INTERNATIONAL STANDARD

ISO/IEC 29182-6

First edition
2014-08-01

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

Part 6: **Applications**

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

Partie 6: Applications

Reference number
ISO/IEC 29182-6:2014(E)

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

Published in Switzerland

Contents

Page

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is 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 that multidisciplinary expertise, such as sensors, communications and networking, signal processing, electronics, computing, and cyber security is required to design a sensor network. Presently, the design process is so complex that one can leverage little from one sensor network design to another. It appears as if one has to start from almost scratch every time one wishes to design and deploy a sensor network. Yet, upon closer inspection, there are many commonalities in instantiations of sensor networks that realize various applications. These commonalities include similarities in the choice of network architecture, and the entities/functional blocks that are used in the architecture.

The purpose of the ISO/IEC 29182 series is to

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

— improve interoperability of sensor networks, and

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

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

The ISO/IEC 29182 series 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.

ISO/IEC 29182-4 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.

This part of ISO/IEC 29182 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.

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

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

Part 6:
Applications

1 Scope

This part of the ISO/IEC 29182 series, describes and provides

— a compilation of sensor network applications for which International Standardized Profiles (ISPs) are needed,

— guidelines for the structured description of sensor network applications, and

— examples for structured sensor network applications.

This part of ISO/IEC 29182 does not cover ISPs for which drafting rules are described in ISO/IEC TR 10000. Due to the generic character of ISO/IEC 29182 fully developed ISPs will not be included in this International Standard.

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 29182-3, *Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 3: Reference architecture views*

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*

ISO/IEC 29182-7, *Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 7: Interoperability guidelines*

ISO/IEC TR 10000-1, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*

ISO/IEC TR 10000-2, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 2: Principles and Taxonomy for OSI Profiles*

ISO/IEC TR 10000-3, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 3: Principles and Taxonomy for Open System Environment Profiles*

3 Terms and definitions

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

4 Symbols and abbreviated terms

ISP	International Standardized Profile

5 An overview of sensor network applications

Sensor network market segments and applications are vast and diverse covering both horizontal and vertical markets. The sensor network potential market segments and their current and future applications that employ wired/wireless sensor networks are listed in the following table.

Table 1 — Examples of sensor network market segments and applications

Market segments	Sensor network applications
Logistics and supply chain management	— Cold chain monitoring — Monitoring of hazardous goods and chemicals — Theft prevention in distribution systems for high value goods — Container monitoring in global supply chains — Monitoring of electronically sealed freight containers — Decentralized control of material flow systems
Energy & utility distribution industry	— Smart grid systems — Automated meter reading
Automation, monitoring, and control of industrial production processes	— Automation of manufacturing processes — Quality control of production processes — Machine condition monitoring — Inventory tracking and surveillance — Personnel tracking at production sites — Control of manufacturing robots
Health care and medical applications at home and in hospitals	— Monitoring of vital physiological parameters — Position and posture monitoring — Hospital personnel and patient tracking
Care for elderly and/or disabled people	— Monitoring of activity patterns for early detection and prevention of hazardous conditions — Fall prevention and detection — Body position and posture monitoring — Remote monitoring and adaptation of habitat conditions (temperature, humidity, etc.) — Remote monitoring of water consumption — Remote monitoring of emotions — Automation of medication management — Nutrition monitoring — Early warning systems for the prevention and detection of emerging chronical conditions like Alzheimer and Parkinson

Table 1 *(continued)*

Market segments	Sensor network applications
Critical infrastructure protection and public safety	— Monitoring of structural integrity for bridges, tunnels, and gymnasiums — Early warning systems for detection of emerging forest fires — Landslide monitoring and early warning systems — Video surveillance, for example, at airports — Monitoring of personnel and environmental conditions in mines — Localization and monitoring of fire fighters and other emergency responders
Automation and control of commercial buildings and smart homes	— Building energy conservation systems — Remote monitoring of habitat for an enhanced feel of security — Monitoring and control of temperature, humidity, heating, light, etc.
Automation and control of agricultural processes	— Precision agriculture — Crop disease management — Nutrient management
Intelligent transportation and traffic	— Parking management systems — Harbour freight intelligent management systems — Advanced travellers information system — Advanced public transportation systems — Commercial vehicle operation systems — Advanced vehicle and highway information and management systems
Environmental monitoring, forecasting, and protection	— Monitoring of permafrost soil for early detection of problems — Detection of water pollution in nature reserves — Temperature monitoring of coral reefs — Sea floor monitoring and mapping — Detection of gas leakage in the chemical industry — Weather observation and reporting — Monitoring of ambient parameters in forest soils — Remote ecological sensor networks for endangered species — Environmental pollution monitoring, seismic sensing, and flood monitoring
Facility management	— Monitoring and control of offices and large buildings — Monitoring and control of industrial sites — Smoke, gas, and fire detection — Security systems for art work, windows, and doors
Asset management	— Management of mobile assets in hospitals — Blood bag monitoring and status tracking

Table 1 *(continued)*

Market segments	Sensor network applications
Defence and military applications	— Battlefield monitoring — Military vehicle operations and maintenance — Monitoring of troop movements — Locating snipers
Homeland security	— Container security in global supply chains — Monitoring of infrastructure like transport and energy systems — Chemical, biological, radiological, and nuclear threat detection — Border control and virtual fences used as anti-intrusion systems

Some of these applications have already been described in larger detail in ISO/IEC JTC1 SGSN N149, SGSN Technical Document Version 3.

6 Guidelines for the description of sensor network applications

6.1 Introduction

ISO/IEC 29182-1/2/3/4/5 provide an overall reference architecture for sensor networks. This reference architecture allows the deduction of questions, which have to be answered during the design of a sensor network application. The following sub-clauses describe which information is needed.

6.2 General information

For a structured description of sensor network applications the following information is needed:

- **Purpose:**

  The purpose of the application has to be described in a first level of detail from the user's point of view ("What is the main problem which is addressed by the sensor network-based solution?").

- **General requirements:**

  General requirements relevant to the application shall be addressed. A broad variety of general requirements is presented in ISO/IEC 29182-1 ("Which requirements have to be met by the solution from a general perspective?").

- **Main characteristics:**

  Main characteristics relevant to the application shall be addressed. The main characteristics of a sensor network are presented in ISO/IEC 29182-1 ("How can the sensor network be characterized from a general point of view?").

- **Information exchange between sensor network and application server:**

  The information exchanged shall be described ("What kind of information is transferred between sensor network and backend application?).

6.3 Architecture

For a structured description of sensor network applications the following information is needed:

- **General description:**

  A figure describing the sensor network application is required. A top level description of relevant data shall be given ("What does the system look like from large distance?").

— **Physical entities:**

The physical entities of the sensor network should be named and described briefly. A detailed list of physical entities can be found in ISO/IEC 29182-4 (“What are the main hardware elements which are working together?”).

— **Operation process:**

The process of sensor network operation should be described following Figure 8 in ISO/IEC 29182-3. Each one of the steps named in the figure has to be commented (“How do the different physical entities work together in order to fulfil the purpose?”).

— **Necessary functions:**

The software modules which are needed for the application should be named and explained briefly. A list of potential functional entities is presented in ISO/IEC 29182-4. They have to be assigned to the different physical entities named above (“Which physical entity has to provide which application function?).

— **Communication network architecture:**

The network topology of the sensor network should be explained. Basic topologies are described in ISO/IEC 29182-1 (“Who is talking with whom and when?”).

— **Relevant interfaces:**

The interfaces should be listed for which standards are needed. Possible interfaces are described in ISO/IEC 29182-5 (“Where are base standards needed?”).

7 Example: Management of mobile assets in hospitals

7.1 Introduction

In the following sub-clauses the design questions mentioned above are answered for the management of mobile assets in hospitals. There are a number of technical solutions for this application problem. The following solution is using a simple sensor network where asset location is determined based on signal strength measurements and multi-lateration. There are other means of locating mobile assets which are not addressed here.

7.2 General information

7.2.1 Purpose

Hospitals use a large number of expensive mobile assets. In order to manage those assets their positions have to be known. The purpose of a sensor network-based application is to determine the position of a given asset within the hospital.

7.2.2 General requirements

The following table shows the main requirements of the needed sensor network:

Table 2 — Main requirements of the needed sensor network

Requirement	Description
Connectivity to other networks	The sensor network has to be integrated into the already existing IT landscape. Depending on the complexity of the area which has to be monitored one or more gateways are needed.

Table 2 *(continued)*

Requirement	Description
Deployment and coverage	The sensor network is used to locate assets within typical hospital buildings. Bed rooms, storage rooms, corridors, halls, operating theatres, and patient preparation rooms have to be covered. Deployment has to be done by IT departments.
Support of heterogeneous sensor networks	In principle, the sensor network is homogeneous. It has to be ensured that the network does not interfere with other wireless networks which are used in the hospital environment. Cooperation with such networks has to be ensured.
Sensor node mobility support	Assets are mobile and can be moved between rooms and different floors. The sensor network has to support full mobility of nodes attached to assets.
Power and energy management	The lifetime of the battery has to be maximized. The lifetime has direct effects on the business case and on the acceptance of the system.
Quality of service support	There has to be a timely response to a location enquiry and the location estimate needs to be precise.
Dynamic adaptation	The sensor network has to support a dynamic topology due to the mobility of the sensor nodes which are attached to the assets.
Context-awareness	The function of the system is limited to identification and locating of mobile assets in the hospital environment. There are no specific requirements concerning context-awareness.
Scalability	Limited scalability is needed due to the mobility of nodes and sometimes large number of assets besides the patient beds or in the storage rooms.
Privacy	In case the location information for an asset can be logically linked to a patient, the location information is private. Therefore, privacy regulations have to be taken into account during the design of the sensor network-based solution.
Security	The probability of attacks is limited. Standard security mechanisms are in order. Nevertheless, a risk analysis should be carried out during the design of a sensor network-based solution. Results of the analysis can provide more information concerning necessary security mechanisms.
Sensor network management	There are no special requirements concerning the management of the sensor network.
Discovery capabilities	The network topology is dynamic. Therefore, nodes have to have the capability to detect the presence of other nodes. Apart from that there are no special requirements concerning discovery capabilities. The nodes are implemented by the IT department of the hospital. The department has to make sure that the new nodes fit into the system. Service discovery is not necessary either.
Routing	In order to minimize the costs of the system, a multi-hop routing algorithm is needed. Apart from that, there are no special requirements concerning routing.

7.2.3 Main characteristics

The following table shows the main characteristics of the needed sensor network:

Table 3 — Main characteristics of the needed sensor network

Characteristic	Description
Service provisioning for individual requirements	In hospitals medical devices move within the building. Especially in emergency situations such movements are not controlled or documented. In order to make the devices available, the position has to be determined. Today, this is done often manually. The sensor network application described here automates the locating process.
Data gathering and pre-processing	Here, the location of a device is determined by the node which is attached to the device itself. The position is then sent to a central computer using the sensor network.
Collaborative information processing	Limited collaborative information processing is needed in this application during the locating process. Nodes attached to the assets and fixed anchor nodes have to work together in order to determine the position.

Table 3 *(continued)*

Characteristic	Description
Maintenance-free operation	All nodes can be accessed by maintenance staff. Therefore, maintenance-free operation is not needed.
Dynamic network topology	In case that an anchor node drops out the network should reconfigure itself automatically so that the functions of the system are not disabled.
Energy efficiency and operating life time	Since maintenance-free operation is not necessary, energy efficiency and operating lifetime does not play a major role. However, long operating lifetime between maintenance cycles are needed in order to create a good business case.
Self-adaption	Self-adaption is not necessary. The different nodes do not change their role within the application context.

7.2.4 Information exchange between sensor network and application server

The following information is exchanged between the sensor network and the application server:

- Identification number of asset
- Identification number of node attached to asset
- Position request
- Position information

7.3 Architecture

7.3.1 General description

Figure 1 shows the typical structure of a sensor network-based system for management of mobile assets in the hospital environment (one floor).

Asset nodes are attached to mobile assets; anchor nodes are distributed in rooms, corridors etc. In this case the connection between the sensor network and the asset management application server is realized by a single gateway. In the case of more complex installations more than one gateway can be used in order to make the system more robust. Each asset node continuously senses the signal strengths of anchor nodes in reach, calculates its own position and connects to the strongest anchor node in order to send the location information to the backend application. Anchor nodes use a multi-hop communication protocol in order to forward information from the asset nodes via a chain of anchor nodes to the nearest gateway and vice versa. In principle, the topology of the network can change dynamically depending on the signal strengths of neighbouring nodes. In case that the asset management application asks for the position of a node, the position is determined by the node of interest and routed back to the application server. The same structure exists on every floor of the hospital building. All gateways are connected with the application server by wire.

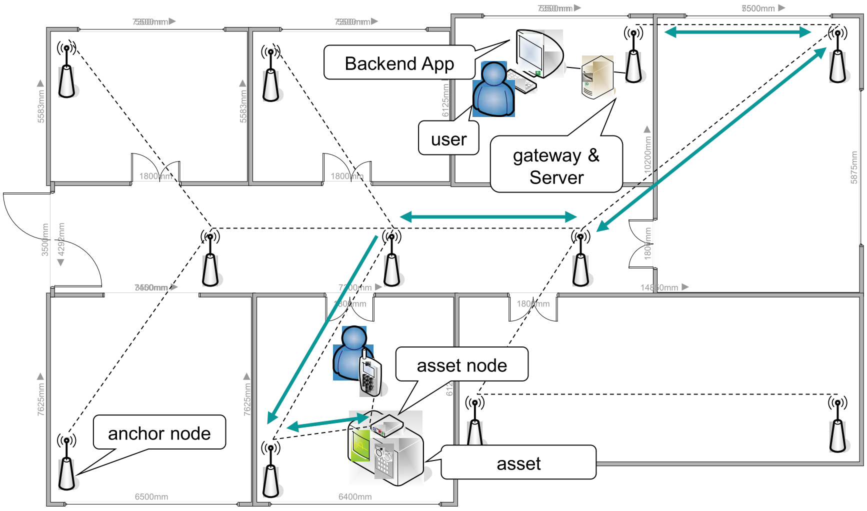

Figure 1 — Asset management based on sensor network

7.3.2 Physical entities

The following physical entities are needed to set up the system:

— **Asset nodes:**

Small nodes which are attached to mobile assets. Each node consists of a processor, a power supply, a wireless communication module, and antenna and memory. Additional sensors or actuators are not needed. The antenna acts as a sensor measuring the strength of signals coming from anchor nodes. Batteries are used as power supplies. During maintenance process batteries have to be changed or recharged.

— **Anchor nodes:**

Nodes which are attached to walls or ceiling. Each node consists of a processor, a power supply, a wireless communication module, and antenna and memory. Additional sensors or actuators are not needed. Batteries are used as power supplies. During maintenance process batteries have to be changed or recharged.

— **Gateway:**

Access point which is attached to wall or ceiling. The device consists of a processor, a power supply, a wireless communication module, an Ethernet interface and memory. Additional sensors or actuators are not needed. The device is connected to the power grid; thus, batteries are not needed.

7.3.3 Operation process

The following table shows the operation process after a locating request.

Table 4 — Operation process after a locating request

Process step	Description
Monitor	In order to locate itself, a mobile node has to monitor the wireless connection with a set of anchor nodes. At least four anchor nodes have to be in reach in a solution that uses multi-lateration.
Detect	For locating the asset, the different connections have to be characterized according to the requirements of the locating algorithm to be used (time of flight measurements, measurement of received signal strength, etc.). Results are stored on the node.

Table 4 *(continued)*

Process step	Description
Assess	A locating algorithm which is installed on the node uses the generated information in order to calculate the position of the node. Additional information on the location of the anchor nodes has to be provided by the anchor nodes and taken into account by the asset node.
Decide	The asset node has to make sure that the requirements concerning quality of service for the location information (e.g. for at least 95% of all locating processes, the accuracy of the location information should be within 3 m of the true location) are met.
Respond	Location information is then combined with the identification number of the asset and sent back to the application server via anchor network and gateway. The identification number has to be stored on the asset node during system set-up.
Confirm	At the end of the process the backend system sends back confirmation information to the sensor node via gateway and anchor network in order to terminate the process.

7.3.4 Necessary functions

Generic functions have already been described in ISO/IEC 29182-4. The following list describes only the most important functions from an application point of view.

The sensor network has to provide the following functions:

Table 5 — Functions

Function	Description
Data acquisition	The software module on the asset node monitors wireless connections between nodes and measures the received signal strength. The information is then stored on the asset node for further use. The measurement is triggered by the user. Simultaneously, anchor nodes in reach have to be asked for their location information. Another option is to pre-load the locations of anchor nodes on asset nodes, so that the latter do not have to ask for the locations of the former for every localization enquiry.
Data processing	An application software module needed is on each asset node. The module receives queries for node location from the gateway, triggers the self-locating function of the node, and sends back results of the locating process together with a number identifying the asset itself. It has to also ensure that requirements concerning quality of service (location accuracy, latency time) are met.
Data communication	All physical entities have to provide a communication module for short range communication. Energy efficient communications protocols have to be used. The protocol has to support dynamic network structures. The only wired connection within the application system is the connection between the gateway and the information backbone of the hospital. Here, Ethernet standards can be used.
Data Storage	The data which has to be stored on the nodes is limited. Asset nodes have to store the location history of the node as well as an electronic licence plate for the asset. Anchor nodes have to store context information like room number and their own exact position which is needed in order to run the self-locating service on the asset nodes.
Identification	Each node needs an identification number. Any numbering system, indigenous to the user, the user group or industry, may be used. The Sensor Node Unique Identifier shall be included in the record sent to the Anchor Node and provides authentication of the asset. The Backend Application or the application module on the asset node has to make sure that there is a logical link between the identification number of the node and the identification number of the asset.
Self-localization	The asset nodes have to be able to determine their locations based on information provided by the anchor network. Different locating mechanisms can be used. The self-localization service has to make sure that the required quality level for the locating information is met.

The following table shows the functions that have to be assigned to each type of physical entity:

Table 6 — Assignment of functions to physical entities

Function	Physical entities		
	Asset nodes	Anchor nodes	Gateways
Data acquisition	X		
Data processing	X		
Data communication	X	X	X
Data Storage	X	X	
Identification	X	X	X
Self-localization	X		

7.3.5 Communication network architecture

The communication network architecture can be characterized as follows:

- The network is a stand-alone network.
- Anchor nodes as well as the gateway are fixed and linked by a wireless connection. They build a multi-hop network serving as a backbone network in this application.
- Asset nodes move through the fixed network and connect with anchor nodes in reach.
- Requests for position information are issued by the application in the backend and are broadcast into the network via the gateway(s).
- Position information is sent into the backbone network via the strongest communication link.
- All anchor nodes in reach are used in order to determine the position of the mobile asset node.

7.3.6 Relevant Interfaces

The following interfaces have to be standardized:

- The interface between the service provider and the user (Interface 1 in Figure 8 in ISO/IEC 29182-5)
- The interface between the gateways and the service provider (Interface 3 in Figure 8 in ISO/IEC 29182-5)
- The gateway between anchor nodes and gateway (Interface 4 in Figure 8 in ISO/IEC 29182-5)
- The interface between asset nodes and anchor nodes as well as between anchor nodes (Interface 5 in Figure 8 in ISO/IEC 29182-5)

8 Example: Container monitoring in the global supply chain

8.1 Introduction

In the following sub-clauses the design questions mentioned in Clause 6 are answered for the monitoring of containers in the global supply chain. There are a number of technical solutions for this application problem. The following solution is using sensor nodes attached to shipping containers, where the status information of shipping containers in a supply chain is communicated to all relevant stakeholders.

8.2 General information

8.2.1 Purpose

The main purpose of the application is to monitor the status of shipping containers in terms of temperature, humidity, shock and impact, tampering and to be able to determine the location of the shipping container with adequate precision.

8.2.2 General requirements

The following table shows the main requirements of the needed sensor network:

Table 7 — Main requirements of the needed sensor network

Requirement	Description
Connectivity to other networks	Containers equipped with sensor nodes are connected using a multi-hop network. In addition, one or more gateways are used to connect the network of containers to the backbone network through an access network. The status information from a container can have several intended destinations such as shipping organizations, freight owners, forwarders, and customers (see Figure 3).
Deployment and coverage	Networking and communications capabilities should be provided anywhere shipping containers can be found, such as in sea/road transport and in ports and terminals.
Support of heterogeneous sensor networks	It cannot be guaranteed that all shipping containers would use the same sensor network protocol. Therefore, the gateways have to support different protocols used by the containers. It has to be ensured that there are no RF interference issues.
Sensor node mobility support	Containers can be in motion. Therefore, the used sensor network protocol has to support mobility.
Power and energy management	Given that containers might be moving on a ship for extended periods of time and the communications have to be supported by a battery in the container, it is important to use energy efficient communication protocols.
Quality of service support	Any change in the container status, such as tampering, has to be delivered to the intended recipients in a reliable and timely fashion.
Dynamic adaptation	Due to the fact that the physical structure of the sensor network is changing the network protocol has to support self-organization, dynamic network topology, and self-healing.
Context-awareness	Depending on the location and content of a shipping container, the warnings regarding the status of the container issued by the sensor node might be different. Therefore, the system has to support different context-specific communication and information strategies.
Scalability	Due to the large number of shipping containers within ports and on ships, the sensor network protocol has to handle tens of thousands of containers and addition and removal of shipping containers.
Privacy	There are no privacy concerns in this application.
Security	Information about the cargo inside the shipping container has to be made available on a need-to-know basis to authorized personnel only.
Sensor network management	There are no special requirements concerning the management of the sensor network.
Discovery capabilities	The containers as well as gateways in ports, on vessels, on trucks etc. offer different types of application specific services like temperature monitoring or providing location-specific context information. In case that a shipping container is recognized by a gateway or by another container, information about services offered shall be exchanged.
Routing	In shipping container environments shadowing always has to be expected. Multi-hop protocols are needed in order to enable communications between shipping containers and gateways.

The following figure shows how different supply chain actors are connected to shipping containers equipped with sensor nodes. Containers, which are part of the same sensor network, run in different supply chains and have to be connected to different information sinks or destinations. In order to support such kind of backend information system all sensor nodes should be integrated into the Internet via multiple gateways using the Internet Protocol.

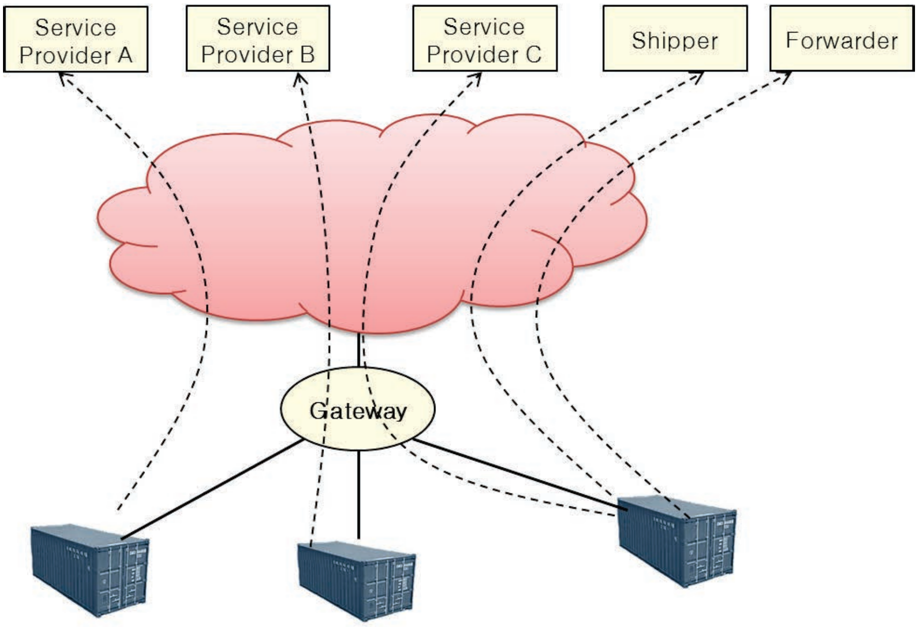

Figure 2 — Destination of container communication

8.2.3 Main characteristics

The following table shows the main characteristics of the needed sensor network:

Table 8 — Main characteristics of the needed sensor network

Characteristic	Description
Service provisioning for individual requirements	Requirements concerning transparency and security in global supply chains are becoming challenging. The main goal of supply chain actors is to reduce risks and enhance the information basis for planning of logistical processes. The shipping container has to provide software services, which address this basic need. In order to keep the system flexible and adaptable, it is necessary to add new and/or configure existing services even during transport. Service management can be handled by an external agent connected to all supply chain actors. Details are depicted in Figure 4.
Data gathering and pre-processing	Since there might be a large number of containers in a given area, it is not reasonable to have a centralized information system. Large amounts of status data acquired by a container have to be pre-processed and turned into business events by the container itself.
Collaborative information processing	There is no obvious need for collaborative information processing as long as there is no set of dispersed sensors inside a container.
Maintenance-free operation	Since it is not easy for maintenance personnel to physically access containers in global supply chains, the sensor nodes have to be robust and remotely maintained.
Dynamic network topology	Since in a given area, shipping containers are added or removed on a regular basis, the network has to handle dynamic topologies.

Table 8 *(continued)*

Characteristic	Description
Energy efficiency and operating life time	The sensors in a shipping container have to be in operation for a long time. Therefore, low power consumption is a necessity.
Self-adaption	Self-adaption is not necessary. The different sensor nodes do not change their role within this application context.

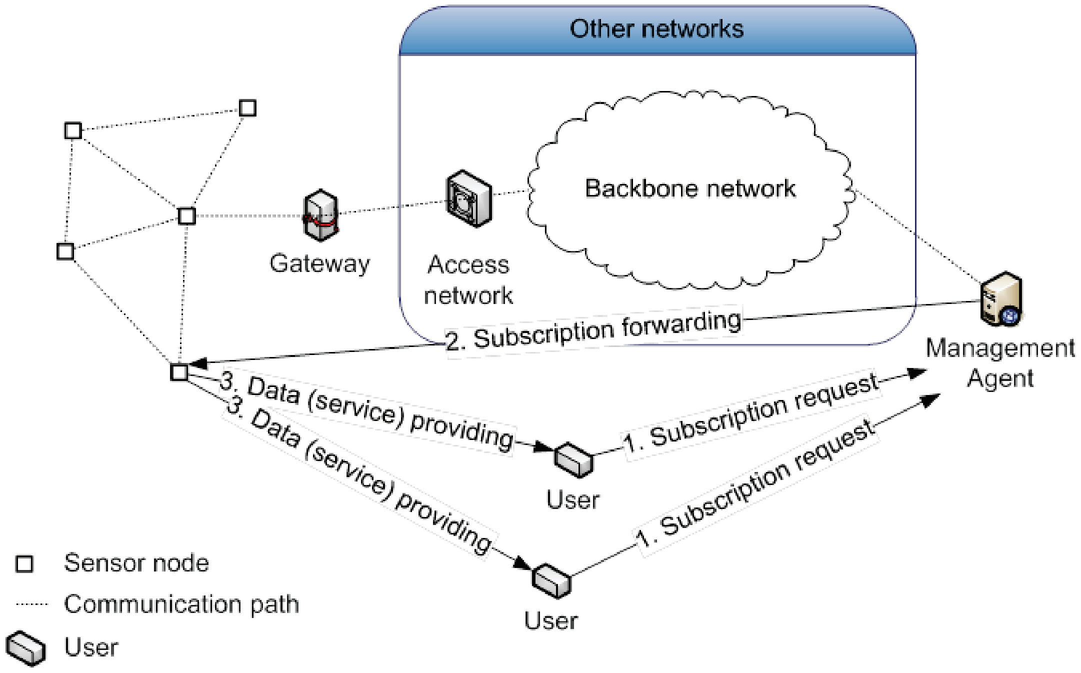

Figure 3 — External service management for service provisioning

8.2.4 Information exchange between sensor network and application server

The following information can be exchanged between the sensor network and the application server:

- Container No.
- Container location
- Door status (Open or Closed)
- Temperature (or status of in range)
- Humidity
- Shock status

8.3 Architecture

8.3.1 General description

In order to ensure global visibility of shipping containers, various modes of communications are used depending on where the container is in a supply chain. End users such as shipping organizations, freight forwarders and transportation companies can get real-time information about a container no matter where it is.

Figure 5 shows different environments where shipping containers may be found as well as the communications and networking architecture in each environment. Radio communications is challenging when shipping containers are stacked up anywhere. Therefore multi-hop networking is used to facilitate communications between a gateway and the shipping containers. This is depicted by the blue arrows in the figure.

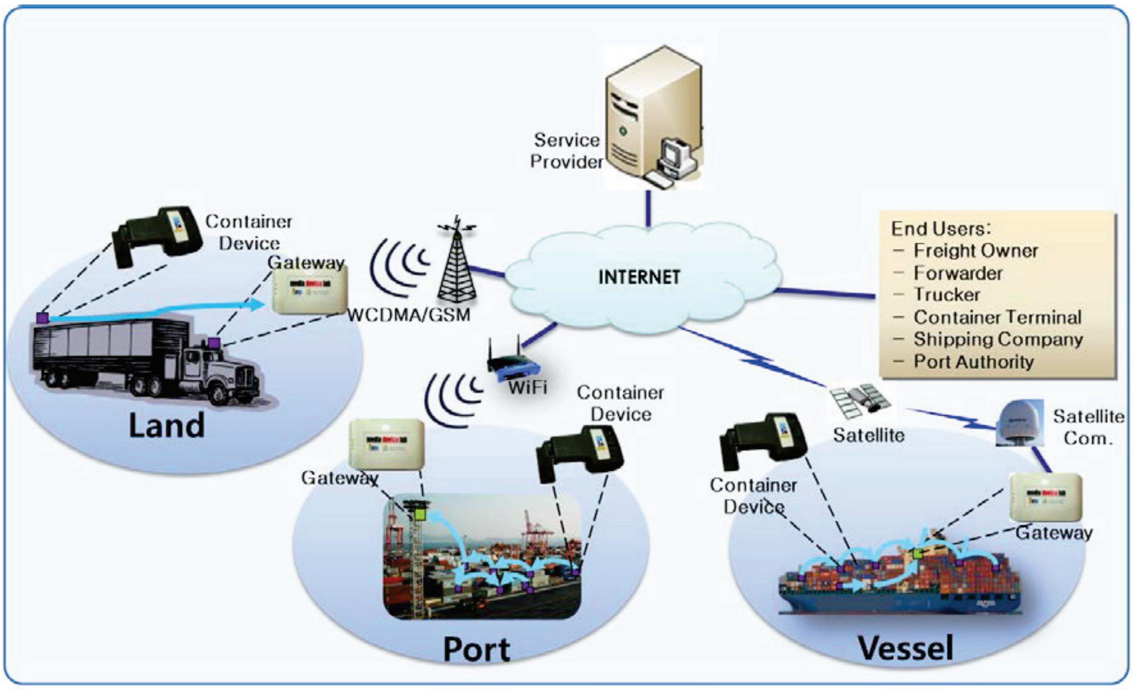

Figure 4 — System architecture

8.3.2 Physical entities

The following physical entities are needed to set up the system:

- **Container Devices:** These devices are deployed inside shipping containers and they provide the sensing and communication capabilities to inform the status of shipping containers. Each such device comprises various sensors, a communications module for communicating with a gateway and a localization module. At the minimum the devices measure temperature, humidity and whether the container door is secured or not.
- **Gateways:** Gateways act as a communications bridge between shipping containers and the backend information system. As shown in Figure 5, they use various modes of communications depending on the environment.

The container device and the gateway can be integrated into one physical entity.

8.3.3 Operation process

The following table shows the operation process for container monitoring

Table 9 — Operation process for container monitoring

Process step	Description
Monitor	Temperature and humidity sensors periodically make measurements inside the shipping container. The shock sensors and the door lock sensors continuously monitor the container. The localization module estimates the container location.

Table 9 *(continued)*

Process step	Description
Detect	Whenever temperature, humidity, or 3D accelerometer measurements deviate from the respective target ranges, the container issues an alert and reports the measurements. In addition, a warning is issued whenever tampering is detected by the door lock sensors.
Assess	Upon receipt of an alert from a container the backend information systems or a human agent assesses the criticality of the situation.
Decide	The system or the human agent decides whether the alert represents abnormal conditions or whether, for example, due to the container being moved by a crane.
Respond	Depending on the type of the alert, a human inspector might be dispatched to the container or some other corrective steps taken.
Confirm	The system or the human agent confirms that the corrective steps taken were effective in mitigating the problem.

8.3.4 Necessary functions

Generic functions have already been described in ISO/IEC 29182-4. The following list describes only the most important functions from an application point of view.

The sensor network has to provide the following functions:

Table 10 — Functions for container monitoring in global supply chain

Function	Description
Data acquisition	Data on temperature, humidity, door lock status, 3D acceleration and location are acquired.
Actuation	As an example, in the case of a reefer container the cooling function can be controlled remotely.
Power generation/ energy harvesting	The battery is complemented with some form of energy harvesting, such as solar panels or vibration generators, to ensure the container functions properly for extended periods of time.
Data processing	Business rule engines and complex event processing mechanisms are used on the container device in order to create business events that can be handled by application software like Enterprise Resource Planning software.
Data communication	Cellular telephony, Wi-Fi, satellite communications, and wired connections are used for communications between the gateways and the backend information system. An energy-efficient multi-hop protocol is used for communications between the containers and the gateways.
Data Storage	The data gathered by the sensors in a container is backed up locally for archival purposes. After the end of the transportation process, the data can be removed from the container device and stored in a central database.
Identification	Each container device needs an identification number. The backend application or the application module on the container has to make sure that there is a logical link between the identification number of the container device and the identification number of container. ISO 6346, which is managed by the International Container Bureau, is used for assigning an identification number to a container.
Self-localization	Knowing the location of a shipping container is of great importance. Given that shipping containers are made of metal both communications and localization pose severe challenges. Some appropriate robust form of localization in this environment needs to be deployed.

The following table shows which function is related to which physical entities.

Table 11 — Interrelationships between physical and functional entities in shipping container monitoring

Function	Physical entities	
	Container devices	Gateways
Data acquisition	X	
Actuation	X	
Power generation/energy harvesting	X	
Data processing	X	
Data communication	X	X
Data Storage	X	
Identification	X	
Self-localization	X	

8.3.5 Communication network architecture

The network of container devices can be regarded as a multi-hop sensor network connected to the backbone network through gateways and appropriate access networks.

8.3.6 Relevant interface

The following interfaces have to be standardized:

- — The interface between users and service providers (Interface 1 in Figure 8 in ISO/IEC 29182-5)
- — The interface between container devices and users/service providers (Interface 2 in Figure 9 in ISO/IEC 29182-5)
- — The interface between gateways and service providers (Interface 3 in Figure 9 in ISO/IEC 29182-5)
- — The interface between gateways and container devices (Interface 4 in Figure 9 in ISO/IEC 29182-5)
- — The interface between container devices (Interface 5 in Figure 8 in ISO/IEC 29182-5)

Bibliography

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

ICS 35.110

Price based on 17 pages