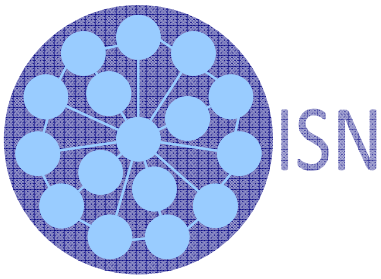

Deliverable D1.1 – Work in progress (pending contribution from MTP and Edosoft)

State-of-the-art: communication, technology, interoperability

Version: 0.3 (October 15, 2011)

Edited by: Walter Colitti (VUB)

Contributions by: Kris Steenhaut (VUB), Nicolas Gueuning (Freemind), Lisiane Goffaux (Freemind)

ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

Project Data

Acronym: ISN

Name: Interoperable Sensor Networks

ITEA number: 09034

Consortium:

- Vrije Universiteit Brussel
- Freemind
- MTP
- Edosoft
- MAIS

Document data:

Doc name: State-of-the-art: communication, technology, interoperability

Doc version: 0.3

Doc type:

Version	Date	Remarks
0.1	October 1, 2011	First draft
0.2	October 10, 2011	Minor modifications
0.3	October 15, 2011	Preliminary version

Contents

1 Introduction

This document provides a study on the emerging standards used in Wireless Sensor Networks (WSN). The standards evaluated are ZigBee, 6LoWPAN and WirelessHART. For each standard we discuss the main functionalities (Section 2), the compliance and certification process (Section 3), the possible hardware and software solutions to equip the ISN gateway with the related technology (Section 4) and the availability of sensors (Section 5).

2 WSN standards functionalities

2.1 ZigBee

ZigBee is a proprietary specification for wireless communication between smart objects based on specific IEEE 802.15.4 radio link layer. The ZigBee specification is owned by the ZigBee Alliance. For non commercial projects, the ZigBee Alliance provides the specification for download from their website. For commercial projects, a membership in the ZigBee Alliance is required.

There are four versions of the ZigBee specifications: ZigBee 2004, ZigBee 2006, ZigBee 2007 and ZigBee Pro. The 2004 and 2006 versions are considered deprecated and are not used in new products. ZigBee 2007 is currently the most used version of the specification. It adds a number of features such as support for packet fragmentation and the ability to dynamically switch physical radio channels. ZigBee Pro increases the amount of devices in each network from 31,101 to 65,540 and add a number of network mechanisms such as multicasting and source routing.

ZigBee is based on the IEEE 802.15.4 standard and does not provide any alternative as underlying radios. The ZigBee protocols are defined around the concepts and addressing modes provided by the underlying IEEE 802.15.4 radio, making it difficult to adapt the ZigBee protocols to other radios.

ZigBee defines three device roles:

- **ZigBee Coordinator (ZC)**. It coordinates the actions of the network as a whole and it is responsible for bootstrapping the network. A ZigBee network can contain only one ZC.
- **ZigBee Router (ZR)**. The ZRs build a network between themselves through which packets are exchanged.
- **ZigBee End Device (ZED)**. The ZEDs are end devices logically attached to a ZR. ZEDs communicate only with their ZR, but cannot communicate between each other.

ZCs and ZRs have higher power requirements then ZEDs and cannot be battery-powered. The ZED has lower power requirements and achieves a long lifetime on batteries. With respect to IEEE 8021.4.4, ZC and ZR are Fully Functional Devices (FFDs), whereas ZEDs are Reduced Function Devices (RFDs).

ZEDs are off most of the time, therefore they are not able to receive any network traffic sent to them. They periodically wake up and check for messages at the ZR they are associated with. The ZR buffers

data sent to their associated ZED nodesand send these data whenever they receive a poll request from a ZED. The wek-up schedule for ZED is defined bythe application developer, not by the ZigBee specification. The number of ZEDs associated with a ZR is limited. In the ZigBee 2007 specification, a ZR can handle a maximum of 14 ZEDs.

As illustrated in Figure 1, the ZigBee protocol stack is composed of four main layers: the physical (PHY) layer, the Medium Access Control (MAC) layer, the network (NWK) layer, and the application (APL) layer. In addition, ZigBee provides security functionality across layers. The two lower layers of the ZigBee protocol stack are defined by the IEEE 802.15.4 standard, while the rest of the stack is defined by the ZigBee specification.

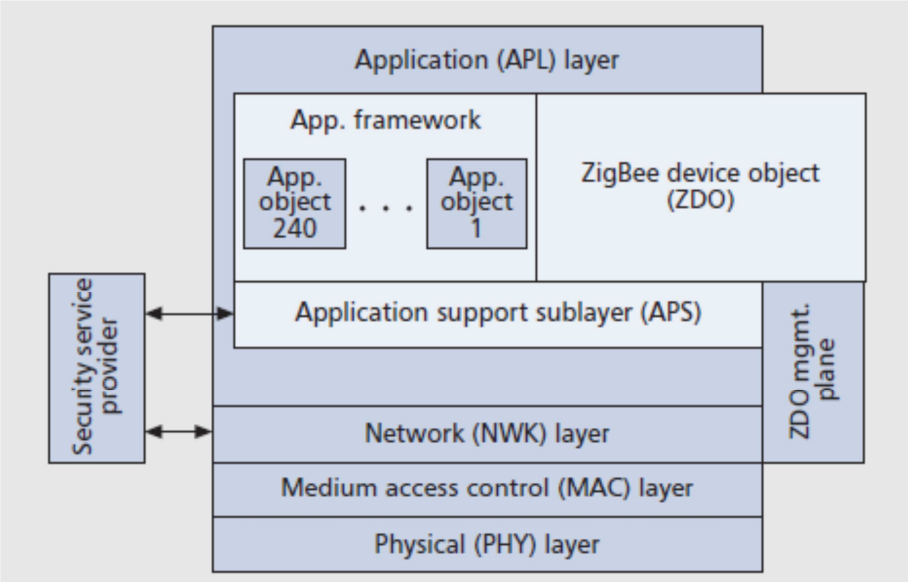

Figure 1. ZigBee protocol stack.

The initial version of IEEE 802.15.4, on which ZigBee is based, operates in the 868 MHz, 915 MHz, and 2.4 GHz bands, which are available in Europe, North America and worldwide, respectively. The data rates are 20 kb/s, 40 kb/s, and 250 kb/s, respectively. Binary phase shift keying (BPSK) is used in the first two bands and orthogonal-quadrature phase shift keying (O-QPSK) is used for the 2.4 GHz signals. These communication mechanisms are combined with direct sequence spread spectrum (DSSS).

The ZigBee NWK layer specifically supports addressing and routing for the tree and mesh topologies. The tree topology, which is adequate for data collection, is rooted at the ZigBee coordinator. This scheme includes a mechanism for address assignment, which also facilitates multihop data delivery. In a mesh topology, routes are created on demand and are maintained using a set of mechanisms based on the Ad hoc On-demand Distance Vector (AODV) routing protocol. This solution is used for arbitrary point-to-point traffic. The ZigBee PRO solution also offers many-to-one routing for communication between several devices and a central controller or sink node. This node may reply back to the devices using source routing. Only ZigBee coordinators and routers participate in routing operations.

2.2 6LowPAN

6LowPAN is the acronym for *IPv6 over low-power personal area networks*. The concept behind 6LowPAN is to bring the Internet Protocol (IP) directly into small, low-cost sensor devices. Since there are not enough addresses in the current IPv4, 6LowPAN starts from the premise of IPv6, with the aim of giving an address to every device.

6LowPAN has been standardized by the Internet Engineering Task Force (IETF). In particular the IETF 6LowPAN Working Group (WG) has defined the frame format and several mechanisms needed for the transmission of IPv6 packets on top of IEEE 802.15.4 networks. These networks are referred to as LoWPANs.

The use of IP in sensor networks is being promoted by the recently founded IP for Smart Objects (IPSO) Alliance.

The 6LowPAN architecture is illustrated in Figure 2

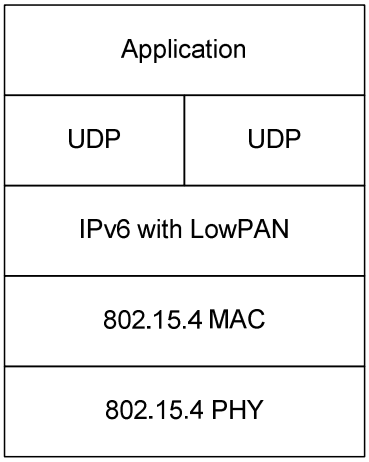

Figure 2. 6LowPAN architecture

The mechanisms offered by 6LoWPAN are:

- **Fragmentation**. IPv6 mandates support for 1280-byte packets but the maximum IEEE 802.15.4 frame size is 127 bytes
- **Header compression**. A common 40-byte IPv6 header can be compressed to a 2-byte header.
- **IPv6 address auto-configuration**.
- **IPv6 neighbor discovery.**

The stack specifies UDP and not TCP as transport, further limiting any unnecessary clutter in the packets. The result is a very compact stack, which is significantly smaller than a ZigBee mesh stack.

Since a LoWPAN is organized in a mesh topology, a routing protocol is needed. Two schemes are envisaged for routing in LoWPANs: *mesh under* and *route over*. In mesh under Figure 3.a), routing is performed below IP using IEEE 802.15.4 addresses. In this configuration the whole LoWPAN appears as a single IP link. In route over Figure 3.b), every radio hop is equivalent to an IP hop, and routing occurs at the IP layer.

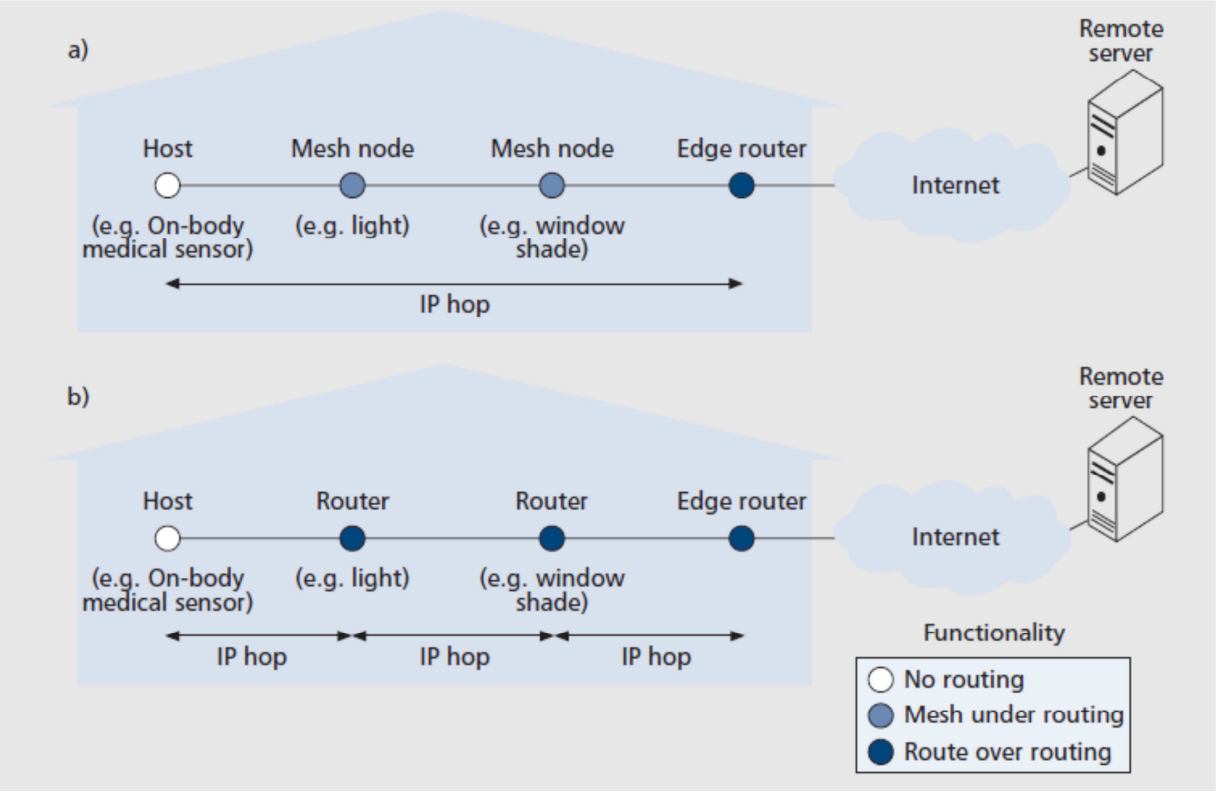

Figure 3. 6LowPAN routing techniques.

In 2008, IETF formed a new Working Group (WG) called Routing Over Low-power and Lossy Networks (ROLL). The objective of the ROLL Working Group was to specify routing solutions for Low-power and Lossy Networks (LLNs). The first objectives of the group were to produce a set of routing requirements, determine whether or not existing IETF routing protocols would satisfy the requirements, and establish a routing security framework and define new routing metrics for routing in LLNs. The WG quickly converged on the conclusion that none of the existing routing protocols would satisfy the requirements for LLNs. Therefore ROLL was re-charted to design a new routing protocol called Routing Protocol Low-power and Lossy Networks (RPL). RPL maintains directed acyclic graphs (DAGs), which may be rooted at sink nodes, and naturally supports multipoint-to-sink and sink-to-multipoint communications. Point-to-point communications are also supported, but routes between arbitrary nodes may not be optimal, since they are constrained to the DAG structures.

6LowPAN is being developed by IETF as an open standard. It is still in its early days, but is attracting considerable interest. The motivation is that it promises to make it very simple to extend existing IP networks to individual sensor nodes. It is creating a lot of interest within the smart energy and smart grid movement, where IP connectivity is seen by the National Institute of Standards and Technology as an important advantage. It is not coincidental that the next release of ZigBee Smart Energy profile includes IP connectivity.

2.3 WirelessHART

Highway Addressable Remote Transducer (HART) is a digital protocol for two-way communication between a host application and smart field instruments, providing access to diagnostics, configuration and process data. Traditionally, HART specified a physical layer which used frequency-shift keying (FSK) superimposed on the analog control signal (4-20 mA).

The HART protocol operates in a master-slave fashion. All communication is initiated by the master. A master can either be a control station or an operating device. There can be a maximum of two masters, primary master — normally the control system — and secondary master — a handheld terminal or a laptop. Slaves (e.g. HART field device) respond only to command messages from a master. After the completion of a transaction the master will wait for a fixed time before sending another command. This enables the other master to break in so that two masters can take turns communicating with the field devices.

HART devices support both long (5 byte) or short (1 byte) addresses enabling the HART protocol to support point-to-point and multi-dropped communication with field devices. When using short addresses up to 64 slave devices may be multi-dropped on one communication link. When using long addresses the number of multi-dropped devices is more or less unlimited.

As of version 7, HART also incorporates an IEEE 802.15.4-based wireless mesh network as an option for the physical layer. This is commonly referred to as WirelessHART.

WirelessHART has been developed after ZigBee had been tested in industrial environments and it revealed to have some deficiencies. The industry demanded secure and reliable communication, but static and multi-path fading sometimes blocked ZigBee due to its use of one static channel.

WirelessHART is designed based on a set of fundamental requirements: it must be simple (e.g., easy to use and deploy), self-organizing and self-healing, flexible (e.g., support different applications), scalable (i.e., fit both small and large plants), reliable, secure, and support existing HART technology (e.g., HART commands, configuration tools, etc).

Figure 4 shows the protocol stack of the HART protocol and its wireless version WirelessHART. WirelessHART is based on the PHY layer specified in the IEEE 802.15.4-2006 standard, but specifies new Data-link (including MAC), Network, Transport, and Application layers.

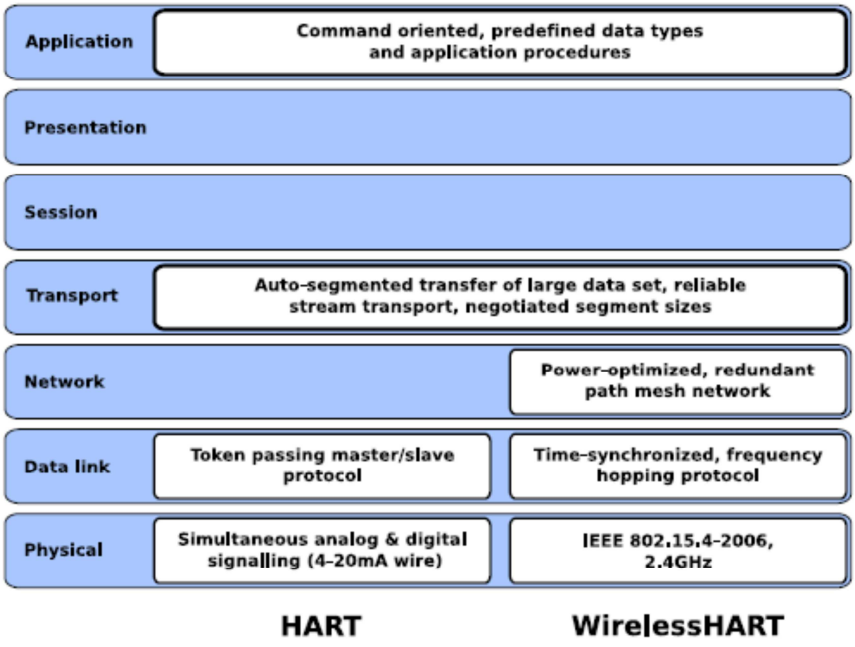

Figure 4. HART and WirelessHART protocol stacks.

WirelessHART is a Time Division Multiple Access (TDMA) based network. All devices are time synchronized and communicate in pre-scheduled fixed length time-slots. TDMA minimizes collisions and reduces the power consumption of the devices.

WirelessHART uses several mechanisms in order to successfully coexist in the shared 2.4GHz Industrial, Scientific and Medical (ISM) band: Frequency Hopping Spread Spectrum (FHSS) allows WirelessHART to hop across the 16 channels defined in the IEEE802.15.4 standard in order to avoid interference. Clear Channel Assessment (CCA) is an optional feature that can be performed before transmitting a message, the transmit power level is configurable, and a mechanism to disallow the use of certain channels, called Blacklisting, is available. All of these features also ensure WirelessHART does not interfere with other co-existing wireless systems that have real-time constraints.

All WirelessHART devices must have routing capability, i.e., there are no reduced function devices like in Zig- Bee. Since all devices can be treated equally in terms of networking capability, installation, formation, and expansion of a WirelessHART network becomes simple as the network is self-organizing.

WirelessHART forms mesh topology networks (star networks are also possible, but not recommended), providing redundant paths which allows messages to be routed around physical obstacles, broken links, and interference. Two different mechanisms are provided for message routing: Graph routing and Source routing. Graph routing uses pre-determined paths to route a message from a source to a destination device.

To utilize path redundancy, a graph route consists of several different paths between the source and destination devices. This is the preferred way of routing messages both up- and downstream in a

WirelessHART network. Source routing uses ad-hoc created routes for the messages without providing any path diversity. Source routing is therefore only intended for network diagnostics, not process related messages.

Figure 5 shows the different Network device types that comprise a WirelessHART network.

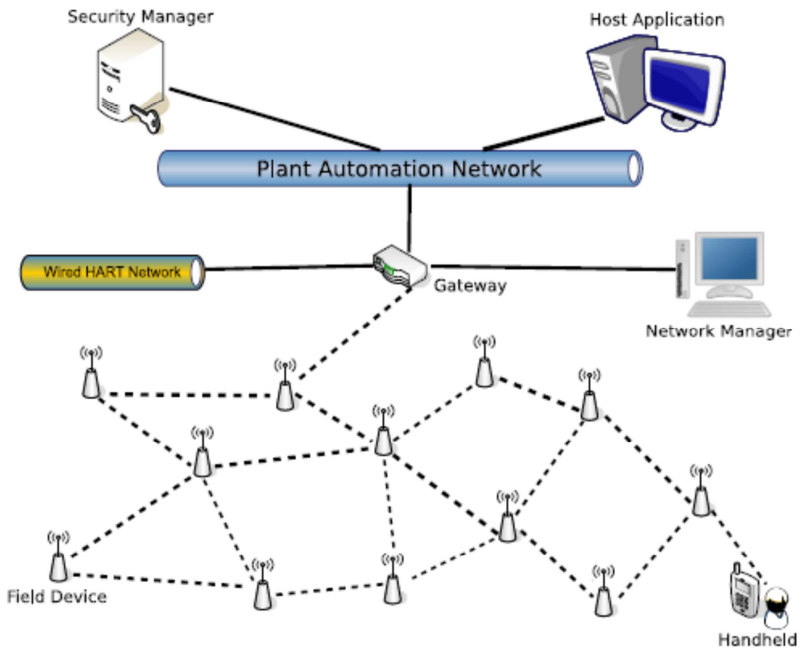

Figure 5. WirelessHART devices and connection to host system.

As illustrated in Figure 5, the devices in a WirelessHART network are the following:

- **Field devices**. They are connected to the process, e.g., sensors and actuators.
- **Router devices**. They are not connected to the process, i.e., lacks the sensor or actuator, instead only having communication functionality. Router devices are not required by the standard, but will be useful in cases where wireless connectivity needs to be improved.
- **Adapter devices**. They connect wired HART devices to the WirelessHART network, e.g., legacy HART or nonwireless devices. One adapter device can provide wireless network access for more than one wired device.
- **Handheld devices**. They are used for the installation, configuration, monitoring, and maintenance of all kinds of WirelessHART devices.
- **Gateway device**. It connects the WirelessHART network to the plant automation system (host). It provides the host system with access to WirelessHART Network devices and will, if required, translate between different protocols.

- **Network Manager**. It is the centralized "brain" of the WirelessHART network. Its responsibility is to manage everything related to the wireless network, e.g. forming the network, scheduling resources, network path configuration and reconfiguration, etc. Only one active Network manager can exist per WirelessHART network, with the possibility to have a backup manager to take over if the active one fails.

3 Compliance and certification

3.1 ZigBee

The ZigBee Alliance has 2 different certification programs: one for platforms and one for end products. The ZigBe, as illustrated in Figure 6.

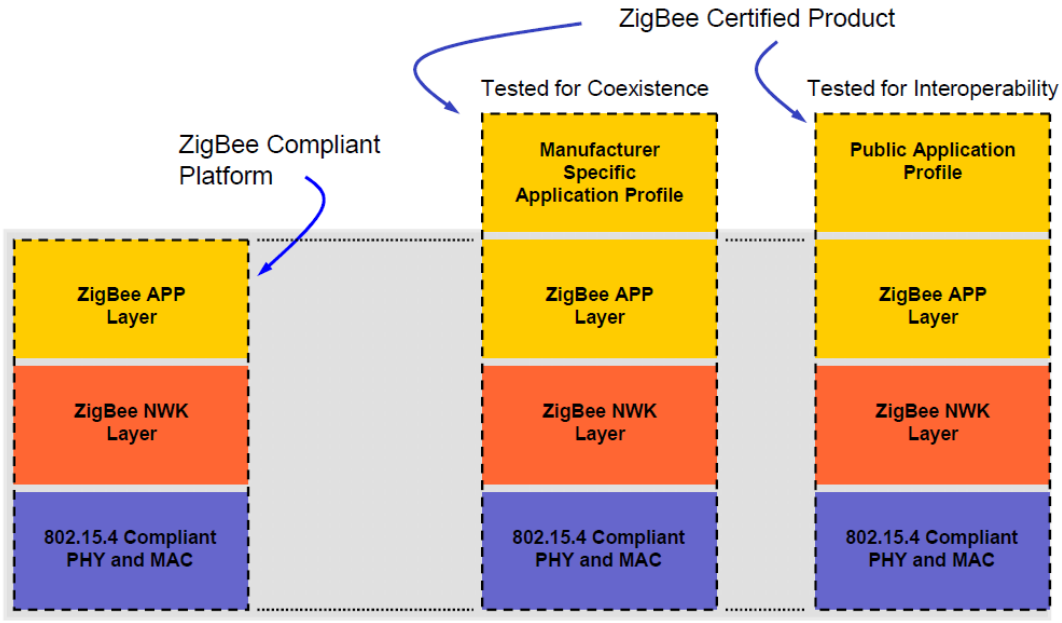

Figure 6. ZigBee compliant platform and Zigbee certified products.

The ZigBee compliant platform program applies to platform providers and must be obtained for each instantiation of a platform. Compliant platforms are the building blocks of the certified end products. In other words, a product can obtain the ZigBee end product certification only if it is built using a compliant platform.

The ZigBee certified product program applies to end products which are also tested at the level of the application profile. The ZigBee Alliance differentiates two types of end product:

- **End products with manufacturer specific profile**. Although the manufacturer needs to applies for obtaining a specific profile from the ZigBee Alliance, this profile is not necessarily made

public by the vendor. This implies that the product is not interoperable at the level of the application profile with products of other manufacturers. In this case the test is intended to ensure the coexistence, meaning that such products coexist successfully with products and networks certified by the ZigBee Alliance and do not adversely impact the operation of other ZigBee certified products and networks.

- **End products with public application profile**. In this case the product is built with a public application profile**,** fully defined and ratified by the ZigBee Alliance through the Application Framework Working Group (AFG) and a Profile Task Groups (PTG). For such products the test is intended to ensure interoperability with other vendors who use the same public profile. After successful completion of the program, the end product may bear the ZigBee Alliance Logo, per the ZigBee Trademarks, Designations and Logos Policy.

The basis for a ZigBee Certified Product is a ZigBee Compliant Platform. Hence, a manufacturer whose final goal is certification must use a compliant platform. He needs to join the ZigBee Alliance to submit a product for testing and may choose between a full or adopter membership levels. Adopter Members are required to pay an additional per-product fee to the ZigBee Alliance for product certification, while full members don't have per-product fee. In addition, the difference between full and adopter memberships is that the former later has an additional administrative fee.

3.2 6LoWPAN

6LowPAN has a less complicated interoperability test program. The test program is the same as the general IPv6 interoperability test program, called *IPv6 Ready Logo Program*. The IPv6 Ready Logo Committee mission is to define the test specifications for IPv6 conformance and interoperability testing, to provide access to self-test tools and to deliver the IPv6 Ready Logo. The Key objectives and benefits of the IPv6 Ready Logo Program are to:

- Verify protocol implementation and validate interoperability of IPv6 products.
- Provide access to free self-testing tools.
- Provide IPv6 Ready Logo testing laboratories across the globe dedicated to provide testing assistance or services.

In order to sell IPv6 based products there is no need to be member of any alliance.

3.3 WirelessHART

In 2009, the HART Communication Foundation board of directors voted to require independent testing in order to register a HART device, wired or wireless. This testing is an addition to the testing required of the manufacturer prior to registration testing.

In order to verify compliance with the HART Protocol Specification, wired and wireless devices that claim to be "HART Registered" must pass the HART Device Registration Program conducted by the Foundation. HART registration is available for all process measurement devices, interfaces such as modems,

multiplexers and I/O systems, HART masters including systems and handhelds and Device Description (EDD)-enabled host applications.

Devices that pass the tests earn the "HART Registered" designation, are issued a Certificate of Registration, and are allowed to display the "HART Registered" mark. The Foundation tests and registers all HART-enabled devices and all HART Device Descriptions to assure that every device submitted, whether wired and wireless, is interoperable across platforms.

Before the Foundation gets the device to test, the manufacturer must do the testing itself—and provide the data to the Foundation, as well as a device for testing. The list of requirements is long, and the procedure is rigorous. Both good and bad data are sent to see that the device responds appropriately.

4 HW/SW solutions for gateway

This section provides a list of the possible available solutions to equip the ISN gateway with standard WN technology. For each vendor we list the hardware solution (radio chip and micro controller) and the software solution (certified protocol stack). Since the final choice will have to be done after testing the technology with evaluation kits, we list only the vendors providing evaluation kits. We will also mention the vendor's place of origin.

4.1 ZigBee

4.1.1 Texas Instruments

Microchip: cc2531 (http://focus.ti.com/docs/prod/folders/print/cc2531.html)

ZigBee stack: Z-Stack (http://focus.ti.com/docs/toolsw/folders/print/z-stack.html?DCMP=HPA_RFIC_General&HQS=Other+OT+z-stack), provided by the same provider

Country: USA and worldwide

Evaluation kit: http://focus.ti.com/docs/toolsw/folders/print/cc2531emk.html

4.1.2 Jennic

Microchip: JN5148 or JN5148 + co-processor (http://www.jennic.com/products/wireless_microcontrollers/jn5148)

ZigBee stack: Jennic ZigBee protocol stack (http://www.jennic.com/products/protocol_stacks/zigbee_pro)

Country: UK

Evaluation kit: http://www.jennic.com/products/development_kits/

4.1.3 Ember

Microchip: EM357 (http://www.embercorp.com/products_zigbee_chips_e300series.html)

ZigBee stack: Ember ZNETPRO (http://www.embercorp.com/products_zigbee_software.html)

Country: USA with office in UK

Evaluation kit: http://www.embercorp.com/products_zigbee_development_tools_kits.html

4.1.4 Microchip

Microchip: MRF24J40 + PIC18
http://www.microchip.com/wwwproducts/Devices.aspx?dDocName=en027752

ZigBee stack:
http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=2113&param=en520422

Country: USA

Evaluation kit:
http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1406&dDocName=en021925

4.1.5 Freescale

Microchip: MC13224V
(http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=MC13224V)

ZigBee stack: http://www.freescale.com/webapp/sps/site/homepage.jsp?code=802-15-4_HOME

Country: USA

Evaluation kit: http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=1321xEVK

4.2 6LowPAN

4.2.1 Jennic

Microchip: JN5148 or JN5148 + co-processor
(http://www.jennic.com/products/wireless_microcontrollers/jn5148)

6LowPAN stack: Jennic 6LowPAN protocol stack
(http://www.jennic.com/products/protocol_stacks/6lowpan)

Country: UK

Evaluation kit: http://www.jennic.com/products/development_kits/

4.2.2 CISCO/Archrock

Microchip: PhyNet Engine (No website available)

6LowPAN stack: provided by the same vendor (No website available)

Country: USA and worldwide

Evaluation kit: (No website available)

4.2.3 Texas Instruments

Microchip: cc2530 (http://focus.ti.com/docs/prod/folders/print/cc2530.html)

6LowPAN stack: Sold by Sensinode, Finland (http://www.sensinode.com/EN/products/software.html)

Country: USA and worldwide

Evaluation kit: http://focus.ti.com/docs/toolsw/folders/print/cc2530dk.html

4.3 WirelessHART

4.3.1 DUST Networks

Microchip: DN2510 (http://www.dustnetworks.com/products/SmartMesh_IA-510_I/DN2510)

WirelessHART stack: Integrated

Country: USA

Evaluation kit:
http://www.dustnetworks.com/cms/sites/default/files/0150017rev8IA510HSmartStartKit.pdf

4.3.2 Freescale

Microchip: MC13224 (same as ZigBee)

WirelessHART stack: Licence bought from Software Technologies Group, USA (http://www.stg.com/wireless/WiHART.html)

Country: USA

Evaluation kit: To come

4.3.3 RFM

Microchip: XDM2510H (http://www.rfm.com/products/spec_sheet.php?record=XDM2510H)

WirelessHART stack: Integrated from DUST networks

Country: USA and worldwide

Evaluation kit: http://www.rfm.com/products/spec_sheet.php?record=XDM2510HDK

5 Sensor availability

This section provides a list of the vendors of sensors solutions for the three standards studied in this report.

5.1 ZigBee Home Automation Certified Products

5.1.1 Adhoco, Switzerland - http://www.adhoco.com/

- Wireless presence and illuminance sensor

- Mini meteo station (outside air temperature, air humidity, solar irradiation and wind speed)
- Combined light on/off actuator and light switch sensor
- Wireless temperature and humidity sensor with setpoint input
- Vast range of actuators for HA

5.1.2 Alertme, UK - http://www.alertme.com/

- Door sensor
- Occupancy sensor
- ON/OFF switch (used as panic button)

5.1.3 Black&Decker, USA - http://www.blackanddecker.com/

- Smart Lock (remotely controls door)

5.1.4 Centralite, USA - http://www.centralite.com/

- Dimmer and on/off light

5.1.5 Simplehomenet, USA - http://www.simplehomenet.com/

- Load Controller high current appliances such as air conditioners, water heaters, pool pumps

5.1.6 Develco, USA - http://www.develco.com/

- ON/Off relay for configuring home appliacnes (also in wall plug version)

5.2 ZigBee Smart Energy Certified Products

5.2.1 Simplehomenet, USA - http://www.simplehomenet.com/

- Load controller for control of pool pumps, water heaters, HVAC and other high-power loads
- Wall plug load controller for control of appliances and lighting.

5.2.2 Comverge, USA - http://www.comverge.com/

- Meter compatible with popular air conditioning units, water heaters, pool pumps, and other auxiliary appliances

5.2.3 Elster, USA - http://www.elster.com/

- Smart meter that supports emerging needs of smart grid initiatives, such as enhanced memory, greater security, and remote upgradeability.

5.2.4 Plogg, UK - http://www.plogginternational.com/

- Wall plug smart meter

5.2.5 HAI, USA - http://www.homeauto.com/main.asp

- Meter for water heaters, pool pumps, outdoor fountains, lighting.
- Meter for low voltage circuits in outdoor air conditioning units, pool and spa heaters & pumps, generators, and more

5.2.6 Itron, USA - http://www.itron.com/

- Meter for natural gas consumption with two-way communication

5.3 6LowPAN

Although being very promising and future proof, 6LowPAN is still in its infancy. Therefore, there are not yet sensors equipped with this technology. An idea to overcome this problem is to integrate the sensor boards with the hardware and software solutions used for the gateway (see Section 4).

5.4 WirelessHART

There are many WirelessHART certified registered products, such as:

- Oxygen Transmitter
- Dual Input Analyzer
- Pressure Transmitter
- Level Transmitter/Controller

- Gauge Pressure Transmitter
- Absolute Pressure Transmitter
- Buoyancy Level Transmitter

However, the new registration product mentioned in paragraph 3.3 has only been introduced in 2009. Therefore, most of the WirelessHART products at the moment have been registered using the old auto-certified program. Many products are under registration at the moment, but there Is not clear indication about that.

Two vendors have been found that already succeed in the new product registration products:

Emerson, USA - http://www.emerson.com/

- Temperature Transmitter
- Pressure Transmitter

Metroval, Brazil - http://www.metroval.com.br/index.php?menu=1