INTERNATIONAL STANDARD

ISO/IEC 29182-3

First edition
2014-02-15

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

Part 3:
Reference architecture views

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

Partie 3: Vues de l'architecture de référence

Reference number
ISO/IEC 29182-3:2014(E)

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 29182-3 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 6: Applications*

— *Part 7: Interoperability guidelines*

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 of International Standards (ISs) is to

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

— improve interoperability of sensor networks, and

— make sensor network components 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, system integrators, and service providers to meet customer requirements, including any applicable interoperability requirements.

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

ISO/IEC 29182-1 provides a general overview and the requirements for the sensor network reference architecture.

ISO/IEC 29182-2 provides definitions for the terminology and vocabulary used in the reference architecture.

ISO/IEC 29182-3 presents the reference architecture from various viewpoints, such as business, operational, system, technical, functional, and logical views.

This part of ISO/IEC 29182 categorizes the entities comprising the reference architecture into two classes of physical and functional entities and presents models for the entities.

ISO/IEC 29182-5 provides detailed information on the interfaces among various entities in the reference architecture.

ISO/IEC 29182-6 provides detailed information on the development of International Standardized Profiles.

ISO/IEC 29182-7 provides design principles for the reference architecture that take the interoperability requirements into account.

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

Part 3: Reference architecture views

1 Scope

This International Standard (IS) provides Sensor Network Reference Architecture (SNRA) views. The architecture views include business, operational, systems, and technical perspectives, and these views are presented in functional, logical, and/or physical views where applicable. This IS focuses on high-level architecture views which can be further developed by system developers and implementers for specific applications and services.

2 Normative references

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

ISO/IEC 29182-1, *Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 1: General overview and requirements*

ISO/IEC 29182-2, *Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 2: Vocabulary and terminology*

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

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

3 Terms and definitions

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

4 Abbreviated terms

1D	One-dimensional
2D	Two-dimensional
3D	Three-dimensional
AL	Application Layer
BFL	Basic Function Layer
CIP	Collaborative Information Processing
CLM	Cross Layer Management

CPU	Computer Processing Unit
GHL	Gateway Hardware Layer
GPS	Global Positioning System
NOAA	National Oceanic and Atmospheric Administration
IS	International Standard
OGC	Open Geospatial Consortium
OS	Operating System
PV	Physical View
RA	Reference Architecture
SL	Service Layer
SNHL	Sensor Node Hardware Layer
SNRA	Sensor Network Reference Architecture
SOA	Service-Oriented Architecture
SV	System View
TS	Technical Standards
TV	Technical View

5 Purpose of Sensor Network Reference Architecture

This International Standard provides reference architecture views consistent with the requirements which are defined in ISO/IEC 29182-1 (General overview and requirements) and can be utilized more effectively with other Parts, especially with ISO/IEC 29182-4 (Entity Models) and ISO/IEC 29182-5 (Interface Definitions).

A Reference Architecture (RA) is a *generalized* architecture of several end systems that share one or more common domains, giving direction downward and requiring compliance upward. Therefore, an architecture for a certain application will contain some, most, or all of the reference architecture. In other words, the developer can reuse entities and elements in the reference architecture that fit his or her application architecture and ignore the rest of entities and elements in the reference architecture. In addition, the RA provides standards and policies for building a specific architecture.

RAs provide a *consistent point of departure* for implementing solutions so that each implementation:

a) Follows a consistent decomposition and design pattern;

b) Reduces cost by exploiting opportunities for reuse of services, products, data definitions, etc.;

c) Reduces schedule by starting with a core architecture to be tailored for implementation; and

d) Reduces risk by:

— Incorporating required global capabilities; and

— Taking advantaged of lessons learned and related expertise.

The Sensor Network Reference Architecture (SNRA) outlines “what” the overall structured approach is for facilitating interoperability and the SNRA, from the details of this structure, indicates “how” the architecture and its entities will operate through the development of interface standards. In short, the SNRA provides rules and guidance for developing and presenting architecture descriptions.

This standard provides not only multiple perspectives of SNRA (e.g. business, information, and technical) but also multiple views of the technical architecture (e.g. physical, system, operational, etc.) describing a sensor network (e.g. business, information, application, and data). The combination of these architecture perspectives and views forms a comprehensive architectural description of the sensor network system. The reference architecture perspectives and views are to:

a) Show how Sensor Networks operate in a homogeneous or a heterogeneous system;

b) Show the systems of equipment and the flows of information that support the sensor networks; and

c) Show the technical rules and guidelines that allow these systems to interoperate.

Typically, a developer begins depicting an architecture with desires and needs for the data/information that could be provided by a sensor network or sensor networks and that could meet the desires and needs (e.g. then translated into a set of requirements). Additionally, the developer needs to have an understanding of the technology available and also the roadmap of technologies to come. For example, the desires and needs could be a computer and a set of sensor nodes (thus, a sensor network) in a car to monitor and control subsystems, or alternatively they could be a large system of systems, such as the sensor networks by National Oceanic and Atmospheric Administration (NOAA) to monitor worldwide weather in order to predict weather patterns and to provide warnings if necessary. Each developer will have specific requirements concerning the capabilities that a sensor node or sensor network should have for target applications and services. The developer also needs to make many decisions in developing a sensor network architecture including whether a sensor network will perform data processing to provide high level information to a user, or a sensor network will make the raw data available to a user who will use its own applications to process the raw data. The Sensor Network Reference Architecture (SNRA) can provide the developer with various options and understanding for the developments, and more importantly, SNRA provides the developer with the architecture starting point.

The SNRA supports the development of interoperating and interacting architectures. It defines the multiple perspectives of SNRA and the multiple views of the technical architecture. Each view is composed of sets of architecture data elements that are depicted via graphic, tabular, or textual products. The SNRA also clearly defines the relationships between these architectural views and the data elements they contain.

6 Overview of Sensor Network Reference Architecture

Sensor network is a system of distributed sensor nodes communicating with each other and also interacting with other sensor networks that monitors environments external to the sensor network in order to acquire, process, transfer, and provide information extracted from a physical world.

This Sensor Network Reference Architecture (SNRA) consists of a set of domains which are concerned with gathering raw data from each domain's physical environment, processing raw data into information, and delivering information to a user or users. The user can be a human or a machine/software (e.g. automated command and control system). In cases where a sensor network has a sensor node or sensor nodes equipped with an actuator or actuators, information in the forms of a decision can flow from the user to the actuator(s) attached to the sensor node to provide an actuation command.

Each sensor network consists of various entities such as sensor nodes, actuators, a network, processing (at a local sensor node, a gateway, and/or fusion centre), applications used by the sensor nodes, applications used by the users[1)], and finally the user. Figure 1 shows a high level physical view of multiple sensor network domains although there are other domains not captured in the figure. Most sensor network domains are designed to be disparate as each sensor network focuses on its own specific application. This figure is to emphasize the importance of interoperability among dissimilar networks, sensors, and

1) [When the user is a person] Personal information belongs to individuals. It shall be implemented with any protection means when personal information is connected to networks. [Reference: NIST-IR7628, Smart Grid Cyber Security Vol.2 “Privacy and the Smart Grid”, and OECD: “Privacy Principles”]

disparate data contents and formats. Figure 1 also shows that sensing can occur in all geospatial expanses (e.g. space, air, maritime, ground, and subsurface (e.g. underground, and below ocean/lake/river surface)). In each geospatial expanse, there are many capabilities that sensor networks can provide as shown in the figure. In space, a sensor network formed by the sensor nodes in a constellation of satellites can provide data and information about Earth's weather, air pollution, oceanic current movements, and so on. In the air, air traffic control cannot be performed without sensor networks (e.g. radars). In maritime, ships rely on GPS for navigating the oceans. The sensor networks can also be effectively used for maritime container tracking, tagging of, and protection for the contents of the containers, On the ground, many different sensor networks are found as there exist many different applications, (e.g. intelligent highway, transportation, supply chain management, medical, military, industrial, finance, first responders, governmental, home, environmental monitoring, perimeter protection and intrusion prevention, health/situation monitoring of elderly or patients, and so on).

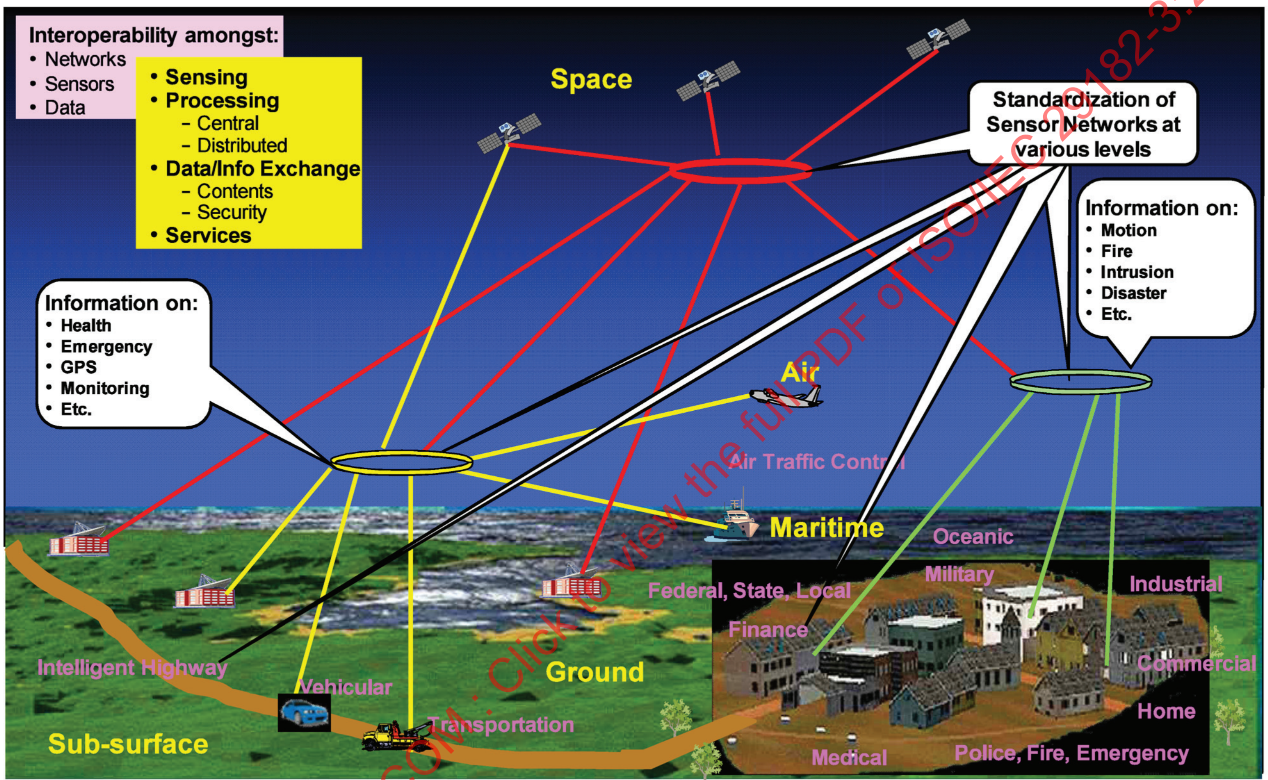

Figure 1 — High level physical graphic of sensor network domains

In summary Figure 1 shows that there are many dissimilar sensor networks in various geospatial expanses, and within each expanse, there are many disparate sensor network applications and services where the disparity exists in types of sensors in the sensor network, networks that support the sensor networks, and data formats utilized by the sensors and the communication networks.

Figure 1 also attempts to illustrate an interoperable sensor network reference architecture, consisting of multiple horizontally interoperable subsystems or modules and the interfaces between those subsystems and modules. Interoperability also needs to exist vertically to transmit the information seamlessly within the hierarchical structure of the sensor networks supporting a complex system of systems. Both horizontal and vertical interoperability can be achieved by a standard developing process that promotes open architecture and also by standardization of interfaces between subdivisions (both subsystems and sensor networks), layered structures in sensor networks and its applications. For the reference architecture to fulfil the requirements of interoperability, existing interoperability standards should be used to describe sensor network systems. Additionally, the needs for new standards, to satisfy new technologies, applications and services of sensor networks, can be identified from the sensor network reference architecture.

Figure 2 describes the sensor network reference architecture by identifying the main entities of sensor networks and the interfaces between the main entities which make up a sensor network. The detailed descriptions of the interfaces (e.g. Interface 1, Interface 2, ..., Interface 5) can be found in ISO/IEC 29182-5.

The main entities identified are:

a) Sensor Nodes, and a sensor node has:

— Sensor Node Hardware Layer (SNHL);

— Basic Functions Layer (BFL);

— Service Layer (SL);

— Application Layer (AL); and

— Cross Layer Management (CLM);

b) Gateway and a gateway is likely to have the same or similar layers and layer structure as those in the sensor node); thus, a gateway has:

— Gateway Hardware Layer (GHL);

— Basic Functions Layer (BFL);

— Service Layer (SL);

— Application Layer (AL); and

— Cross Layer Management (CLM);

c) External Environment through Access Network and Backbone Network connecting to service providers and users.

In Service Provider, it is likely to have the similar layer structure as the one in a gateway.

The interfaces between these main entities, identified in grey colour-filled boxes in Figure 2, are:

a) Within a sensor node, there are:

— Interface between Sensor Node Hardware Layer and Basic Functions Layer (SNHL / BFL);

— Interface between Basic Functions Layer and Service Layer (BFL / SL);

— Interface between Service Layer and Application Layer (SL / AL); and

— Interfaces between Cross Layer Management and Applications Layer, Service Layer, and Basic Functions Layer (CLM / AL-SL-BFL);

b) Interface between a Sensor Node to a Sensor Node within a Sensor Network; and

c) Interface between Sensor Network Gateway Node and other networks (ISO/IEC 29182-1, Figure 3 designates "Backbone Network and Access Network" as "Other Networks," which is also shown in Figure 9 of this standard).

The interfaces between Sensor Node Hardware Layer and Basic Functions Layer (SNHL / BFL) are realized by the functions reside in SNHL and those that reside in BFL.

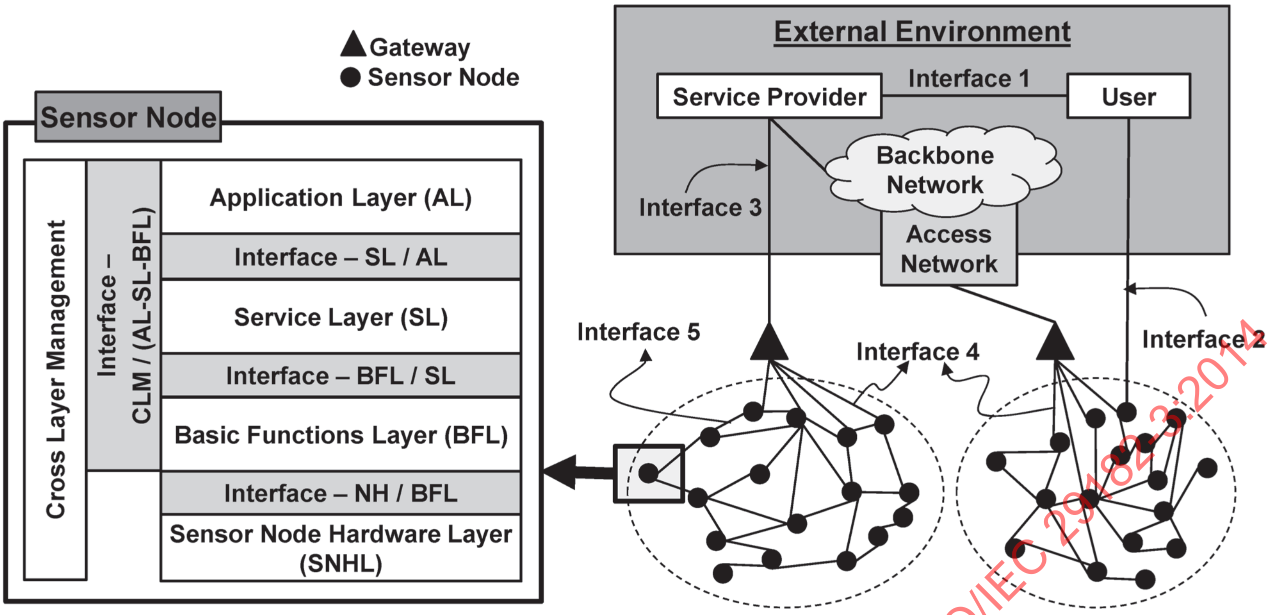

Figure 2 — Overview of sensor network interfaces in a sensor node, sensor node to sensor node, and sensor node to the External Environment

Figure 3 describes the physical architecture of a sensor node, which can be mapped to the Sensor Node Hardware depicted in Figure 2, sensor node physical reference architecture. The sensor node physical reference architecture includes:

— Computer processing unit (CPU): A CPU embedded in a sensor node enables the node become intelligent. It hosts an Operating System (OS), application algorithms, and other software. A CPU could be located outside of a sensor node and a sensor node transmits its measurements to the CPU for processing.

— Storage: A storage device is a memory unit which can be embedded in a sensor node or can be located outside of the node. The memory unit stores various event data experienced by the node, e.g. measurements, processed data if an on-the-node processing is performed, and other event data.

— Sensor: Sensor or sensing element is a measuring device of external environment of a certain phenomenology. Typically, this device converts raw measurements into a stream of measureable electrical signal. Depending on the type of a sensing device, the device can measure acoustics, seismic or vibration, magnetic, various light spectra (e.g. visual, infrared, etc.), electromagnetic (e.g. radio frequencies), temperature, gas, pressure, motion, contaminants, objects, etc. Depending on the complexity and technology implemented in the sensor, the sensor can measure 1-dimensional, 2-dimensional, and 3-dimensional signals along with time tagging.

— Communication unit: A communication unit is an essential component of a sensor node. This communication unit provides either wired or wireless data link which is used to transmit the data collected by the sensor or sensing element and any processed data if available in real-time or in non-real-time. For the case of non-real-time data transmission, a type of storage device is required.

— Actuator(s): An actuator may reside in a sensor node or outside of the sensor node. Actuators are means to interact with physical environments, e.g. automatic temperature control. Actuator(s) can receive information (e.g. command) directly from sensor after data processing through wired or wireless data link.

— Power supply: A sensor node will require a power supply. If a sensor node is physically connected via a wire, such sensor node typically does not require on-board power supply, e.g. batteries. In case of a wireless sensor node, a battery is required. Power management for a sensor node is a critical matter, and a power management utility firmware may be hosted in the CPU, especially for the sensor nodes remotely located wirelessly.

Power supply to power a sensor node is a critical element for sensor nodes and thus for an entire sensor network. This criticality becomes even greater for a wireless, geographically dispersed sensor network. The power supply is typically primary batteries (non-rechargeable); however, the idea of self-generating power sources leveraging natural phenomena (e.g. sun light (solar), vibration, wind, so-called energy harvesting methodologies) are under research and development.

The power supply will greatly depend on the type of sensor and sensor node functions. Power management on remote sensors is of great importance to the functionality of the sensor node. The remoteness of the sensor node will dictate the power supply capacity and power usage management. The required frequency of inter-nodal communications will also dictate how the power should be managed.

The interface lines inside of the sensor node shown in Figure 3 are not specified. This is because the implementation of a sensor node is highly dependent on application requirements and on its hardware constraints.

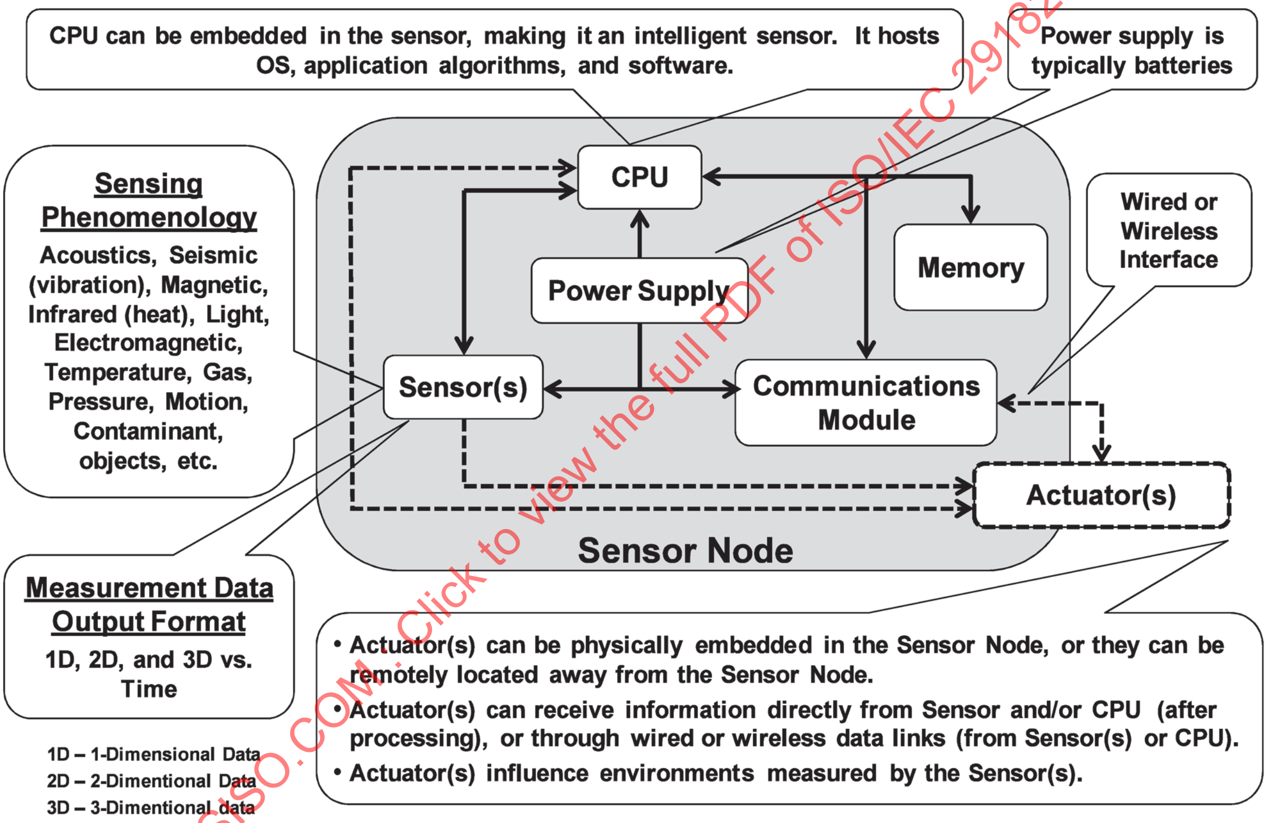

Figure 3 — Sensor node physical reference architecture

Figure 4 illustrates a set of functional entities that realizes various sensor network services, and it depicts the functional view of the sensor network reference architecture. This sensor network functional architecture lists many significant functions in a sensor network, but this figure does not include all functions. This functional architecture shows three domains, namely:

— Sensing Domain: This domain interfaces with sensors, gateways, and other entities (e.g. storage devices) in a sensor network or sensor networks. This domain receives data from the sensor network(s) and transmits to Service Domain via Network Domain per requests made by users. Additionally, Sensing Domain can have capabilities to process measurements (e.g. raw data) from sensors in the sensor network via local area network and/or wide area network.

— Network Domain: This domain provides data/information links between Sensing Domain and Service Domain.

— Service Domain: This domain hosts various applications that provide requested services by users. To perform the required applications, this domain can also support various data processing capabilities from data (e.g. measurements) and/or information (e.g. data from processing the measurements) from Sensing Domain via Network Domain.

And this figure also shows two groups, shown in the vertical rectangular box:

— Data, Information, and Communication Group: This group of functions is responsible for data processing, information generation, and communications of the data and information generated between the domains and to data/information requesters (e.g. users).

— Control and Management Group: This group of functions is responsible for managing entities within each domain. Sensing Domain and Service Domain have similar management functions; however, what these functions manage in each domain are different. For example, for Sensing Domain, the devices being managed by Device Management are typically sensor entities. For Service Domain, the devices being managed are typically computer assets. For Network Domain, the devices being managed by Device Management are communications devices.

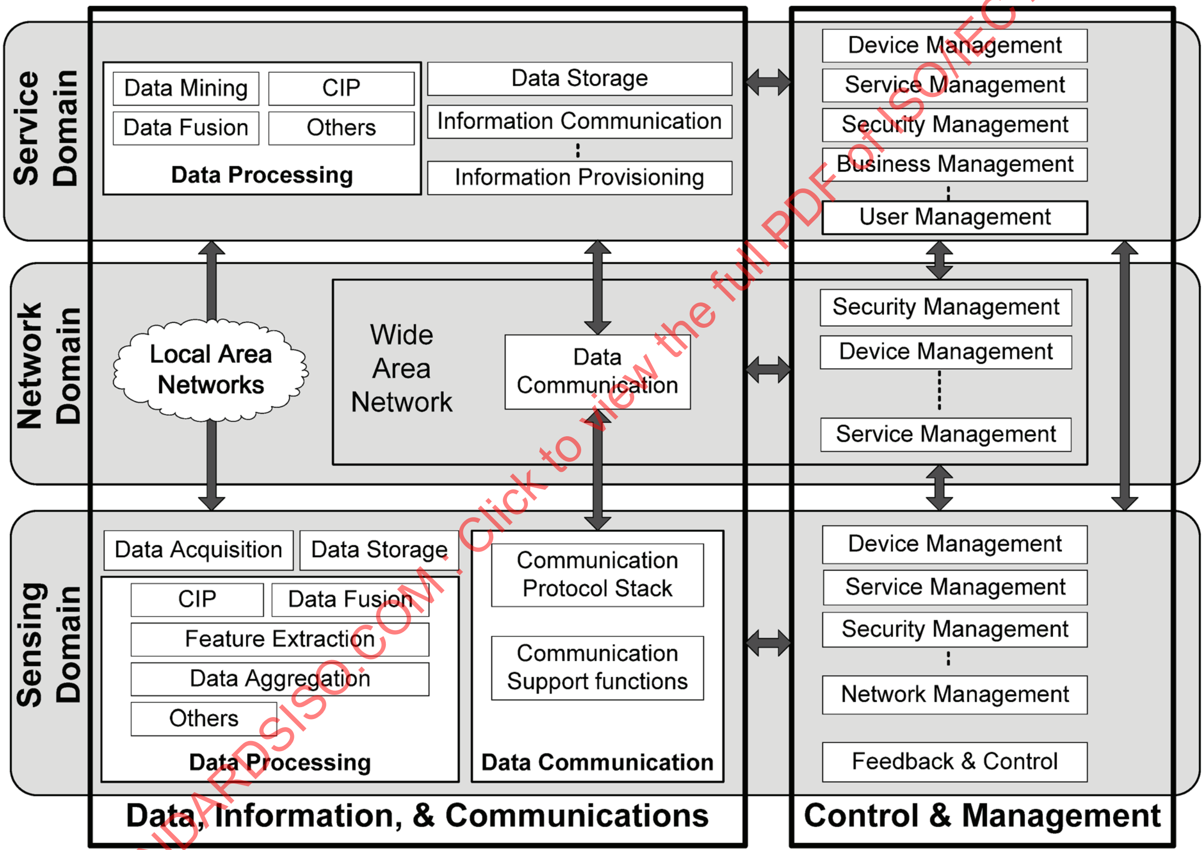

Figure 4 — Sensor Network Functional Architecture

In the sensor network functional architecture shown in Figure 4, Sensing Domain transports data/information to Service Domain through Local Area Networks or Wide Area Network. As shown in the figure, there are two main groups responsible for data and information generation: Data, Information, and Communications Group and Control and Management Group within Sensing Domain. Data, Information and Communication Group provides functions such as data acquisition, data storage, data processing (e.g. Collaborative processing, data aggregation, feature extraction, data fusion, etc.), data communication (e.g. communication protocol, communication support function, etc.). Control and Management provides functions such as sensing device management, service management, network management, security management. Once data/information is passed to Service Domain, the data/information is processed by the functions such as data mining, information extraction, data fusion and other relevant functions not shown in the figure. Additionally, the data/information can be stored, communicated, and provisioned in Service Domain.

Sensing Domain

Table 1 describes the functional entities in Sensing Domain depicted in Figure 4. Comprehensive description of the entities can be found in ISO/IEC 29182-4.

Table 1 — Function model and descriptions in Sensing Domain

Functional Entities	Descriptions
Data acquisition	Sense and capture data from the environment for applications.
Data storage	Store sensor data, control instructions, and management data.
Data processing	Use data/signal processing algorithms to extract requested or useful information from sensor data and metadata. The information extraction algorithms include collaborative information processing (e.g. data fusion, feature extraction, data aggregation and data presentation).
Data communication	Transmit and receive data among sensor nodes and sensor network gateway through a communication protocol stack and communication support functions. Examples of data transmitted and received are temperature, humidity, time synchronization and location data.
Device management	Manage devices in Sensing Domain, including power, system parameter, identification, and embedded software/firmware programs in the device.
Service management	Manage the service(s) provided by sensor nodes and sensor network gateways, including service registration, service discovery, service description, service analysis, and service processing queue.
Security and Privacy management	Manage the security of communication and data, including authentication, authorization, encryption, and key management. Manage the protection of personal information, including data minimization, anonymization, pseudonymization and so on. Privacy management typically begins with a privacy risk/impact assessment, including the identification of safeguards required to mitigate the identified risks.
Network management	Manage the network topology, routing table, configuration information, performance and reconfigure network information.
Application Management	Manages the parameter changes or application updates in sensor nodes or in a sensor network or sensor networks
Feedback & control	Trigger control instruction on actuators according to user's feedback depending on the application requirement. Whether feedback control is needed or not depends on the application requirement.
Feature extraction	There are different levels of feature[a] extraction. Feature extraction methods can vary depending on sensor type and the data the sensor generates. In general, features can be extracted from raw data from a sensor or from processed data. The feature extraction is performed typically by an algorithm or algorithms.
Data Aggregation	Data aggregation assembles the similar data from multiple sources (e.g. sensors, processors, databases). It also may assemble the data chronologically when needed.
Data Fusion	Data fusion is the use of techniques that combine data from multiple, disparate data/information sources and translates that information into discrete, actionable items through inferencing. Data fusion processes are often categorized as low, intermediate or high, depending on the processing stage at which fusion takes place. For example, low level fusion, data fusion algorithm/software combines several sources of raw data to produce new raw data. The fused data is likely provides more complete pictures of the physical world, especially for objects of interest in the physical world compared to individual data from the multiple sources that have not been fused.

Table 1 *(continued)*

Functional Entities	Descriptions
Collaborative Information Processing (CIP)	Collaborative information processing is similar to Data Fusion in many respects. The emphasis is given to network level data fusion where there are multiple networks involved. The fundamental ideas of combining data from multiple sources to produce actionable items are the same as Data Fusion.
Information Extraction	A type of information retrieval whose goal is to automatically extract structured information from unstructured and/or semi-structured data.
Data Mining	Data mining is a process of discovering new patterns from large data sets involving methods from statistics and artificial intelligence but also database management. In contrast to for example machine learning, the emphasis lies on the discovery of previously unknown patterns as opposed to generalizing *known* patterns to new data.
[a] In OpenGiS® Implementation Standard for Geographic Information – Simple feature access – Part 1: Common Architecture (Open Geospatial Consortium OGC 06-103r4, 28 May 2011), “feature” is defined as “abstraction of real world phenomena”; however, in this standard, feature is used in a general sense including such definition in the OGC document.	

Network Domain

In the Network Domain, only functions concerning sensor network are shown in the sensor network functional architecture. Table 2 describes the functional entities in the network activities domain in Figure 4. Network Domain can be realized by Local Area Network and/or by Wide Area Network. A Local Area Network can be used when Sensing Domain and Service Domain are within the same network while Wide Area Network can be used when Sensing Domain and Service Domain reside in different networks. There will also be cases where (1) one Sensing Domain serves multiple Service Domains; (2) multiple Sensing Domains serving one Service Domain; or (3) more than one Sensing Domain serve more than one Service Domain.

Table 2 — Function model and descriptions for Network Domain

Functional Entities	Descriptions
Data communication	Transmit and receive data among devices using existing or emerging data transmission technologies.
Device management	Manage information about the devices in a Wide Area Network, including power, system parameter, identification, and embedded software/firmware programs in the device.
Security management	Manage the security of transporting data, including access control, authentication, authorization, encryption, and key management.

Service Domain

In Service Domain, business management and user management entities are shown along with other entities. The use of these two management entities is dependent upon the requirements of the application(s) of the sensor network being designed and developed. Table 3 describes the functional entities in Service Domain depicted in Figure 4.

Table 3 — Function model and descriptions for Service Domain

Functional Entities	Descriptions
Data storage	Store data, including sensor data from Sensing Domain, and control instructions from user.
Data processing	Use data/signal processing algorithms to extract requested or useful information from sensor data and metadata. The information extraction algorithms include collaborative information processing or data fusion, feature extraction, and data aggregation, for example.
Information communication	Transmit and receive data among the devices in Service Domain using data transmission technology of legacy network.
Information provision	Provide useful information to users through user interface.
Device management	Manage information about application end devices, including the power, system parameter, identification, and programs of the device.
Service management	Manage the service provided by application service to the users, including service registration, service discovery, service description, service analysis, and service processing queue.
Security management	Manage the security of data and communication in service domain, including access control, authentication, authorization, encryption, and key management.
Business management	Manage the business procedure, business rules, business operations and statistical analysis of business data. Whether business management is necessary depends on application requirement.
User management	Manage information about users, including user identification, application requirement, and authorization of users. Whether user management is necessary depends on application requirement.

7 Business architecture

Business architecture is an integral part of a system or technical architecture. The development of the business architecture must be completed prior to any other architectures being developed (e.g. system (logical) architecture, technology (physical) architecture, functional architecture) which all together comprise an enterprise architecture. Business architecture diagrams or figures are application-specific; therefore, the detailed business architecture is out of scope of Part 3. However, the generalized entities of a business architecture are described at a high level which can be applicable to any architecture development.

The business architecture can be defined as a conceptual reference model developed by an owner who sees the business case and market and who will invest to develop the applications and/or services for the market. The business architecture is also to communicate with key stakeholders to generate their support and participation in the creation of an enterprise architecture and also in the implementation of the architecture as a physical system or systems.

A business architecture or business conceptual reference model can be comprised of:

a) A semantic model defining business entities and business relationships between the business entities;

b) A business process model defining business process and business resources;

c) A business logistics system model defining business locations and business linkage from a business in logistics and supply chain perspective;

d) A work flow model defining organization units to perform the business and product to be generated;

e) A master schedule defining the project time line for business events and business cycle; and

f) A business plan defining business objectives and business strategy.

It is also useful to document the potential changes in the business models in order to provide the required flexibility in the sensor network design.

8 Information architecture

8.1 Introduction

Information architecture is a component of enterprise architecture that deals with the information component when describing the structure of an enterprise. It focuses on the application and data aspects of an IT system. Information architecture often includes application architecture and the corporate data model. Application architecture highlights the data flows between applications in an integrated information system.

One of the goals of information architecture is to derive common data model and standardize data exchange formats across organizations and agencies. By standardizing data objects, architecture complexity will be much lower and tome to deliver new services will be significantly reduced. Information architecture is an enterprise wide activity that includes such aspects as data architecture, metadata management and knowledge management.

8.2 Application architecture

Application architecture, like the one shown in Figure 5, provides an outline for the specific applications to be adopted, their associations, and their relationships to the business processes of the enterprise. The applications are not described as systems, but as groups of capabilities that manage the objects in the data architecture and support the business processes in the business architecture. The applications and their capabilities are described without reference to specific technologies. The applications are relatively established with updates on a periodic cycle. On the other hand, the technology used to implement the applications will change over time, based on the technologies currently available and changing business requirements. In general, "user" means an entity (human or non-human (e.g. machine, computer, software)) that consumes data and/or information. The functions (e.g. Visualization, Reporting, and Alerting) associated with Sensor Applications as shown in Figure 5 can reside in User Applications depending on the application/service being developed and implemented. Sensor network applications could include, but not limited to Visualization, Reporting, and Alerting.

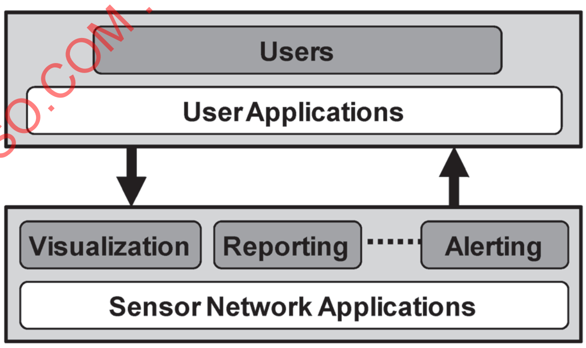

Figure 5 — Application architecture

8.3 Data architecture

Data architecture describes the structure of an organization's logical and physical data assets and data management resources. The objective is to define the major types and sources of data necessary to support the enterprise, in a way that is understandable, stable, complete and consistent. It is important to understand this endeavour does *not* include database design; this will take place as the architecture expands. The purpose is to define the data entities relevant to the enterprise.

A data architecture is an important part of sensor networks; however, architecting data access, storage, retrieval, and movement varies from one application to another. Therefore, a data architecture is addressed in this document to emphasize the data architecture's necessity in a system-level reference architecture or an implementation architecture.

9 Technical architecture

9.1 Introduction

The reference architecture consists of a set of entities which are concerned with describing a sensor network. These entities may be described in multiple ways. Each sensor network consists of a sensing domain, a service domain, and management and control as shown in Figure 4, which depicts the functional reference architecture for a sensor network. For example, sensor networks have to be established for:

— Utilizing wireless and/or wired networking technologies

— Connecting to a backbone network (e.g. public networks, Internet, Next Generation Networks, mobile communication network)

— Developing middleware that may be incorporated to perform intelligent and context-awareness processing

— Implementing application-layer technologies such as integrated service (e.g. a service-oriented architecture (SOA)), sensory information description and presentation for various sensor network applications

— Capturing data using sensor nodes and transferring the data to Application Layer through Access Network and Backbone Network

Figure 6 shows levels of services below Sensor Application Layer shown in Figure 5. Figure 6 is a graphical representation of an interoperable sensor network reference architecture from service point of view, with the arrows representing the interfaces that allow the seamless interoperability between the layers.

The interoperable sensor network reference architecture has three levels of services and two levels of applications: Sensor Service, Sensor Network Services, Sensor Processing Service, Sensor Network Applications, and User Applications/Users. The reference architecture also shows four interfaces: Sensor Device Interface, Sensor Network Interface, Sensor Processing Interface, and Sensor Application Interface.

Figure 6 illustrates all of the main entities that can be found in a sensor network. Once the top level of the architecture is documented, the physical and the system entities may then be separated and described in various architectural domains. Any single application/service or all applications/services in Figure 6 may be used in a specific architecture depending on the requirements of the architecture. A key benefit of the sensor network architecture is that it allows one to recognize and categorize the different requirements for the various parts of a sensor network and select different components to achieve interoperability.

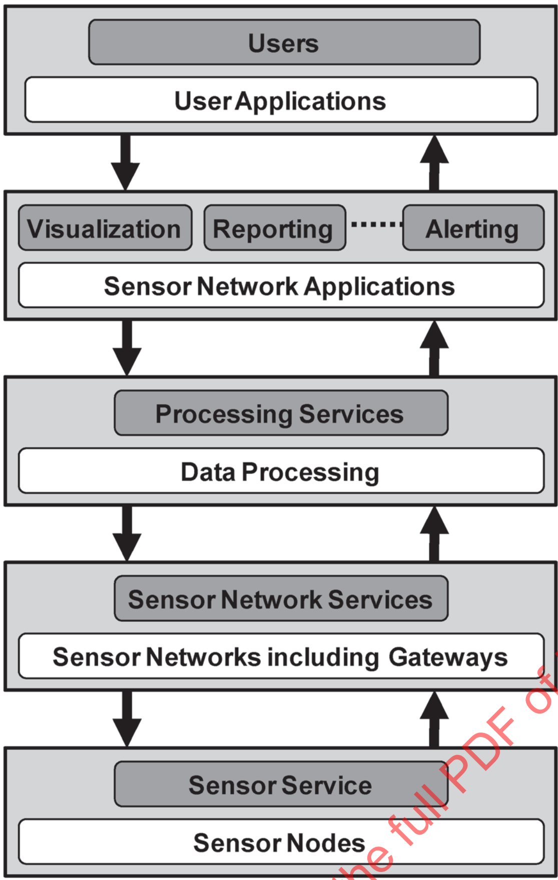

Figure 6 — Graphical representation of the interoperable sensor network reference architecture from service point of view

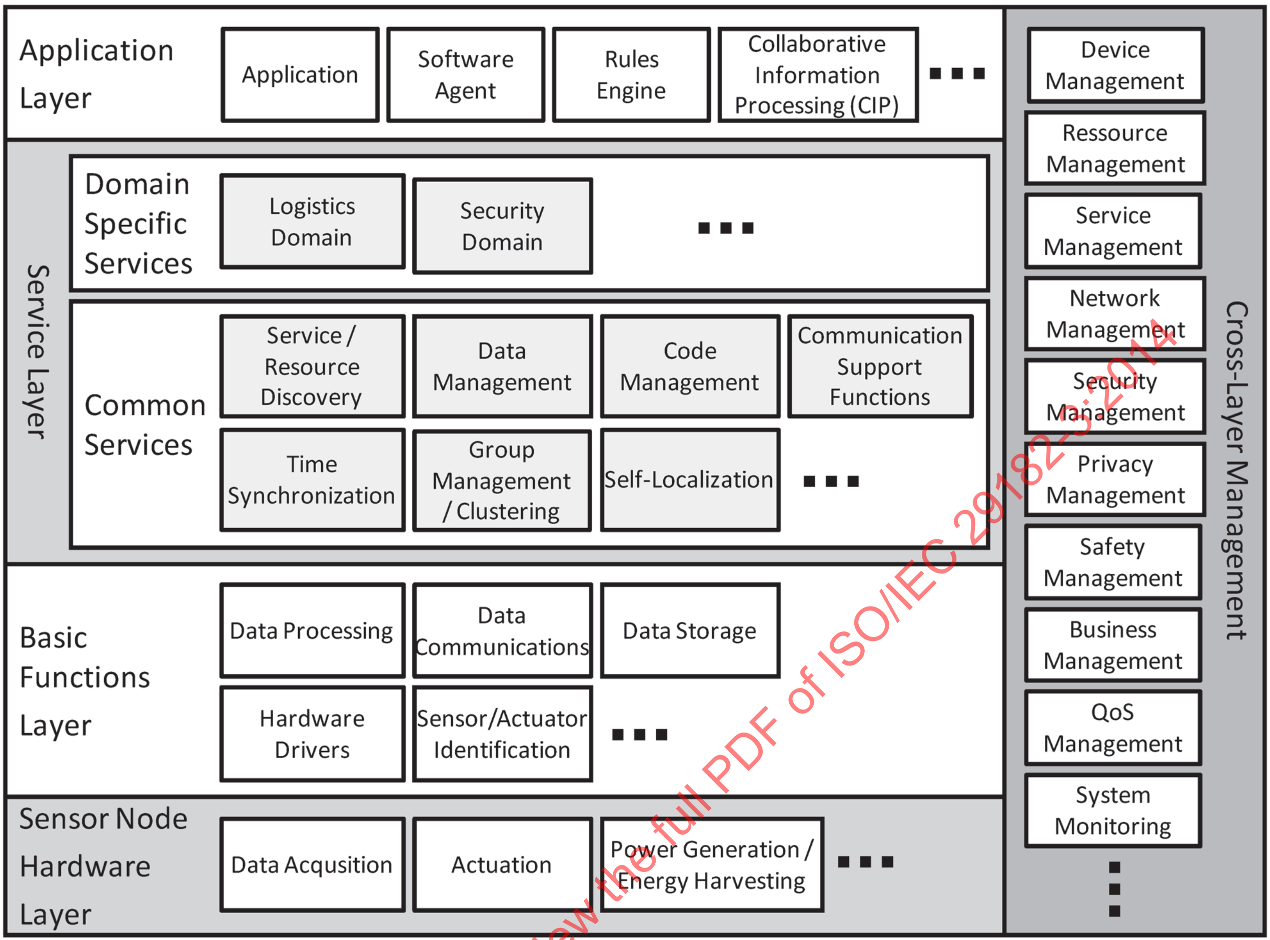

Figure 7 — Functional model of the sensor network application layer, service layer (or middleware layer) and basic functions layer, and the generic functions in the layers

Figure 7 depicts the four major layers, and the three-dotted line indicates there are other functional items can be inserted or developed, and can be considered. This figure can be mapped to Figure 6 which depicted the sensor network reference architecture from the applications and levels of services point of view.

The Service Layer functions that support the service layer represent a set of functions commonly required by sensor network applications and sensor network functions. The Service Layer functions may include, for example, sensor information gathering, filtering by various policies and rules, data comparison and analysis, data mining, context modelling, context-aware processing, context-aware decision and estimation, integrated management of sensor information, and service integration.

Figure 7 shows two functional sub-layers within Service Layer. These two sub-layers are:

a) Common Services includes services which are available within the network and can be used by other nodes or by the gateway via the backbone network. The services offer basic functionalities which are common for sensor networks. Common Services also includes support function that are generic and locally available on the sensor node; and

b) Domain Specific Services support the development of applications for a specific market segment or application area.

Using Service Layer and its functions of the sensor network reference architecture to develop an application-specific sensor network architecture, the following activities need to be performed:

a) Identification of the different functions or services within Service Layer categories: domain-specific services, common services, and support services;

b) Description of the functions required in the Domain Specific Services. The details of functionality must be worked out by companies that use Service Layer and by the service layer (or middleware) developers; and

c) Definition of interfaces between:

— Service Layer and Application Layer; and

— Service Layer and Basic Functions Layer.

The interface definition for each and every module inside the middleware, Application Layers, and Basic Functions Layer is the job of software/middleware developers and implementers. The sensor network designers and developers need to provide the software/middleware developers with sensor network system requirements and the interface definitions between middleware and application layer and also the interface definition between middleware and basic functions layer.

The functional model should be applied to middleware on the node, the gateway and the "middleware" or integration platform which is used in order to connect sensor network infrastructures to the information backbone within a company providing a sensor network based service to a customer.

9.2 Physical View

The Physical View (PV) is a description of the tasks and activities, operational elements, and information exchanges required to accomplish the business processes from the human side. The PV contains graphical and textual products that identify the operational nodes and elements, assigned tasks and activities, and information flows required between nodes. It defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of the information exchanges.

Figure 8 illustrates a generalized sequence of a sensor network's operational activities required to achieve its any given task:

a) Monitor – the inputs to this activity is typically a sensor operational planning and programming and any feedback data/information from any other activities in the activity sequence, and the output from this activity is typically an observation information of the physical world under monitoring;

b) Detect – the input to this activity is the observation information, and the output from this activity is typically the data/information about a detected object or objects in the monitoring area. The data/information can include the object(s)' features;

c) Assess – the inputs to this activity is the data/information about the detected object(s) and also location data which is the data about the location or area where the object(s) is/are detected, and the output from this activity tells about what this or these objects potentially is/are (e.g. type, identification, etc.);

d) Decide – the inputs to this activity is the data/information about the object(s) and any other data available from other sources (e.g. data level) if available, and the output of this activity is accurate parameters about the detected object(s);

e) Response – the inputs to this activity is the parameters about the detected object(s) and any other data/information from other sources (through data fusion or collaborative processing – decision level), and the output from this activity is an action or reaction plan which is assigned to actuators linked to a sensor network or to a human operator; and

f) Confirm – the inputs to this activity is the observation data from Monitor activity to determine the action or reaction execution has been performed and its effectiveness and the output is the confirmation of the execution and effectiveness. If the execution is ineffective or the action/reaction cannot be confirmed, this activity may reissue the execution plan.

Each of these tasks describes the individual responsibilities along with the systems that are being utilized. In System View (SV), the systems used to accomplish the physical architecture will be dealt with in more detail.

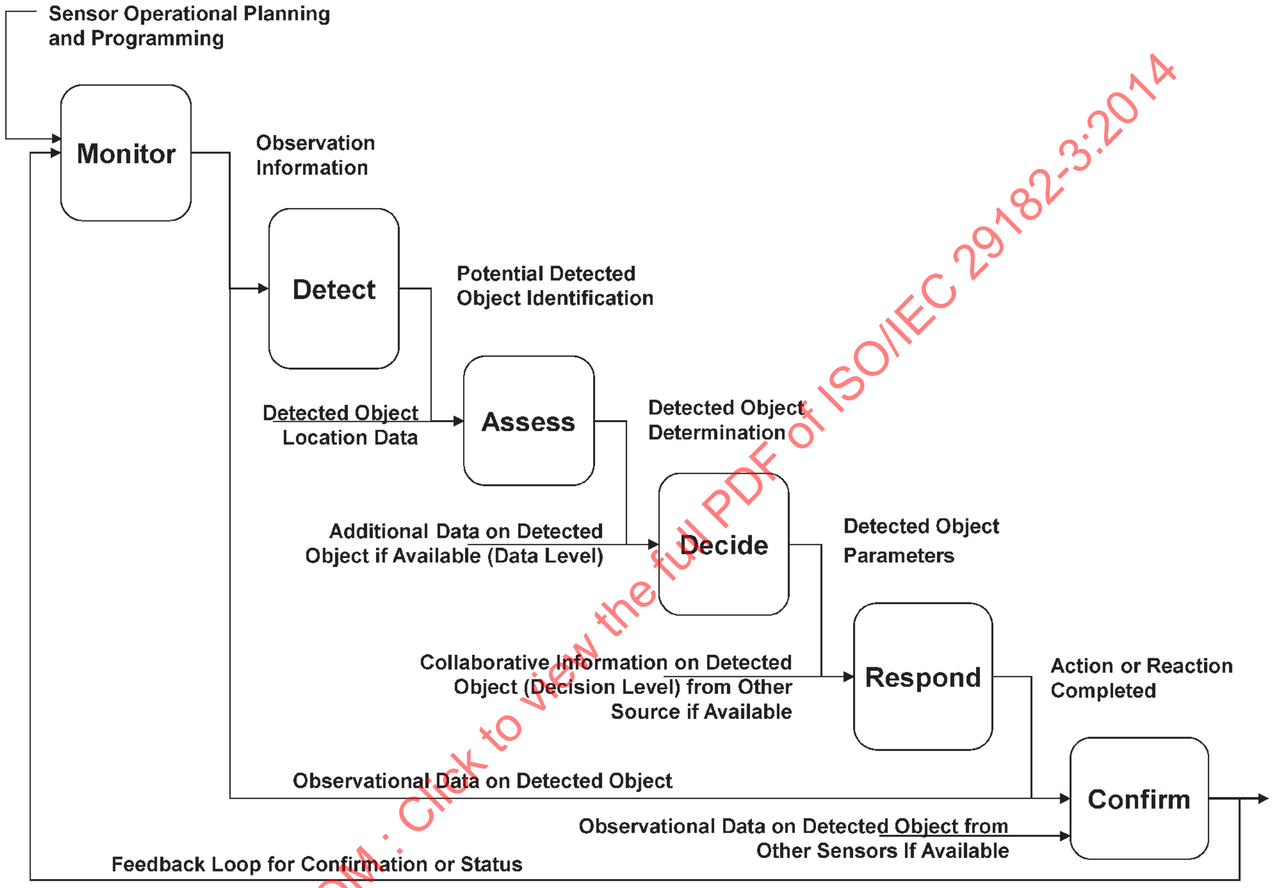

Figure 8 — Physical operational activity model

9.3 System View

The System View (SV) is a set of graphical and textual products that describe architecture systems (e.g. entities in architecture) and interconnections (e.g. lines in architecture) which provide application functions and interconnection characteristics. These functions and interconnects are called the business processes. Application functions include both business operations and business functions. The SV associates systems resources to the PV. These systems resources support the operational activities and assist the exchange of information among operational nodes. The SV describes the technological systems and their functions to support the human side of the PV.

Figure 9 shows the system view of the sensor network communications architecture of one instantiation based on Figure 2. This figure shows that two sensor networks are connected to a backbone network through Sensor Gateway Node and Access Network. A sensor network consists of multiple, geographically dispersed sensor nodes that gather data from its environment. Data gathered by sensor networks are transmitted to Service Providers and to Users through the gateway, access network, and then backbone network.

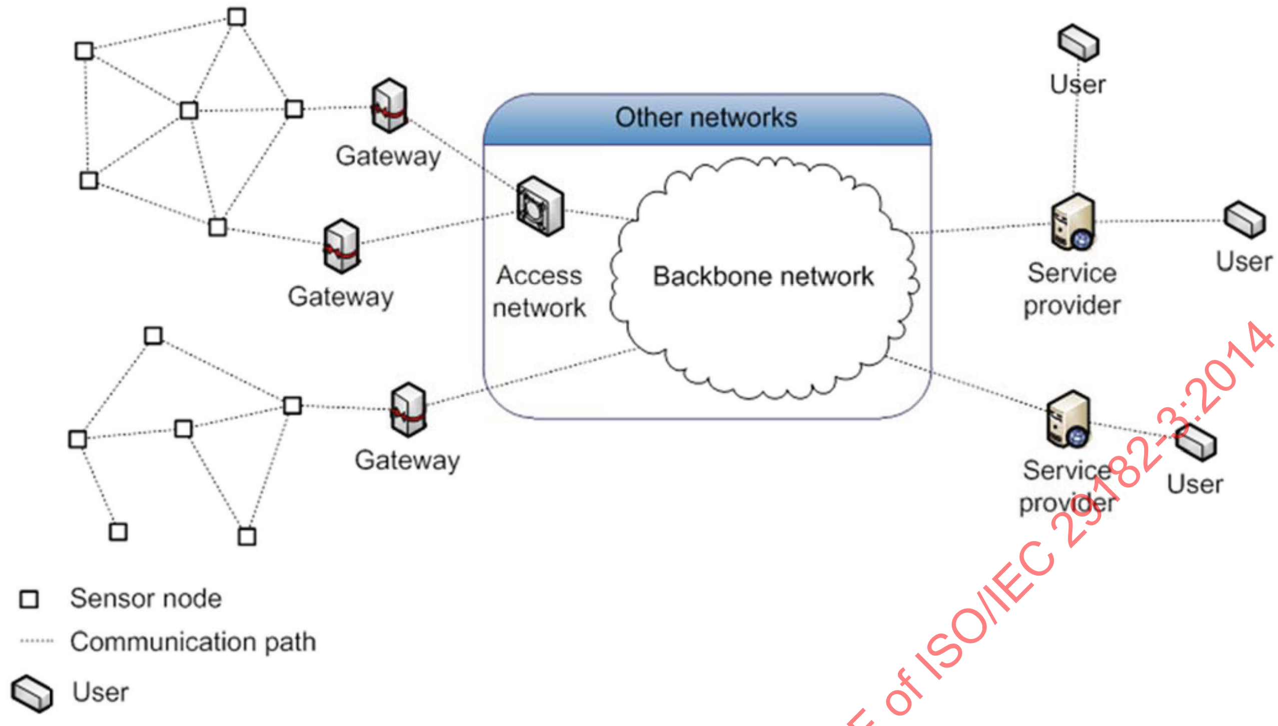

Figure 9 — Communications network architecture for Sensor Networks

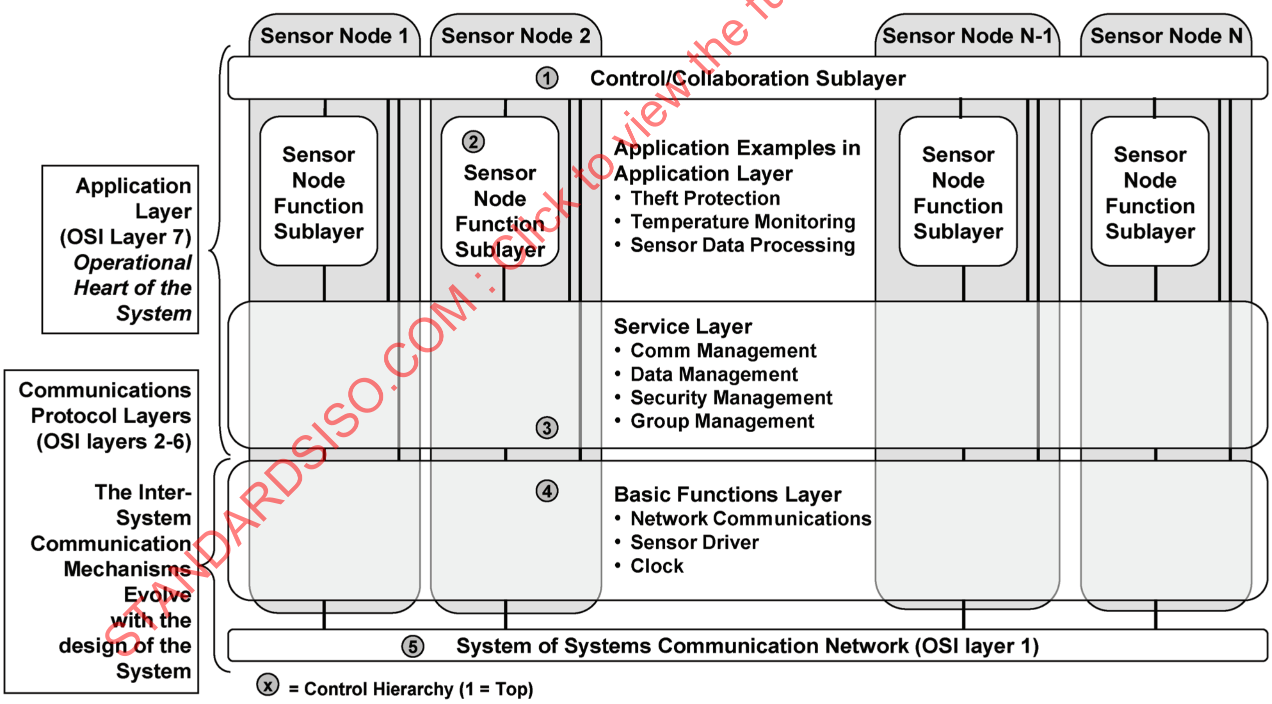

Figure 10 — Sensor networks system architecture – Layer focused

Figure 10 focuses on the application layer and the sub-layers of the sensor network reference architecture that are created to service multiple applications (e.g. theft protection, temperature monitoring, and sensor data processing) as shown in this figure. The application layer interacts with software applications that implement data/information communications. 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. Figure 10 also shows the control hierarchy with numbers where "1" being the top level in the

