nodes and resulting sensor networks detect physical status; they transmit sensor data to backend application systems; the application systems collect sensor data and perform data processing functions; and the application systems produce value-added information contents and services.
Operation domain	Single	Sensor data are captured, transmitted, processed and delivered within a single operation domain.
Type of user	Dedicated	Value-added data are provided to dedicated users: owner and partners.

4.1.2 Advanced service model

An advances service model can be considered as a service infrastructure and has following characteristics:

Table 2 — Features of advanced service model

Features	Type	Description
Application model	Dynamic	Services depend on the usage of users who anybody can be. It is very difficult to fix application features and relevant functions statically in advance. For weather information services as an example: – Fishermen may request on-demand and periodic weather information for fishing; – Tourists may request periodic and alarming information of the nature condition for a week, a few days, or a month by a service subscription; – National disaster center may request the whole weather information to observe the natural phenomena of an area and detect emergency situations; etc.

Operation process	Elaborated	Transmitting, processing and provisioning step have additional functions as follows: – Various sensor networks may be integrated and sensor data may be acquired via other sensor networks by business contracts; – Due to dynamic service models, a variety of application functions have to be involved such as filtering, analyzing, context processing, data mining, decision making, forecasting, integration, exporting, etc.; and – Since anybody can be information user and information contents cannot be pre-defined, sensor data may be delivered in different forms such as text, audio, voice, image, etc. according to information users.
Operation domain	Multiple	Multiple business domains are incorporated by business partnerships.
Type of user	Dedicated and arbitrary	Services are provided to consumers as well as business partners: – Pre-defined users by contracts or agreements result in B2B-type sensor network services; and – Consumers by service subscription result in B2C-type sensor network services.

[Contributor's Note] Clause 4.2 comes from SGSN-N149-Technical Document Ver.3.

4.2 Characteristics of sensor networks

Many differences can be found between the emerging wired/wirelessly networked sensors and traditional wired/wireless networks such as communications network. Compared with the traditional networks, not only do sensor networks perform data transmission but also perform data processing, data aggregation, data management, networking management, resource management, automation (sense and actuate), and many other functions and services. The 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. Therefore, although there are some common characteristics, sensor networks have many unique characteristics that the traditional communication networks do not.

4.2.1 Dynamicity of service

The existing legacy sensor networks (or sensors-on-the-network) have been installed for specific application purposes such as structures monitoring, street light control, agriculture monitoring and management, military surveillance, city facilities management, home utility control, and flood and fire monitoring where consumer service models are not considered. As an information service infrastructure to improve the quality of life, the sensor networks should incorporate various service technologies such as sensor data gathering from various data sources, for example, sensor nodes themselves, other service providers, and private enterprises with functions including data filtering, data mining, context-aware decision making, estimation and forecasting, and so on. Moreover, the type of services provided depends on users' service requirements and expectations; therefore, it is very challenging to pre-determine the application/service features and relevant functions for a wide variety of users. To satisfy the different levels of services for the different users, a certain sensor data may be dynamically processed to meet individual user's requests. 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.

4.2.2 Application inter-working

There are many kinds of legacy sensor network applications such as industrial automation, various types of monitoring and control applications, civil engineering, intelligent building, home automation. And these applications usually operate in a mutually exclusive manner. Technologically evolving capabilities and application of sensor networks enables business partnerships whose business areas have been mutually exclusive, e.g., auto industry and private safety/emergency monitoring services industry. Thus, for certain business cases, the sensor network capabilities and functions should be developed benefiting multiple business partnerships. 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.

4.2.3 Types of user

The existing legacy sensor network applications typically have a dedicated group of users. But the emerging intelligent sensor networks and their applications/services aim at arbitrary 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 result in B2B-type sensor network services. Arbitrary consumers by service subscription result in B2C-type sensor network services.

4.2.4 Extension of Internet

Wired/wireless sensor networks have to be regarded as an extension of Internet towards the physical world ("Internet of Things") connecting 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 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.

4.2.5 Data gathering and pre-processing

The main objective of a sensor network implementation is to gather and pre-process sensor data. Therefore, intelligence on the sensor node is necessary. Sensor networks have to ensure that all the information is available and comprehensive for the tasks given. Communication/data links in the sensor network system have to be reliable and robust. If one of the links is terminated, the wired/wireless sensor network has to 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.

To bring intelligence to a sensor node, a level of comprehensive data processing (e.g., data compaction, signal/image processing, etc.) is required. The "a level" is determined by the sensor network's target application. To enable the intelligence in the node, the following needs should be considered:

- Sensor nodes in the network are automatically selected and organized to work collaboratively and perform certain tasks or functions after processing their own data collected from physical world;

- Users take action according to information provided by the sensor networks. Therefore, information provided to the users should be comprehensive and reliable;

- Nodes process data without the intervention of human decisions.

4.2.6 Association with location information

For many wired/wireless sensor network applications, sensor data are required to be associated with sensor's location information. Thus, a sensor network needs to offer a service to provide the sensor location information by a type of localization process, e.g., triangulation, data routing latencies, etc. 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. Producing the location information of a sensor is one of the most important services provided by a sensor network. The location information is then associated with the sensor data. The localization processing in the sensor network should be scalable because the networks may become very large and complex.

4.2.7 Collaboration of work

In many sensor network applications, the sensor nodes have to collaboratively work 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. Depending on applications, intermediary data/information, such as features or estimated parameters, need to be extracted from raw sensor data during the pre-processing. The results from this pre-processing should 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. For data sharing in the network, the bandwidth must be considered. In many applications, the sensor data processing may require a transmission of large amount of data over the network; while other applications may only require transmitting a few bits and bytes. Thus, sensor network standards should be sufficiently flexible and scalable to facilitate collaboration information processing (CIP) and data/information transmission in order to support various sensor network applications.

4.2.8 Non existing communication infrastructure-based communication

Sensor nodes must communicate with each other without an existing communication infrastructure. For this reason, a multi-hop capability and clustering algorithms will 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 certain applications, 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 should carefully select data routing schemes and communication protocols that support both types of applications. The design must also consider the cost-effectiveness in developing and operating such a sensor network.

4.2.8 Efficiency of power

One of the most important characteristics of a wireless sensor network is the fact that sensor nodes are energy-limited as they typically run on batteries; therefore, computing has to consider the resource-limited nature of the sensor nodes. The more frequent the sensor nodes become active to transmit data, the shorter life the sensor node has. It is said that "every bit processed or transmitted is one bit closer to the dead battery[1]."

For example, in the theft prevention system, its batteries need to be quite large in order to operate sensor nodes and networks for two or three months. In other applications, sophisticated energy management algorithms are needed to keep 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

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

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.

4.2.9 Dynamic topology of network

The topology of the wireless sensor network is rarely fixed. Normally, it has to adapt to the availability of data/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. Applications where nodes move within the network are more difficult to manage. The routing and communication protocols have to be very fast and flexible, yet energy efficient. This flexibility in the sensor network topology should not affect networks' performance when sensor nodes enter or leave the network, e.g., the self-healing and self-organizing nature of sensor networks.

4.2.10 Long operation time

A wireless sensor network has to 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 are restricted to remote maintenance and resolution operations. Thus, the sensor networks are desired to have basic functions such as self-maintenance, self-organization, redundancy and failure tolerance. These functions are, in fact, based on the key concepts of sensor networks. Without these embedded key functions, a sensor network-based product will have a very difficult time to find its market in the real world.

4.2.11 Human-user oriented application

Functions and services provided by sensor networks are quite diverse in many applications and in various market segments. This diversity requires developing an application profile to define an application's requirements and operation concepts for each sensor network application. In developing the application profile, the developer must focus on the end-user of the system, typically the human users. The ultimate goal of sensor networks is "to improve quality of life and change the life style."

For example, the application profile for a subway station security monitoring network should 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.

4.3 Analysis of service requirements

The following are service requirements for sensor network applications and services. These requirements are used to define functional requirements of sensor network reference architecture.

4.3.1 Connectivity

There are many types of sensor networks, such as IP-based, non IP-based, wired or wireless sensor networks. In IP-based sensor networks, every sensor node is capable for IP networking. Although the underlying wired or wireless media access control is tightly managing the connectivity of sensor nodes, connection between end user and a sensor network is through IP. In this sensor network type, it may happen that a single sensor node may directly connect to the backend network without a gateway, although normal scenario would use gateway to interconnect sensor networks and access networks.

In non IP based sensor networks, sensor nodes do not have IP address, and the connection between end user and a sensor node is through sensor network gateways. The gateways interconnect sensor networks and access networks.

Therefore it is required to support connectivity between sensor networks and the backend network, regardless of sensor network type, i.e. IP based or non-IP based, wired or wireless sensor networks.

4.3.2 Sensor network management

IP based sensor networks and non-IP based sensor networks, and wired and wireless sensor networks can co-exist. Application level gateways or overlay IP networks can be used for the connectivity between sensor networks and the backend network, and the diverse types of sensor networks need to be managed.

4.3.3 Service registration and discovery

In order to discover the sensor network services, they should be registered beforehand. The association of senor network and sensor data should be registered to service registry. The registered services are needed to be discovered by applications or end-users.

4.3.4 Mobility support

The challenge of achieving mobility in sensor applications and services depends on the technologies used in the sensor networking. Existing IP mobility technologies can be adapted for IP-based sensor networks.

An example sensor network application scenario illustrating mobility requirements can be found in the healthcare application. For instance, a patient's medical check-up data may be monitored via a sensor network: several sensors may be attached to the patient, resulting in a body area sensor network. The sensors periodically gather the medical check-up data and send them to his/her doctor via a home-gateway when he/she is at home; while moving, the data can be sent via an access gateway in a network-enabled car, bus, train, or subway. Various cases of mobility may occur in such an application scenario.

4.3.5 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.

4.3.6 Security and privacy

In general, sensor network services 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.

[Contributor's Note] Clauses from 4.3.11 to 4.3.15 come from SGSN-N149-Technical Document Ver.3.

4.3.11 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.

4.3.12 Scalability

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

4.3.13 Heterogeneity

Heterogeneous sensor networks supporting an application or applications shall have interoperability among the sensor networks.

4.3.14 Deployment and coverage

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

4.3.15 Power and energy management

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

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

5 Overview of the reference architecture of sensor network

[Contributor's Note] Text of this clause comes from SGSN-N149-Technical Document Ver.3.

Sensor network reference architecture, describing generic and generalized sensor network services, is an architectural representation of sensor network entities' (e.g., sensor nodes, gateway nodes, and other hardware in the node) functions, activities, and roles through operation layer and interoperable interfaces to provide the sensor network developers and implementers with reusable sensor network architecture for their target applications.

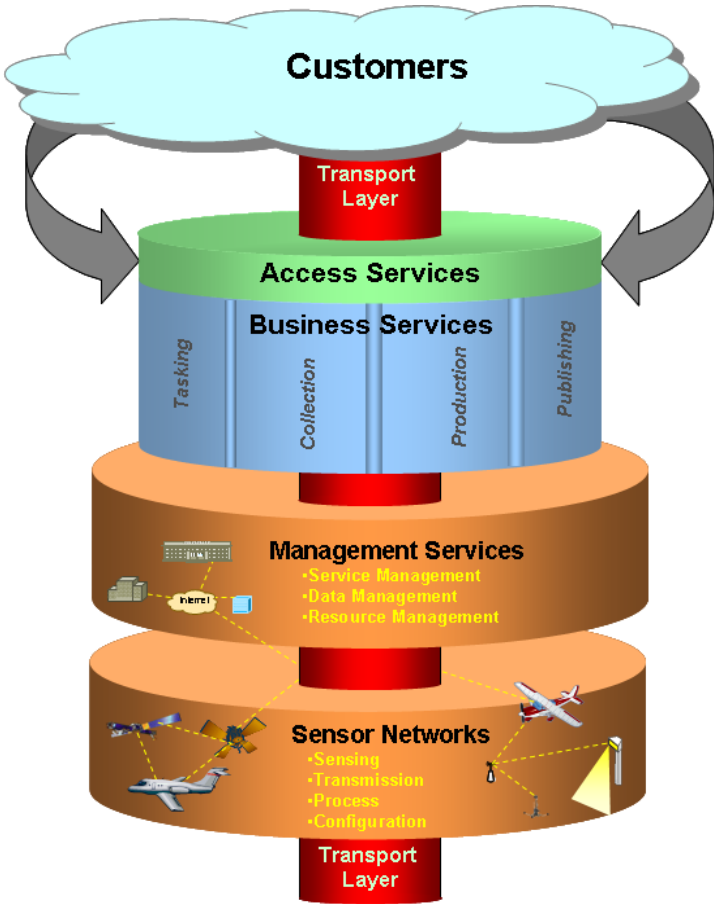

Figure 1 – Sensor networks high level operational graphic

Figure 1 shows the high level graphic that depicts the customer as the top layer of any sensor network. The sensor networks exist to serve the consumer or customer.

To be able to access the sensor network in a service-oriented application, the access services handles all of the system access for both man and machine. This service is the gateway from the outside world into the sensor network. It could be open or restricted.

Business services explain the processes that the sensor network employs to provide the services requested. Business services could have tasking service, collection service, production service, and publishing service as shown in Figure 1. Based upon the tasking and the sensor type, the data must be collected and stored in a repository for system use. This collected data could be raw data from the sensors or pre-processed data, or even predefined processing could take place at the sensor and stored in the repository. The production service is the area where fusion, exploitation, and end-to-end processing take place. In a service oriented application, publish as subscribe is a request and delivery method that allows the consumer the ability to monitor information on specific areas of interest.

Management Services are where security, storage, data management, etc. allow the service-oriented application to provide the services for the enterprise.

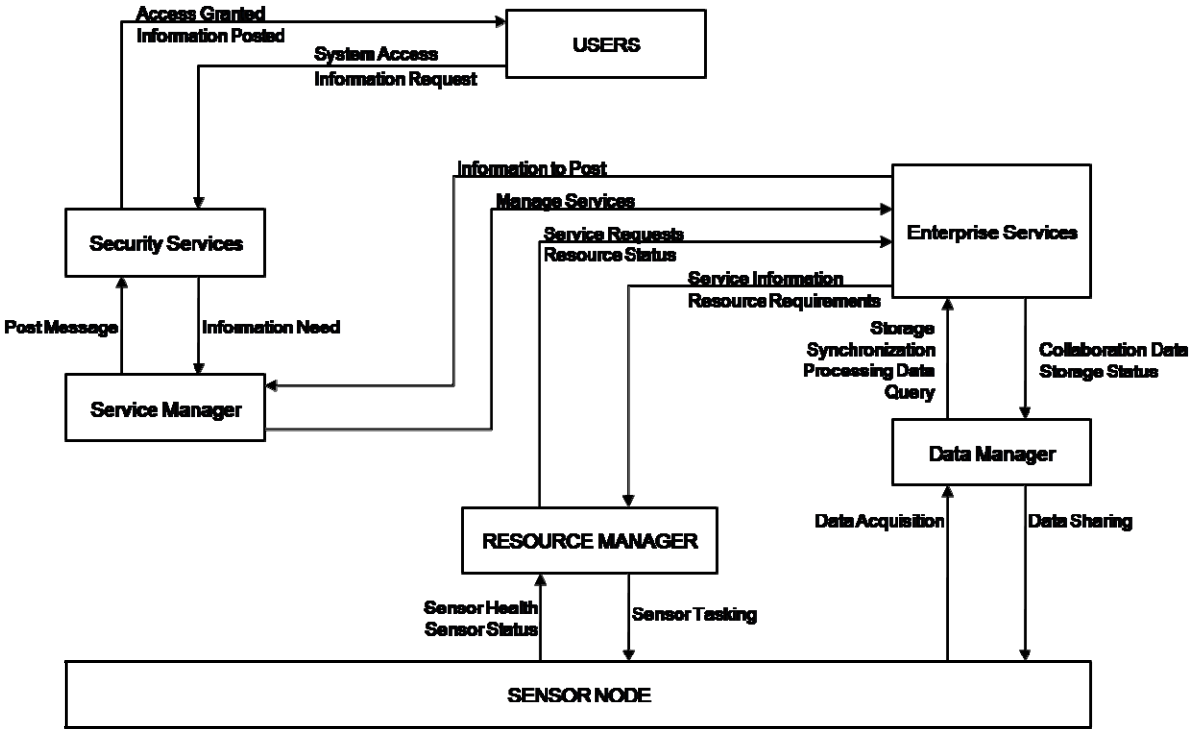

Figure 2 – Sensor networks entity/node connectivity diagram (an initiation)

Figure 2 shows the entities that are depicted in “Management Services” layer in Figure 1,the high-level operational graphic, illustrating the entity (or node) connectivity. Thus, Figure 2 is called an entity or node connectivity diagram. This figure is an example on an instantiation, and this does not represent or intend to be comprehensive, encompassing all sensor network applications. The purpose of this type of architecture diagram is to show the need of information exchange among the entities in sensor network system.

These types of architectural artefacts or diagrams show: who needs to exchange information, whom to exchange, and what information needs to be exchanged. Each of the need-lines (lines that show information need) carries multiple information exchanges. Each line carries all of the information exchanges between the entities in the diagram. For example, the Enterprise Service node has a need to exchange “Information to

Post" to the Service Manager. Contained in this need-line could be status on a request, or sensor status. It could contain a message with the location of the data requested by a user, or it could push data to a user depending on the request. After all this type of diagrams supports the function, activity, and role of the entities described in the high-level graphic (Figure 1) and their need to exchange information.

6 Generalized sensor network functional architecture

This clause explains the generalized functional architecture for the sensor network and defines the generalized functions. This architecture can be applied to general applications and services of sensor network. Also this architecture is technology-independent, therefore this architecture can be customized to respond to specific contexts in terms of the applications and services offered and the technologies used.

[Contributor's Note] Newly added text comes from SGSN-N149-Technical Document Ver.3.

Figure 3 focuses on the application layer and the sub-layers that are created to service multiple applications, e.g., theft protection, temperature monitoring, and sensor data processing, as shown in the figure.

This application layer interacts with software applications that implement data/information communications. These application programs fall outside the scope of the OSI stack. Application layer functions most often include identifying communication partners, resource availability and management, and synchronizing communication. The sensor network and sensor management will interface with this layer of the OSI stack. This figure also shows the control hierarchy with numbers where "1" being the top level in the hierarchy. It also lists some management entities in service layer, e.g., communication management, data management, security management, and group management. Basic function layer lists its entities such as network communication, sensor driver, and clock. With these layers, the sensor node function sub-layers are connected with control/collaboration sub-layer through application layer and service layer. Thus, this type of architectural diagram shows the sensor network architecture from a view of involved layers and their functions, activities, and roles.

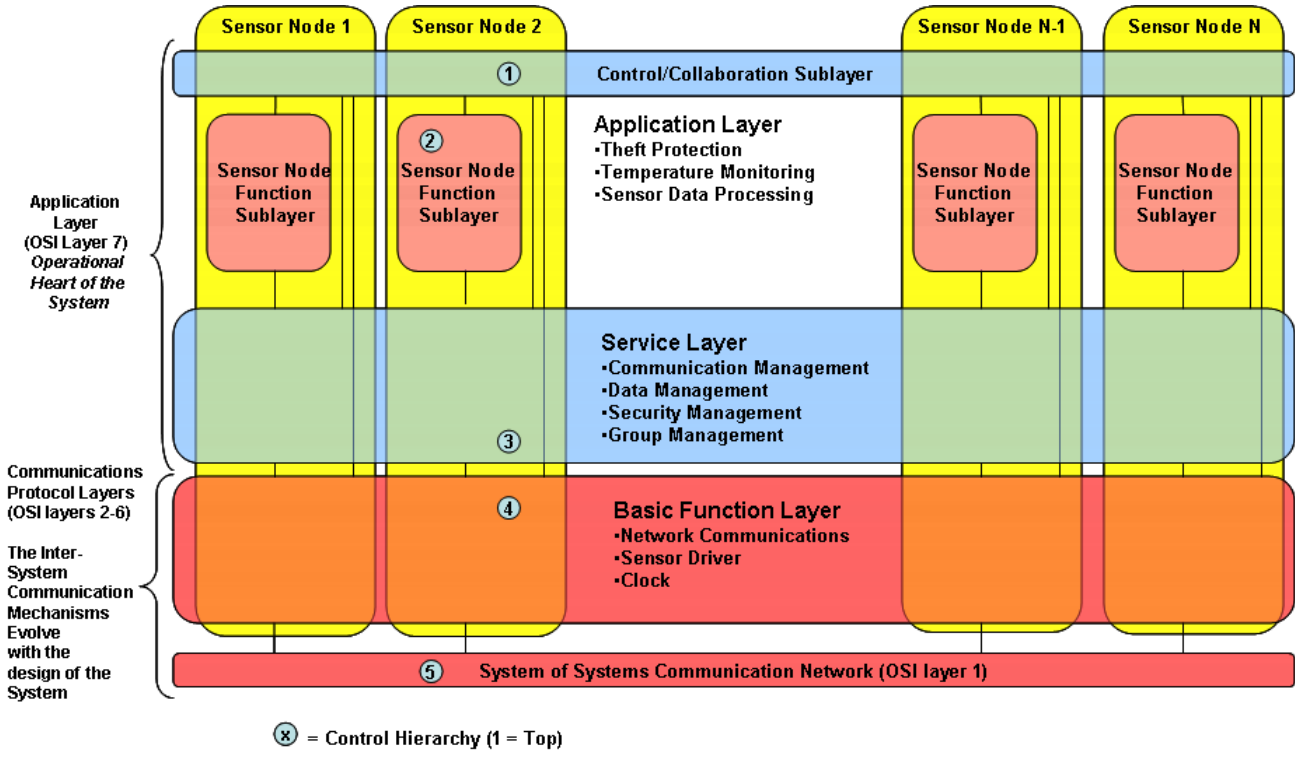

Figure 3 – Sensor networks systems architecture (layer focused)

Figure 4 describes service and functional connectivity between the sensor network application layer and communication network layer. The figure shows all involved layers and sub-layers, their purpose and what each layer's part is in the sensor network communication process. This figure is limited to the networking between sensors. The external nodes would also reside above the control/collaboration sub-layer. Thus, this figure is a different view of the sensor network system architecture focusing on the layers compared to Figure 3.

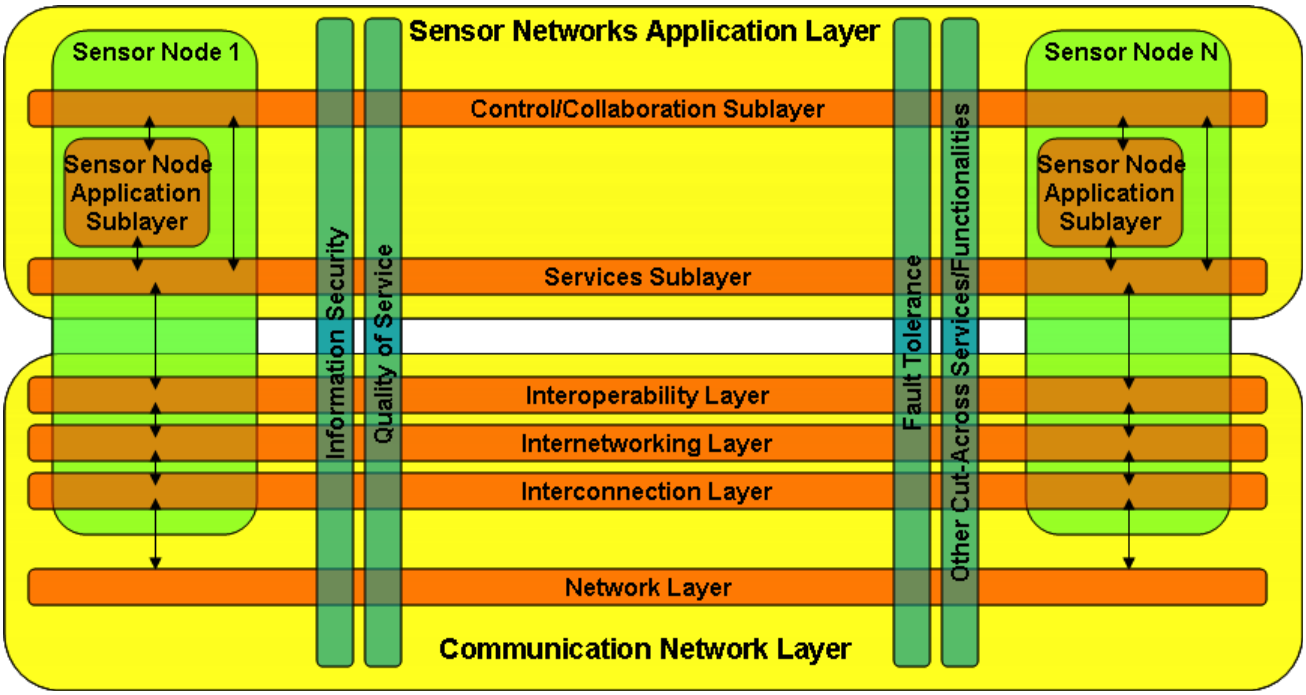

Figure 4 – Service/functionalities cut-across sensor network layers

6.1 Sensor network device architecture

In this section, a sensor network device – sensor node and sensor network gateway – is described in detail from the node layer and their functional entities point of view. Thus, this is one of the architectural views of the sensor network device.

From the layer architectural views, the sensor network device consists of:

- Three layers
  - Application layer
    Application layer has the target application module(s) for the sensor node as shown in the figure, e.g., theft protection, temperature monitoring, sensor data processing. Depending on applications, the modules in the application layer can be complex.
  - Service layer
    Service layer has the services that are provided to the sensor network device itself as well as to the external entities. These services are provided by communication management, group management, data management, security management, localization service, etc.
  - Basic functions layer
    Basic functions layer has the interfaces to physical connectivity such as network, driver, clock, and other hardware (e.g., sensors and actuators) that support the sensor node functionality.

- A device management entity
  The device management entity provides the functional services such as program management, identification, and node resource management, and other functions.

These layers and entity along with the function blocks in each layer and management entity are illustrated in Figure 5. In the following sections, we discuss each of the layers in Figure 5 in detail.

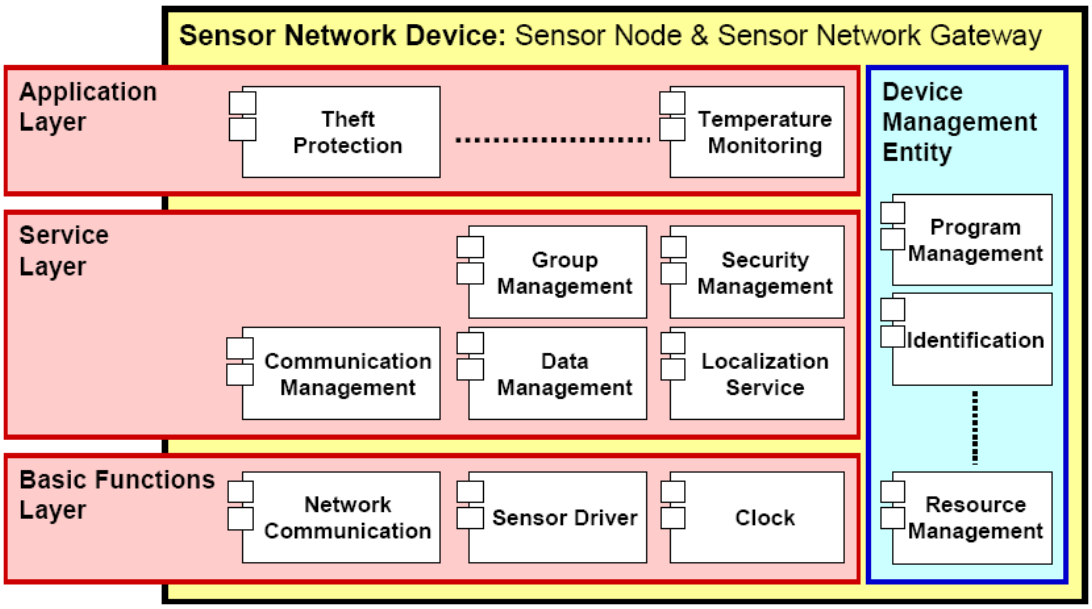

Figure 5 – Operation layer view of sensor node device

6.2 Generalized functions

6.2.1 Basic functions layer

Basic functions layer consists of components which address the physical world. The components are communication protocol stacks and drivers for interfaces, sensors, actuators, etc. The components of basic functions layer offer standardized interfaces to the other layers and the device management entity. Table 1 shows basic functional areas for basic functions layer and corresponding components per each functional area.

Table 1 – Basic functions layer components

Functional Areas	Components
Sensor interface	• Interface to physical networks • Interface to sensor buses • Interface to sensor data
Actuator interface	• Interface to physical networks • Interface to control actuators
Network communication	• Protocol stacks (comprising PHY, MAC, DLL, NWK) • Stateless or state auto-configuration • Mesh network establishment and management • Network topology management • Routing protocol

	• Topology management • Routing table management • Network information reconfiguration • Reliable data transmission • Unreliable data transmission
Clock	• Real time clock

6.2.2 Service layer

Service layer consists of components which offer generic services and management to support applications. The services may use interfaces of basic functions layer components and can interact with other services. Table 2 shows basic functional areas for service layer and corresponding components per each functional area.

Table 2 – Service layer components

Functional Areas	Components
Mobility management	• Intra-area (e.g., WPAN) mobility function • Inter-area mobility function • Network mobility function • Service mobility function
Group management	• Establishment of groups • Group communication
Service management	• Service registration • Service discovery • Service description • Service analysis • Service processing queue • Management of object identification
Network management	• Topology management • Routing table management • Network information reconfiguration • Performance management • Configuration management • Time synchronization
Security management	• Authentication • Authorization • Encryption • Privacy protection • Key management • Security routing mechanism
Data management	• Data acquisition • Data compression • Data storage • Data sharing • Data synchronization

	• Data directory • Data aggregation or fusion • Capability declaration entity (CDE), • Collaborative strategy planning entity (CSPE) • Communication requirement specification entity (CRSE)
Localization service	• Localization algorithms • Location table • Area Management • Neighborhood table
Event management	• Event generation • Event filtering
QoS management	• Admission control
Protocol conversion	• Address conversion • Protocol conversion

6.2.3 Application Layer

The sensor network applications are specific for each market segment and the needs of the users in that market. The applications may use standardized interfaces of components of service layer, basic functions layer and device management entity.

6.2.4 Device management entity

Device management entity manages the device resources. Table 3 shows basic functional areas of the device management entity and corresponding components per each functional area.

Table 3 – Device management entity components

Functional Areas	Components
System management	• Power control • Start-up and shutdown • System parameter reconfiguration
Identification	• Sensor node identification
Program management	• Migrating and updating of programs or components
Resource management	• Managing the node resources (e.g., memory, processing ability) • Energy Management

6.3 Service access points (SAP)

Within the sensor network device each component offers its services via a service access point to other software modules. This is illustrated by the yellow arrowed in Figure 6.

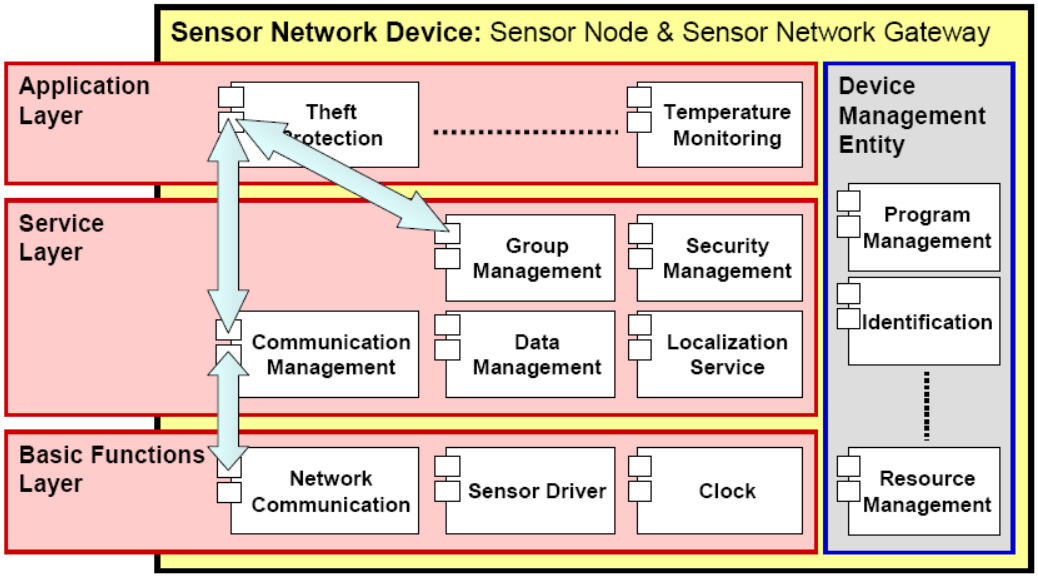

Figure 6 – An example of component interconnections via service access points

Bibliography