ISO/IEC JTC 1 N 9067

2008-05-15

ISO/IEC JTC 1
Information Technology

Document Type:	**Other Document(Defined)**
Document Title:	**Wireless Sensor Networks: Applications, Architectures and Protocols for consideration at the 1st SGSN Meeting, 26-27 June.**
Document Source:	**SGSN Convenor**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for information**
Action ID:	**Information**
Due Date:	
No. of Pages:	**23**

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC JTC 1
Study Group on Sensor Networks

Document Number:	SGSN N008
Date:	2008-05-15
Replace:	
Document Type:	National Body Contribution
Document Title:	Wireless Sensor Networks: Applications, Architectures and Protocols
Document Source:	National Body of Germany
Document Status:	For consideration at the 1st SGSN Meeting, 26-27 June.
Action ID:	FYI
Due Date;	
No. of Pages:	22

SGSN Convenor: Dr. Yongjin Kim, Modacom Co., Ltd (Email: cap@modacom.co.kr)

SGSN Secretary: Ms. Jooran Lee, Korean Standards Association (Email: jooran@kisi.or.kr)

Paper on

Wireless Sensor Networks: Applications, Architectures and Protocols

Contribution to first face to face meeting of
the JTC1 Study Group on Sensor Networks,
Shanghai, 25. – 27. June 2008

Author
Dr. Alexander Pflaum

10. May 2008

Content

1 Background and Goal of the Paper

1.1 Call for Contribution

In December 2007 JTC1 established a study group on sensor networks. Main goal of this group is to identify and to describe standardisation requirements which have to be addressed by national and international bodies during the next years.

For the first face to face meeting in June in Shanghai a table of reference has been set up. During the meeting the following aspects of sensor networks have to be addressed:

1. Review the current definitions, visions and requirements for target applications of Sensor Networks within JTC1 and outside JTC1 in connection with different application areas (e.g. home, medical informatics, transport informatics, industrial communications, RFID etc.) as well as JTC 1 SCs roles in these application areas
2. Review and identify
   - the unique characteristics of Sensor Networks and the commonalities and differences with other networks
   - the system architectures of Sensor Networks in terms of functionalities
   - the entities that together comprise Sensor Networks and their characteristics
   - existing protocols that can be used for Sensor Networks and the elements of protocols that are unique to Sensor Networks
   - the scope of infrastructure that can be considered to be a Sensor Network
   - the types of data that need to be handled (acquired, processed, transported, stored, rendered etc) by Sensor Networks and any specific QoS attributes required by those categories
   - the interfaces that need to be supported by Sensor Networks
   - the services that need to be supported by Sensor Networks
   - aspects such as security, privacy, identification that may be relevant to specific sensor Networks
3. Monitor other activities in international standardisation bodies and consortia and fora where specifications related to Sensor Networks are being developed.
4. Produce a report covering 1) and 2) above and information on other relevant standardisation activities.

5. In the light of published SC scopes and work programmes and the results of 1) to 3) recommend potential areas of work to JTC 1 and appropriate SCs to ensure that all necessary aspects of Sensor Networks within the scope of JTC 1 are standardised.
6. Recommend how the work on Sensor Networks can be efficiently coordinated in JTC 1.
7. Hold workshops to gather requirements or publicise the results.
8. Meetings of the group may be physical or via electronic means.

1.2 Identification of Standardisation Issues for Wireless Sensor Networks as the main Goal of the Paper

It is impossible to address all topics from above in one single paper. The text on the next twenty pages focuses especially the following issues:

- Target applications of wireless sensor networks
- Unique elements of sensor networks
- Basic system architectures and services to be supported
- Interfaces to be supported and data types to be handled
- Protocols and their unique elements
- Remarks concerning standardisation issues

Main goal is to identify and to describe standardisation issues for wireless sensor networks by discussing different applications which are driven within research and development projects in Germany and Europe.

2 Target Applications of Wireless Sensor Networks

2.1 A short Overview

In 2007 a comprehensive study on existing applications for wireless sensor networks has been conducted at the Engineering Centre for Smart Items in Logistics which is a part of the Fraunhofer-Institute for Integrated Circuits in Erlangen, Germany. The following table shows the applications that have been found in literature and on web pages of the more important technology providers.

Industry	**Application**
Logistics	Temperature monitoring (e.g. in the FMCG industry)
	Hazardous goods monitoring (e.g. for chemicals on oil platforms)
	Asset Management (e.g. for tools in the aviation industry)

	Theft prevention (e.g. in distribution systems for high value goods)
	Container monitoring (e.g. sea containers in global supply chains)
	Control of material flow systems (e.g. decentralised control based on wireless nodes)
	Process optimisation (e.g. identification of bottle necks)
	Supply chain event management (e.g. in for JIT processes in automotive)
Production	Quality control (e.g. monitoring of temperatures during painting processes)
Health care	Patient localisation (e.g. for people ill with dementia)
	Monitoring of vital parameters (e.g. for people with coronary problems)
	Position and posture monitoring (e.g. for elderly people living alone at home)
Civil protection	Monitoring of building integrity (e.g. of a gymnasium or a bridge)
	Early warning systems (e.g. detection of emerging forest fires)
	Emergency management (e.g. position monitoring of fire fighters)
Security	Border control and virtual fences (e.g. securing of large plants and factories)
	Monitoring of troop movement (e.g. in training camps)
	Building security services (e.g. detection of intruders and/or fire)
Building Autom.	Air monitoring and control (e.g. for home automation
	Energy consumption optimisation (e.g. in private households)
	Intelligent living room (e.g. adaptation of environment to personal requirements)
Agriculture	Monitoring of growing areas (e.g. for irrigation strategies)
Traffic	Car-2-car communication (e.g. for early warning systems)
	Driver assistance systems (e.g. for detection of speed limits)
Environment	Monitoring of permafrost soil (e.g. for early detection of environmental problems)
	Detection of water pollution (e.g. monitoring of nature reserves)
	Monitoring of coral reefs (e.g. by temperature measurements)
	Detection of gas leakages (e.g. for emergency management)

Table 1: Target applications of sensor networks

A lot of pages would be needed to describe all these applications in detail. It is assumed that a more detailed description of a subset will suffice for the identification of the more important standardisation issues. Therefore the following pages concentrate on selected applications.

2.2 Examples for Target Applications for wireless Sensor Networks

2.2.1 Theft Prevention System for expensive Goods in Distribution

The following figures show the prototype of a theft prevention system which is based on a wireless sensor network.

Figure 1: Theft prevention system based on wireless sensor network

Definition and Vision:

Packages on a pallet are equipped with sensor nodes that detect manipulations and monitor the physical presence of their neighbour nodes. In case of intrusion or theft an alarm message is generated and routed to a security service provider. Sensor nodes can additionally support logistical processes. For example it is possible to identify all nodes or packages coming through a gate.

The more important requirements:

- Sensor node should not be larger than a smart card.
- Latency time between a theft and registration in a central data base should be less than 5 seconds.
- The price of a sensor node should be less than 2 € (this is an estimated value, actually their is no business case for this application).
- It is absolutely necessary that sensor nodes are able to operate together with RFID-readers in the same environment without disturbances.

2.2.2 Monitoring of Engine Conditions

Knowing about the current state of a helicopter, aircraft or ship engine would allow preventive maintenance. A lot of money could be saved from the manufacturers and maintenance service providers point of view.

Definition and Vision:

Miniaturized and energy autonomous sensor nodes could be attached to critical parts of an engine and identify and monitor the state of these parts. The nodes

could additionally be used for identification in logistics processes as well as for documentation of maintenance activities.

The more important requirements:

- Sensor nodes have to be integrated into parts if possible.
- They have to be robust and insensitive to high temperatures because they are operating in extremely hazardous environment.
- A short latency time is needed in order to avoid damage to the engine in case that a problem has occurred.
- High reliability and redundancy is also needed in order to meet life cycle requirements of the machinery industry.
- Passive operation of nodes would be a helpful feature in order to minimize maintenance costs for the sensor network (but: at least the aviation industry does not accept active nodes at the moment).

2.2.3 Temperature Monitoring of Blood Bags

In order to keep patients alive during operations donated blood has to be of good quality. During logistical processes the cool chain has to be maintained. The following figures show a blood bag and the type of sensor node which might be used in the future to monitor the temperature of the blood.

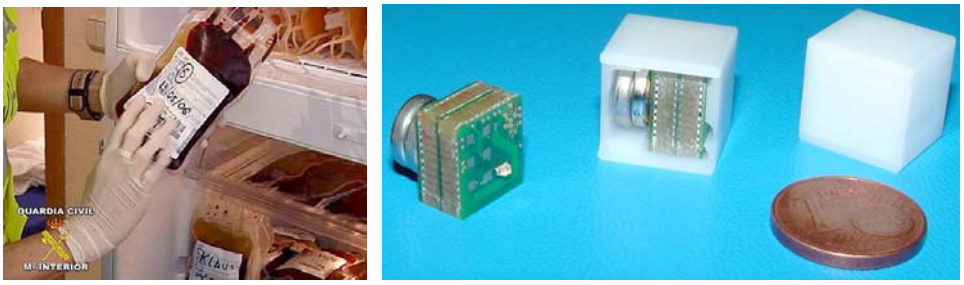

Figure 2: Sensor nodes for blood bags (right picture: with courtesy of Fraunhofer IZM in Berlin)

Definition and Vision:

In order to guarantee that the cool chain was not corrupted miniaturized sensor nodes with a temperature sensing function are connected to blood bags. The logistical infrastructure (fridges and other storage devices, transportation media etc.) is equipped with anchor nodes for localisation and information routing. In case that the temperature of the blood exceeds certain limits somewhere in the network an alarm is generated and routed to an internal service provider.

The more important requirements:

- Compliance with EMC regulations for clinical environments is needed for the sensor nodes.
- Sensor nodes have to be robust and reliable, for example they have to cope with acid cleaning agents.

– Localisation resolution less than a few meters is needed in order to meet the requirements coming from the application.
– Due to the sensible object to be tagged »real time« localisation is necessary. Only a few seconds latency time are acceptable.

2.2.4 Monitoring the Integrity of global Distribution Systems

In global supply chains many different types of integrity breaches are possible. Shrinkage, delays, out of stock situations, non-compliance with reference or standard processes are just a few examples. The following figure shows an information system based on different types of sensor networks which work together in order to avoid or at least to identify integrity breaches.

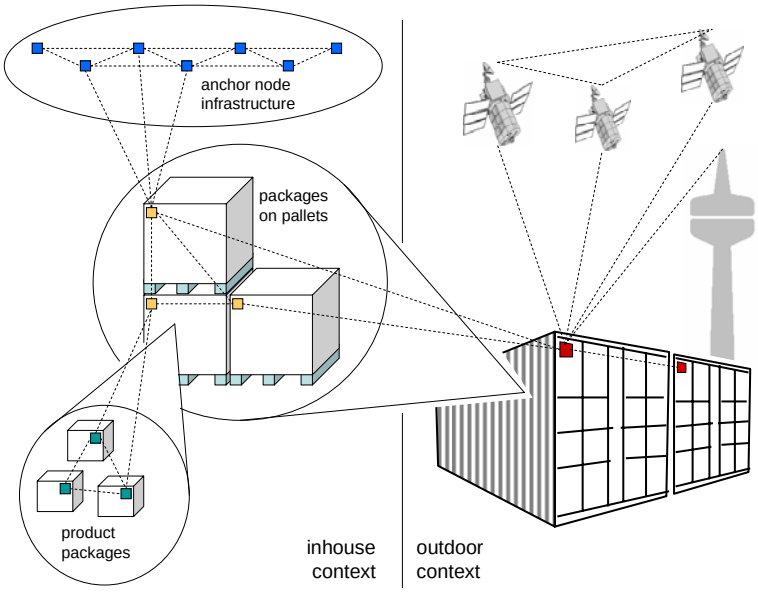

Figure 3: Supply chain integrity system based on sensor networks

Definition and vision:

Different types of sensor nodes with unique functional profiles are attached to items on different hierarchical levels (product packages, pallets, containers). On each level logistical objects are connected to each other using a wireless sensor network protocol. One of the attached nodes has to work as a gateway and to realise the connection to the next higher level of objects. Inside a building a network of fixed anchor nodes is used to determine the position of the mobile ones, outside GPS or other positioning systems do the localisation job. The system enables total transparency of objects in worldwide supply chains without integration of existing tracking & tracing systems for different object types.

The more important requirements:

- Same requirements of product and pallet nodes like in the theft prevention case have to be fulfilled here.
- Protocols have to support hierarchical clustering of nodes.
- Especially on the container level sophisticated energy consumption management algorithms have to be implemented. In a cluster of containers the energy level should decrease equally.

2.2.5 Context specific Posture Monitoring for Patients

Old and fragile people often have to be taken care of in nursing homes because living at home is by far to risky. Falling down to the floor without anybody to help them up again might result in critical situations. The worst case could be that the person dies. Sensor networks might help to detect such situations and to call somebody for help.

Definition and vision:

For example intelligent sensor nodes can be connected to the four extremities of the body, a central unit could be attached to the belt. If the sensor nodes are able to determine their relative position to each other and to the central unit as well as their three-dimensional orientation in space movement models could be used to determine whether the person is sitting, walking etc. If the position and orientation does not meet the normal conditions in a given context like lying in bed in a sleeping room or standing under the shower in the bathroom an alarm message can be generated and routed to a emergency service.

The more important requirements:

- Small nodes are needed which can be integrated into clothing. A crude and clumsy black box attached to arm or leg would not be appropriate.
- Localisation resolution has to be less than a few centimetres in order to determine position and posture of the body.
- The nodes have to be able to detect their orientation in space.
- The sensor network connected to the body has to communicate with a intelligent environment delivering context information (e.g. anchor nodes in the different rooms of a house or a flat).
- The sensor network has to protect the personal sphere of the patient in order to avoid that someone iabuses the gathered information.

2.2.6 Tracking of Persons in large Areas or Buildings

There are a lot of applications where people have to be located in large areas and buildings. Using sensor nodes fire fighters could be tracked and rescued in case of an emergency situation. Persons who have fallen ill with dementia or Altzheimer's disease can be localised in case that they have lost their way. The

position of patients in hospitals can be determined in order to optimise logistics processes.

Definition and vision:

Persons are equipped with small sensor nodes which are able to determine their own position using different localisation mechanisms. A network of anchor nodes in a building delivers necessary beacon signals and routes location information to a central IT-System.

The more important requirements:

- Scalability of the system is important in case that buildings and areas are really large.
- The communication link between the nodes has to be highly available, the nodes have to be robust in order to meet the requirements of security applications.
- Realtime location has to be guaranteed. Even in large buildings with complex network structures only a few seconds latency time are acceptable from the application point of view.
- Low energy consumption is necessary in order to enable long operation times without maintenance processes.

2.3 Special Features of Sensor Networks

The applications described above make quite clear that there are a lot of differences between wirelessly connected and networked sensors and other wireless networks.

First of all wireless sensor networks have to be regarded as the extension of the internet towards the physical world (»Internet of Things«). Things which never have been able to communicate with their environment start to »think« and to produce information which has to be processed and routed to a user. The »user« might be man or machine as well. In most cases the human user does not stand in the foreground. That means that objects to which a sensor node is attached can not rely on human intelligence and decision.

Main target of a sensor network installations is gathering and pre-processing of sensor data. Therefore intelligence on the node is needed. Sensor networks have to make sure that all the information is available and comprehensive. Communication links in the system have to be absolutely reliable and robust. If one of the links is cut off the wireless network has to find other ways to rout the information or data to the sink where it is needed. There is nobody who is able to reboot the system or to rearrange settings and configurations.

For most wireless sensor network applications sensor data has to be connected with location information. Objects or sensor nodes in the network have to be able to determine their own position. In many applications there will be no communication infrastructure that can be used for the localisation process. Due

to that the sensor network itself has to provide the localisation capabilities. Localisation is one of the most important services offered by sensor networks. The networks might be very large. Scalability is therefore very important.

In most cases the nodes have to work together in order to solve complex measurement problems. Sensor data has to be pre-processed by the single nodes, results have to be exchanged in the network, output coming from other nodes has to be compared with own results of a node, own calculations have to be revised based on the outcome of this comparison. In a lot of applications the measurement process is connected with a lot of traffic in the network. In some others only a few bits and bytes are transferred in a while. Standards have to be flexible enough to support both types of applications.

The nodes have to communicate with each other without an existing communication infrastructure. Due to that multi hop capabilities and clustering algorithms are needed. Different applications place different requirements on latency time. Sometimes an alarm message has to be routed through a large network in less than a few seconds, for other applications a minute or an hour might be acceptable. Routing and communication protocols have to be able to support both types of applications.

One of the most important characteristic of a wireless sensor network certainly is the fact, that computing has to be energy aware due to limited energy resources within the nodes and the network. The more often nodes have to be active and/or information has to be transmitted or routed through the network the more critical that issue becomes. In case of the theft prevention system which has been described in chapter 2.2.1 batteries need to be quite large in order to operate nodes and networks for two or three month. In other cases and applications sophisticated energy management algorithms are needed that keep the energy level in all nodes in a network on the same level.

The topology of the wireless network is rarely fixed. Normally it has to adapt to availability of communication links between nodes, to changing positions of objects to which sensor nodes are attached, to energy levels and roles of nodes. Applications where all the nodes are fixed are relatively easy to handle. Applications where nodes move within the network are more critical. Here the routing and communication protocols have to be very fast and flexible on the one hand and energy efficient on the other hand side.

Last but not least a wireless sensor network has to work for a long time without maintenance. There is no system administrator who is able to solve existing problems. Maintenance and problem solution capabilities are restricted to remote maintenance. At least the basic functions of the network have to work all the time. The concepts of self maintenance, self organisation, redundancy and failure tolerance are key concepts for sensor networks. Without these concepts a product will never find it's way to a comprehensive roll-out into the real world.

3 Basic Systems Architectures

3.1 Entities that comprise a Sensor Network and their Characteristics

A closer look onto the applications that have been described in chapter 2.2 shows that in general there are two different types of nodes or entities within a sensor network:

- Stationary nodes which are attached to parts of the infrastructure (walls, fences, ceiling, trees etc.)
- Mobile nodes which are attached to moving objects (cars and other vehicles, logistical objects like pallets, containers etc.)

More detailed characteristics depend on the application. For the mobile nodes there are no general characteristics apart from small size and high energy efficiency. When talking about the application specific requirements for the design of sensor nodes and networks two different types have to be taken into account:

- Applications which are based on stationary nodes (A)
- Applications where networked mobile nodes flow through a network of stationary nodes (B)

Both types are shown in the following figure:

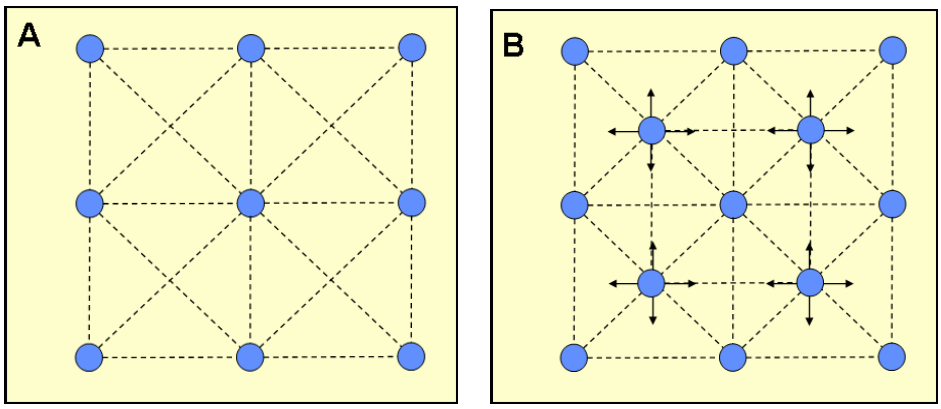

Figure 4: Different types of sensor network applications

3.2 Sensor Networks and Applications

3.2.1 The main Idea behind the Service »Issue«

Sensor networks are always embedded into applications and more complex »services« for the end consumer or customer. Application software is distributed. That means that application modules on the nodes are connected to a central application module somewhere in the IT-backend of the company. In order to connect the hardware of the node and the application module on the node a kind of »middleware« is needed. This middleware delivers more technical services to the application module on the node. The following figure shows the concept.

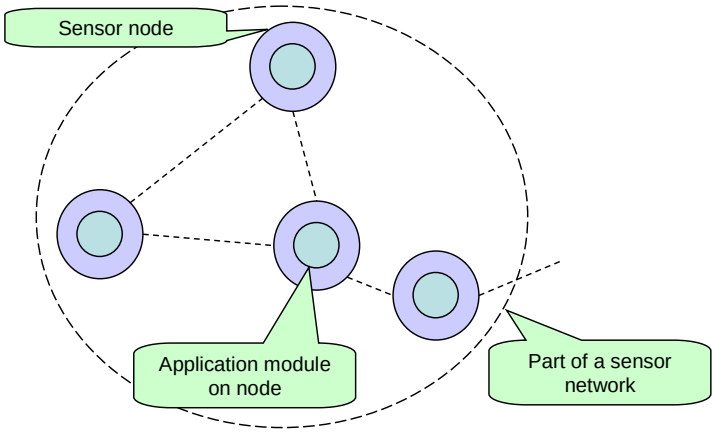

Figure 5: Sensor network with embedded application modules

The following discussion focuses the services which are delivered by the node itself in order to support application modules or »business logic« installed on the node. Services a human user is supported with by the whole network are not taken into account.

3.2.2 Services to be supported by Sensor Networks

The following list presents the services a node might deliver to it's application module. They are needed to support the different applications described in chapter 2.2. Others might be necessary for other applications. The list does not claim to be exhaustive. The services might also be understood as application specific »functions« of sensor nodes and networks.

- Long range communication service: For some applications sensor nodes have to »talk« with public communication infrastructures like the Global System of Mobile Communication GSM..
- Short range communication service: Nodes have to communicate with each other using energy efficient network and communication protocols.
- Clustering services: Depending on the application clustering of sensor nodes is necessary. The cluster concept is also used to level the energy consumption in the whole network. Energy reservoirs in nodes have to scale down equally.
- Routing service: Software packaged or messages which have been created by the application software on the sensor nodes have to be routed from node to node in order to reach the information or data sink.
- Installation service: A sensor node purchased from the manufacturer will be delivered without an application software module. The node as well as the network has to deliver a service which enables the installation of the application modules on the nodes.
- Security services: There is a lot of applications which are used in security environments. Services on the node have to make sure that the communication links, the data storage as well as the application program on the node are secured.
- Data storage services: Data which comes from the sensors has to be buffered in a storage area which is large enough for the application. A data storage or buffering service is needed.
- Data processing services: Sensor nodes have to solve complex measurement problems in a cooperative way. Intermediate results have to be calculated, communicated to other codes, compared with intermediate results coming from other nodes etc. In order to do the necessary calculations (e.g. for sensor fusion) a data processing service is required.
- Control services: In some cases sensor networks are used in applications where machines or servo engines have to be controlled by the node. This task has to be supported by special control services.
- Linkage services: In applications where the sensor node is not part of an object but is attached to one it has to be made sure that nobody disconnects the two entities without being noticed. Especially logistics and security applications need a service which guarantees a secure link between node and physical object.
- Orientation detection services: For some applications the relative orientation of a sensor node in space has to be determined. A corresponding service has to be delivered by the node.
- Self localisation service: It has already been mentioned that most applications of sensor networks need the position of the different nodes in order to work properly. Therefore the network has to be enabled to determine the position of every single node and to hand the position information to the node concerned.
- Monitoring service for communication links: In the theft prevention scenario the sensor nodes have to monitor the communication links to the

neighbour nodes continuously. The nodes therefore have to support monitoring services which can be called on by the application module which has been installed.

- General sensing service: A sensor node is often able to sense different types of environmental parameters. Services are needed which are able to operate the sensing hardware, to transform analog measurements into digital information and to give this information to the application module on the node.
- Identification Service: For some applications it is necessary to determine the unique identification number of the object the node is attached to. RFID-technology could be used for that issue. In that case the node is required to operate a RFID reader and to hand the EPC number or another identification number to the application software on the node.
- Data entry services: In some applications sensor nodes are attached to human beings. It might be necessary that the human user gives information to the sensor node by keying in information using a small panel. The information is than forwarded to the application module on the node. The node has to deliver that functionality as a service.
- Indication services: In other applications the node is required to switch on a LED or to generate a sound in order to inform the human user about certain circumstances or situations. The application software on the node needs a corresponding service.
- Display Services: Sometimes it might be necessary to inform the user by displaying figures or plain text. The node has to be able to operate a display and to show information which has been generated by the application module on the node.

All these services and some more which are necessary for other applications have to be defined in an API. Without this interface the implementation of sensor networks in practical applications might take a very long time. This issue should be addressed by standardisation activities during the next years.

3.3 Functional Architectures of Sensor Networks

How theses functions or services are distributed to different sensor nodes is defined by the application. Today there is no generic architecture in terms of functionalities. The following table gives an example and shows how services or functions are distributed to nodes in case of the integrity monitoring system which has been described in chapter 2.2.4. The columns represent the different objects respectively the nodes which are attached to these objects. The lines represent the different functions or services (coming from the previous chapter). If one cell of the resulting matrix is grey the corresponding service has to be implemented on the corresponding node.

Service or function	Product	Pallet	Container	Anchor
Application specific services				
Long range communication			■	
Short range communication	■	■		■
Installation services	■	■	■	■
Security services	■	■	■	
Data storage services	■	■	■	■
Data processing services	■	■	■	
Control services				
Linkage services	■	■	■	
Orientation detection services				
Self localisation service		■	■	
Neighbourhood monitoring	■	■	■	
Sensing service	■			
Identification service	■	■	■	■
Data entry service				
Indication service	■	■	■	
Display service				
Network function				
Clock master		■	■	
Gateway to backend network			■	■
Anchor services				■
Network router	■	■	■	

Table 2: Distribution of services and functions in case of a sensor network based supply chain integrity system

The example makes quite clear that it won't be easy define a generic architecture which meets all imaginable sensor network applications. In order to identify generic rules for the distribution of functions all applications which have been mentioned in chapter 2.2 and maybe some more have to be analysed. Whether it could be done without a tremendous effort should or could be discussed during the meeting in Shanghai.

4 Interfaces and Data Types to be handled by Sensor Networks

Like RFID systems a sensor network based application is or has to be embedded into an organisation. The organisation could be a company, a supply chain or a network of different companies working together. A kind of »middleware« which connects the gateway node of the sensor network to the organisation's process- and IT-landscape is needed. In principle this middleware fulfils the same functions a RFID-middleware does in a RFID-based information system. Hardware abstraction, data aggregation, device management, event management etc. are the most important. Due to the broader variety of functions of a

sensor node the middleware for sensor networks will be much more complex than the type of middleware which is currently in use for integration of RFID-systems into companies. The following figure shows the complete system on a relatively abstract level.

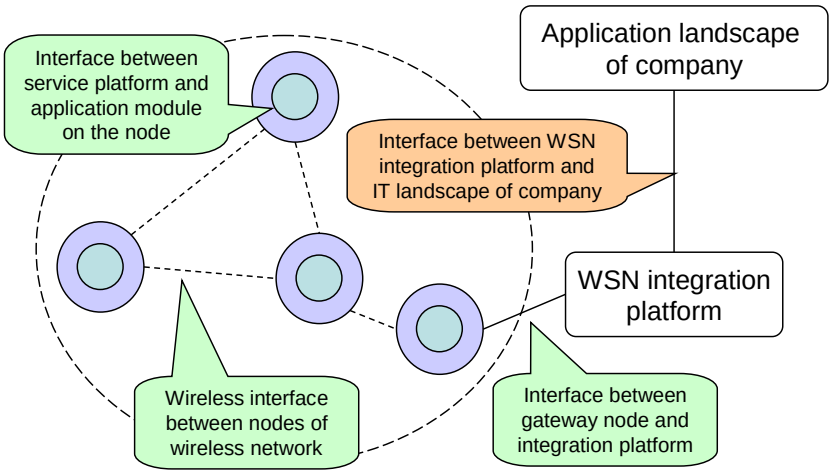

Figure 6: Integrated sensor network-based information systems

At least the following interfaces have to be standardized:

- The interface between the node hardware and the application module which is installed on the node (compare the services that have been defined in 3.2.2).
- The wireless interface between nodes of the wireless network (here the routing protocol as well as the communication protocol has to be addressed).
- The interface between the gateway node and the integration platform (the reader protocols which have been developed by GS1 and EPC global for RFID systems have to be taken into account here).
- The interface between the WSN-middleware (wireless sensor network) and the IT-landscape of the organisation (here again EPCglobal and GS1 have done some preliminary work for RFID-systems).

Data types which have to be handled at these interfaces are:

- Identification number of node.
- Sensor data, position and context information.
- Business logic or business rules (in form of software).
- Private or personal information.
- Configuration data and network management information.

If more details are needed for standardisation activities applications have to be analysed more comprehensively.

5 Sensor Network Protocols

5.1 Standards and Application Requirements

Today two different types of protocols are used in sensor network applications:

- Standard or quasi-standard protocols like Zigbee, Bluetooth, WLAN (for high end applications) or TinyOS.
- Whole bunch of proprietary protocols like »Slotted MAC« of Fraunhofer IIS in Nuremberg and others.

The problem is that requirements of the more challenging applications can often not be met using existing standards. Due to that fact the number of proprietary and highly application-specific protocols is growing.

5.2 Reducing the Latency Time in a Network as one of the major Problems

A good example is the theft prevention system which has been introduced in chapter 2.2.1 and which is currently developed by a group of Fraunhofer-Institutes in Germany. Here a sensor node in form of a thin smart card with more than three month lifetime without maintenance is needed. For the whole network less than five seconds latency time in a highly dynamic network-environment are required. With existing standards these requirements can not be met. The following figure helps to explain the problem. It shows the tree structure of communication which is typical for sensor networks and also used for the theft prevention system.

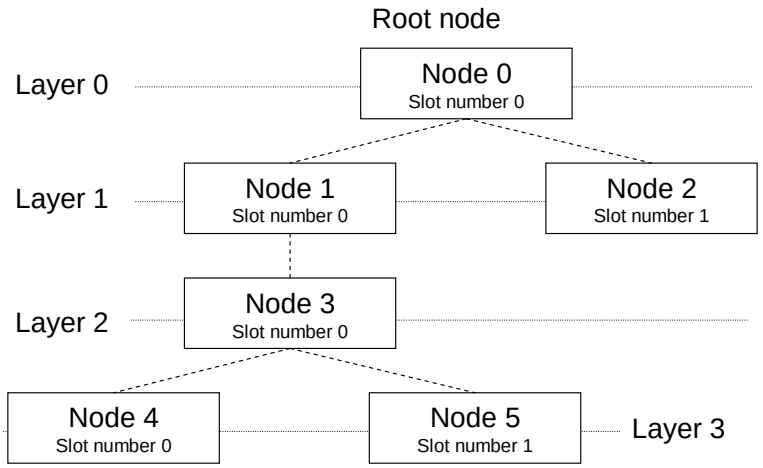

Figure 7: Typical tree structure of communication links in a wireless sensor network.

The problem is the latency time between the generation of an alarm message on a node and the corresponding entry in a central data base. With today's sensor network products five seconds are not possible due to the special characteristics of existing standards. The situation becomes critical when an alarm is generated on one of the lower network levels (many hops to root) and when many items with sensor nodes are on the pallet (many layers). In that case a thief has enough time to remove himself from the location where the criminal act took place. A lot of money might be lost.

Therefore a special problem solution had to be developed in case of the theft prevention system. The solution is a proprietary protocol which combines the efficiency of Time Division Multiple Access as well as the flexibility and scalability of other competing protocols. Latency time can be reduced by a smart configuration of time slots.

5.3 Designing a wireless Network Protocol understood as a »Trade-off« Process

But latency time is not the only problem. The following considerations should make absolutely clear that designing a sensor network could be and normally is a serious challenge. Main targets of a design process are:

- Low energy consumption (lifecycle time) of the nodes.
- Short latency time (data extraction) of the network.
- High data throughput (sensor information) on the communication links.
- High scalability (number of objects) of the total system.

The real challenge is that there is a conflict if all targets should be reached equally. The following figure helps to explain this issue.

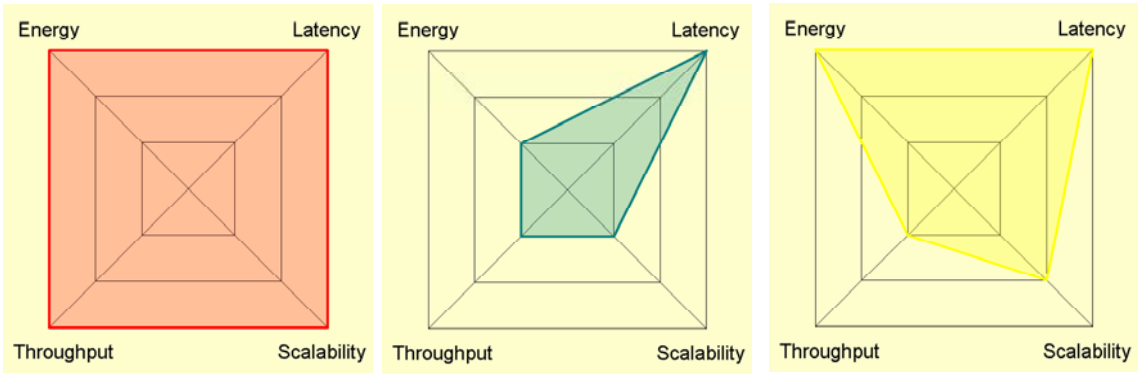

Figure 8: Trade-off between different targets during the process of designing a wireless sensor network protocol

It is very easy to design a protocol which delivers a short latency time when throughput, energy consumption and scalability are not really important for the application ((b) in Figure 8). It is nearly impossible to design a protocol when energy consumption and latency time should be as low and throughput and scalability as high as possible ((a) in Figure 8). All other alternative combinations between these two extremes cause at least some difficulties ((c) in Figure 8).

This trade-off problem might be the reason why so many researchers and product developers try to create their own proprietary protocols. From a standardisation point of view this is a critical situation which has to be addressed within the standardisation activities to come.

6 Concluding Remarks on Standardisation Requirements for Sensor Networks

Following the line of thinking which has presented on the last twenty pages there are at least a few issues which should be taken into account during a standardisation process:

- There is a large variety of different applications of wireless sensor networks in different areas! Due to unique requirement profiles a generic standardisation approach »one size fits all« doesn't seem to be possible.
- A solution might be the identification and description of different application classes. Standards could then be developed for each class.
- Wireless sensor networks differ heavily from other existing networks. It will therefore be difficult to transfer elements of existing standards. Only in exceptional cases such a transfer might be possible.
- Application modules require a lot of different services to be supported by the sensor node. In order to push the implementation of the technology all these services need to be identified, described and standardized. An API is needed not only between »middleware« and IT-backend of a company but also between hardware and application software modules on the nodes.
- There is no generic system architecture in terms of functionalities. The basic architecture as well as the distribution of system functions to nodes and IT-backend depend on specific requirements of a given application. Again clusters or classes of similar applications could be identified.
- Exactly the same is true for the routing and communication protocols. Energy efficiency which is needed for most applications requires a specific adaptation of existing protocols to the application which has to be supported by the sensor network.

– And last but not least: Sensor networks will operate in the same environments like RFID-systems. Therefore standards have to be compatible. The standardisation bodies and working groups that focus on RFID and sensor network technology have to cooperate.