UNIVERSITY of OULU
OULUN YLIOPISTO

CONTROL ENGINEERING LABORATORY

WIRELESS TECHNOLOGIES IN PROCESS AUTOMATION - REVIEW AND AN APPLICATION EXAMPLE

Marko Paavola

Report A No 33, December 2007

University of Oulu
Control Engineering Laboratory
Report A No 33, December 2007

Wireless Technologies in Process Automation - A Review and an Application Example

Marko Paavola

University of Oulu, Control Engineering Laboratory

Abstract: This literature review studies the wireless technologies, their applications, characteristics, design criteria and requirements for process automation applications, focusing especially on wireless sensor networks (WSN). Additionally, implementation of an application example, wireless monitoring of temperature and pressure of a steam boiler, is also presented.

The review indicates that the wireless automation systems are often hybrid in nature, combining legacy fieldbus systems and heterogeneous networks. The design criteria and requirements for industrial applications are stricter than compared to some other domains, for example environmental monitoring, home and building automation. According to review, wireless technologies provide potential for industrial applications, but additional research may be required on interoperability, reliability, data processing techniques and energy consumption, the last especially from whole system point-of-view.

Keywords: wireless sensor networks, industrial automation

ISBN 978-951-42-8705-3
ISSN 1238-9390

University of Oulu
Control Engineering Laboratory
PL 4300
FIN-90014 University of Oulu

1 INTRODUCTION

The field of wireless communications is diverse and it may be difficult to get a picture of the different technologies utilised in a certain field. In industry, the proposed and already employed technologies vary from short-range personal area networks to cellular networks, and in some cases even global communications via satellite are applied.

Recently, the use of wireless sensor networks (WSN) in industrial automation has gained attention. WSNs are technically a challenging system, requiring expertise from several different disciplines. Therefore, the information about important design criteria is often scattered. Additionally, characteristics for the industrial automation applications are often stricter than the other domains, since the failure of the communication system may lead to loss of production or even lives.

This report attempts first to give a short review about the emerging and already employed wireless technologies in process automation, excluding proprietary solutions provided by different manufacturers. Additionally, some standards and regulations, which may be relevant for wireless applications in the industrial automation, are shortly introduced.

After the technology review, WSN are introduced briefly. Next, industrial applications of WSN and categories of wireless communication are discussed. Finally, some important design criteria in the context of industrial automation applications are presented.

The importance of gaining experience of applying wireless sensor networks to process automation environments has been addressed in the literature. The experience is important, as it can be used to show, as well as to get rid of, the problems in the current technology, and to enable larger variety of applications.

To study the applicability of the wireless sensor network in process monitoring applications, an example application to steam boiler was implemented. This report describes the implementation of wireless monitoring of temperature and pressure in the steam boiler. Finally, some conclusions and future research suggestions are presented.

2 WIRELESS TECHNOLOGIES IN PROCESS AUTOMATION

2.1 Overview

A survey investigated wireless technologies used in industrial automation. The most exploited were Wi-Fi (34%), Radio frequency identification (RFID) (21%), Bluetooth (14%), and ZigBee (6%) (Hoske, 2006). Similar results were presented in (Welander, 2007), though ZigBee had been strengthening its position. Namely, RFID and ZigBee were reported to have highest number of new uses (RFID +17%, ZigBee +16%) (Welander, 2007). The landscape of wireless technologies is presented in Figure 1.

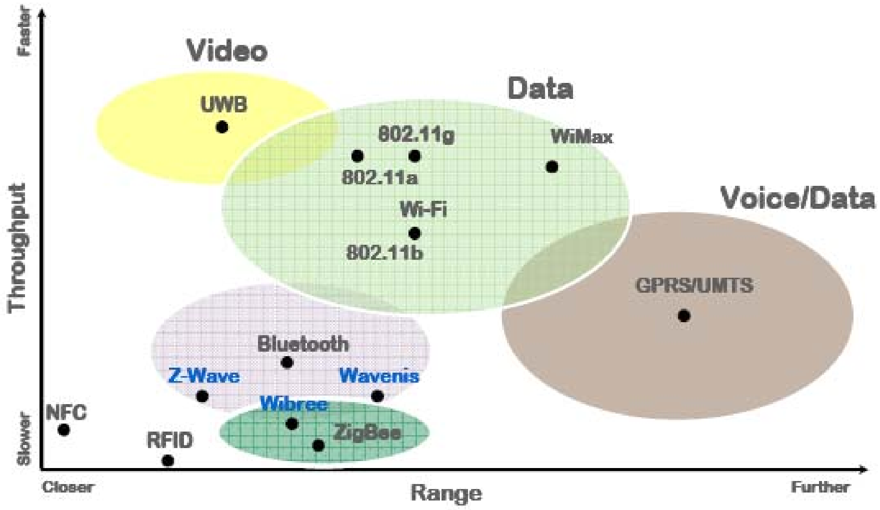


Figure 1. Wireless technologies landscape described in terms of throughput (y-axis) and range (x-axis) (Koumpis, 2006).

Several of the technologies in Figure 1 are applied (or planned to be applied) in process industry (see Section 2). The choice between different (or combination of) technologies is dependent on application: different approach is applicable e.g. to monitor remote tanks and monitoring robotic installations (See APPENDIX 1 for examples). Moreover, adoption of several network technologies in a single environment is becoming more common nowadays (Low et al., 2005). Figure 2 illustrates an example about wireless sensor/actuator network.

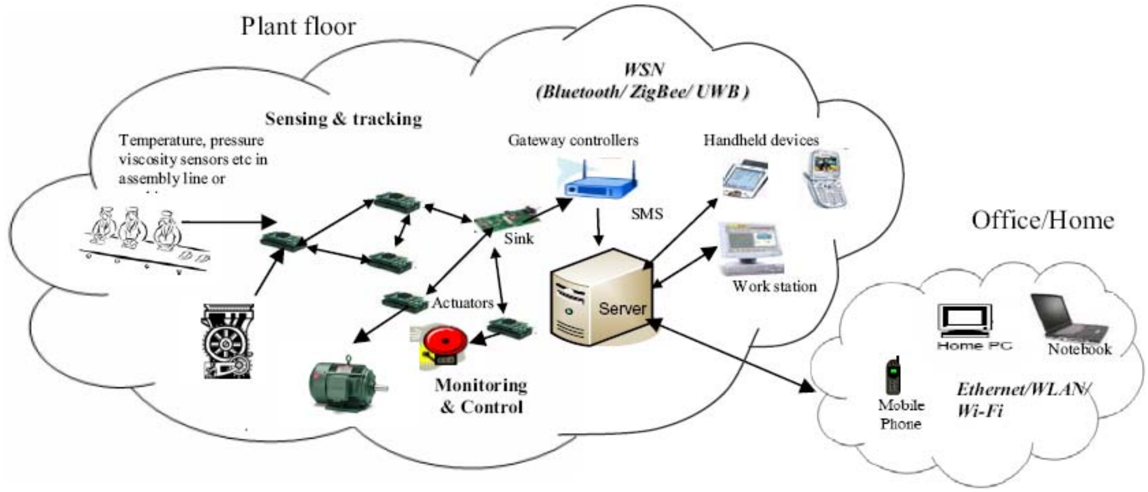


Figure 2. An example about industrial sensor/actuator network combining several network technologies (Low et al., 2005).

Next, the wireless technologies applied in process industry are shortly introduced. Proprietary technologies are excluded, and therefore, Z-Wave and Wavenis mentioned in Figure 2 are not discussed (it should be noted, however, that proprietary technologies may have applications in some cases (Sallinen et al., 2007). After introduction, some of the related standards in industry are presented and finally, a technology roadmap is discussed.

2.2 Wireless Local Area Networks (WLAN, 802.11)

Wireless local area networks (WLAN), or commercially Wireless Fidelity (Wi-Fi), operate at 2.4 GHz or 5 GHz ISM bands and offer speeds up to 54 Mbps. They support two modes: ad-hoc and infrastructure. The ad-hoc mode allows stations to spontaneously form a wireless LAN, in which all stations communicate with each other in peer-to-peer manner. The infrastructure mode, the network has an access point (AP), through which each client station communicates. A typical Wi-Fi AP may have range of 45 m indoors and 90 m outdoors. The properties of the most important 802.11 standards (802.11a, 802.11b, and 802.11g) can be found for example from (Cisco).

In process automation, Wi-Fi Networks can serve as the backbone for data concentration and networking. For example, it can used in conjunction with short-range, low-power devices in a wireless field network to collect data from the gateway further sending it to the control room or other data collection point (Emerson, 2006b).

The advantages of WLAN in process automation include high range, open standards, robustness, cost-effectiveness, easy accessibility to process control by mobile workers and high data transmit rate (Emerson, 2006b). Recently, also the security has increased with two important security enhancements, Wi-Fi Protected Access (WPA) and WPA2, which replace older and less secure technology, Wireless Equivalent Policy (WEP).

Additionally, used in conjunction with for example wireless sensor networks, they provide sufficient bandwidth for supporting multiple gateways. However, WLAN may not be applicable for wireless device-to-device communication because of high power consumption, requiring line power or power over Ethernet (PoE). The expense of providing the power lines may limit the size of the network (Emerson, 2006b). Additionally, WLAN is more designed to high throughput applications for small number of terminals (Dzung et al., 2005), which is quite opposite to some WSN characteristics (see Section 3.1). Figure 3 presents an example of Wi-Fi backbone implementation by Honeywell.

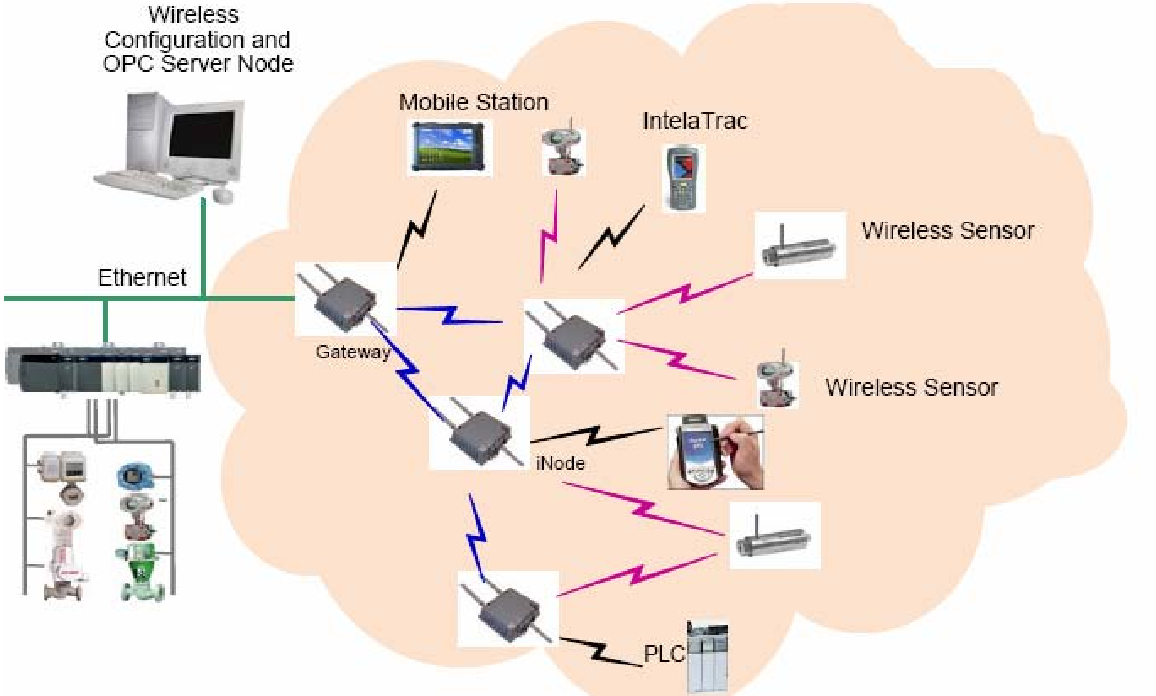


Figure 3. Wi-Fi backbone architecture concept developed by Honeywell (Gonia and Budampati, 2006). Information is transmitted between field equipment (wireless sensors, Programmable Logic Controller (PLC), mobile station, IntelaTrac, mobile phone) and Wi-Fi backbone wirelessly and connected to the whole automation system via gateway (IML Group plc, 2007a).

2.3 Wireless Metropolitan Area Networks (IEEE 802.16, IEEE 802.20)

WiMAX (Worldwide Interoperability for Microwave Access), synonym for IEEE 802.16 standard, is a metropolitan access technique, and its characteristics are long distance transmissions and high data capabilities (Sun et al., 2007). WiMAX coverage can reach up to 50 kilometres and the capacity of network backbone can be increased to 75 Mbps (Cungor and Lambert, 2006). WiMAX not only provides wireless access but may also be used to expand the network access coverage e.g. to remote or suburban areas (Sun et al., 2007).

In industry, WiMAX could serve as the backbone in a hierarchical network strategy, e.g. for ZigBee (see Section 2.4.3) (Cleaveland). In (Cungor and Lambert, 2006), a WiMAX backbone for electric system automation is presented (see Figure 4).

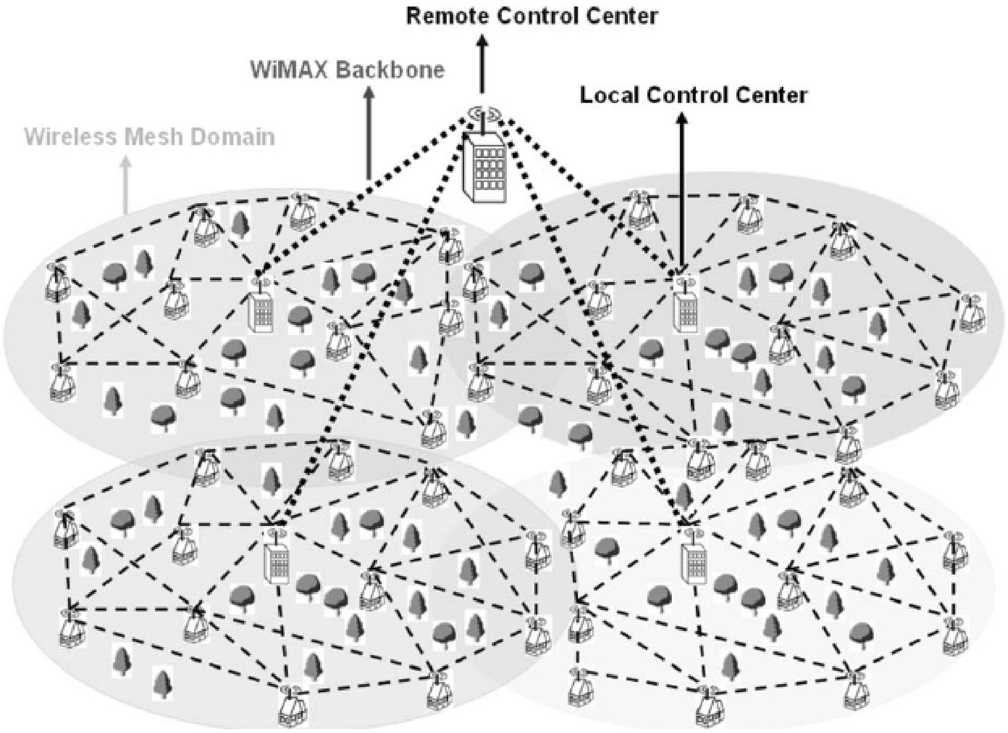


Figure 4. Illustration of hybrid architecture of WiMAX and wireless mesh networks (Cungor and Lambert, 2006).

(Cungor and Lambert, 2006) also discusses several advantages of utilising WiMAX as a part of hybrid architecture in electric system automation, namely: increased reliability, low installation costs, large coverage area and automatic network connectivity. As a challenge for the proposed solution (Cungor and Lambert, 2006) mentions harsh monitoring environments, optimal placement of WiMAX towers, mobility support, integration of heterogeneous networks, scalability, coordinated resource management and security issues.

An emerging standard in WMAN is Mobile Broadband Wireless Access (MBWA), IEEE 802.20. However, according to (VAN, 2005), the standardisation is ongoing and products are not yet available.

2.4 Wireless Personal Area Networks (WPAN)

2.4.1 Bluetooth and Wibree (IEEE 802.15.1)

Bluetooth operates at 2.4 GHz ISM band and employs frequency hopping spread spectrum (FHSS) modulation technique (VAN, 2005). Bluetooth has been considered as one possible alternative for WSN implementation (Aakvaag et al., 2005). However, due to its high complexity and inadequate power characteristics for sensors, the interest towards Bluetooth for WSN applications has decreased (Aakvaag et al., 2005). Additionally, Bluetooth is designed for high throughput applications between small numbers of terminals (Dzung et al., 2005). IEEE 802.15.1 specification covers physical and link layers from Bluetooth 1.1 -specification (VAN, 2005).

Wibree specification is a part of Bluetooth specification as an ultra-low power technology addressing devices with very low battery capacity. This extension to Bluetooth allows for data rates of up to 1 Mbit/second over distances of 5 to 10 meters in the 2.45 GHz band. Though Wibree is similar to Bluetooth and can employ the same chips and antennas, it has some important differences. Wibree does not use frequency hopping to avoid interference, as Bluetooth does. It has a variable-length packet structure, compared to Bluetooth's fixed length. It also employs a different-unspecified-modulation scheme. Additionally, the implementation of the security algorithm (AES) has been taken into account from the start. It has been discussed, that Wibree also may not be applicable to industrial environments due to short range (<10 meters), lack of mesh networking capabilities and limited number of radios in network. (Mannion, 2006)

2.4.2 Ultra-wideband (IEEE 802.15.3)

Ultra-wideband (UWB) is a short-range technology based on transmission of impulses lasting only fractions of nanoseconds emitted in periodic sequences (Hancke and Allen, 2006; Zeng et al., 2006). IEEE 802.15.3 specification defines the physical layer for UWB.

Formerly, the applications of UWB mainly considered multimedia and personal area networking (Porcino and Hirt, 2003), but recently also the industrial applications have gained attention as can be seen from (Hancke and Allen, 2006; van de Kar et al. 2006; Zeng et al., 2006). In (van de Kar et al., 2006), the results of the brainstorming session about UWB use in process industry are presented. UWB was estimated to be very applicable e.g. for automated registration and localization of equipment and persons; the rapid commissioning of the process control equipment (especially in pilot plants); remote control; plant wide communications not related to process control; and secondary sensor & control networks like gauging in tanks (van de Kar et al., 2006). UWB is not seen applicable for communication over longer distances or measuring data from unsafe zone (latter because high peak energy of pulses). Additionally, it should be noted that maximum amount of devices per network, 2 (Kinnunen, 2007), may provide restrictions for utilisation of UWB in some applications.

The advantages of UWB are good localization capabilities (Zeng et al., 2006), possibility to share previously allocated radio frequency bands by hiding signals under noise floor (Hancke and Allen, 2006), ability to transmit high data rates with low power (Hancke and Allen, 2006), good security characteristics due to the unique mode of operation, and ability to cope with multipath environments (Hancke and Allen, 2006). The existing challenges lie e.g. in hardware development, dealing with medium access control (MAC) and multipath interference, and understanding propagation characteristics (Hancke and Allen, 2006).

2.4.3 ZigBee, Wireless Hart, 6loWPAN, (IEEE 802.15.4)

ZigBee

ZigBee aims for cost sensitive, very low-power and low-speed wireless networking, targeting to industrial, home and building automation (Aakvaag et al., 2005). The good characteristics of the ZigBee are extremely low energy consumption and support for several different topologies, which makes it a good candidate for several sensor network applications (Aakvaag et al., 2005). However, it is reported in (Dzung et al., 2005) that ZigBee cannot meet all the requirements for at least some industrial applications. For example, it cannot serve the high number of nodes within the specified cycle time (Dzung et al., 2005). IEEE 802.15.4 standard defines physical and data link layers for ZigBee (VAN, 2005).

Wireless HART

In (IML Group, 2007b) release of the wireless HART specification has been reported. The technology employs 802.15.4-based radio, frequency hopping, redundant data paths, and retry mechanisms. Devices that comply with the wireless HART specification are interoperable and support tools that work with both wired and wireless HART equipment. (IML Group, 2007b)

Wireless HART networks utilize mesh networking, in which each device is able to transmit its own data as well as relay information from other devices in the network. Each field device has two routes to send data to the network gateway; the alternative route is used when the primary route is blocked either physically or by interference. Additionally, a new route is established if a route is seen permanently blocked. The range between devices is approximately 200 meters. (IML Group, 2007b)

The standard uses time division multiple access (TDMA) to schedule transmissions over the network (IML Group, 2007b). In TDMA, a series of timeslots (10 ms for Wireless HART) are used to coordinate transmissions. The media access control (MAC) header is designed to support the co-existence of other networks, such as ZigBee. Wireless HART is aimed for new applications (e.g. for asset monitoring) rather than replacing the wired solutions. (IML Group, 2007b)

6loWPAN

6loWPAN aims for standard Internet Protocol (IP) communication over low-power, wireless 802.15.4 networks utilising Internet Protocol version 6 (IPv6). The advantages of 6loWPAN from the industrial point of view are ability to communicate directly with other IP devices locally or via IP network (e.g. Internet, Ethernet) (Culler and Hui, 2007), existing architecture and security (Culler, 2006), established application level data model and services (e.g. HTTP, HTML, XML) (Culler, 2006), established network management tools (Culler, 2006), transport protocols and existing support for IP option in most industrial wireless standards (Culler, 2006).

2.4.4 Radio Frequency Identification (RFID)

RFID uses a small radio-frequency transponder called an RF tag (Emerson, 2006a). The tag is electronically programmed with unique information, which can be read from a distance (Emerson, 2006a). The RFID operates from frequencies ranging from several hundred kilohertz to tens of gigahertz (Yeager et al., 2006). Typically, the RFID reader transmits the required power and data to the tag (Yeager et al., 2006). There are two types of RFID tags, active and passive (Yeager et al., 2006). Active tags are battery-powered, more expensive, and use higher frequencies, whereas the passive tags use lower frequencies, and do not have the internal power source (Yeager et al., 2006). The reading range is up to 100 meters for active and about 20 meters for passive tags (Yeager et al., 2006).

RFID is used for example in inventory-tracking applications (industrial examples can be found e.g. from (IDG Communications, 2005; King, 2005)). It is also possible to update some types of tags, e.g. as the item progresses down an assembly line (Emerson, 2006a). However, because RFID information is static and must be programmed into the tag it cannot be used directly for the measurement or diagnostic data that is constantly subject to change (Emerson, 2006a).

Future research seeks to further expand the capabilities of RFID technology. One promising area of development is the integration of sensors and dynamic computing power into RFID chips. Advances in integrated circuit (IC) fabrication have reduced the power requirements of microcontrollers to the point that they can operate on the scavenged power of passive RFID tags. Coupled with the breakthroughs in micro-electro-mechanical-systems (MEMS) and IC sensor technology, this may enable wireless, battery-free sensors. (Yeager et al., 2006)

Near field communication (NFC) is a very short-range (max. 20 cm), wireless point-to-point interconnection technology, which has evolved from a combination of earlier RFID contactless identification and interconnection technologies. It is based on inductive coupling and uses 13.56 MHz carrier frequency and the available data rates are 106, 212 and 424 kbps. (Ailisto et al., 2007).

NFC technology is becoming into large-scale use in mobile phones. The expansion of the use of NFC is driven by an industrial alliance, which opens new possibilities for mobile devices also in industrial applications. The advantages of the NFC compared to RFID are its diverse and flexible interfaces. Additionally, NFC offers more potential to implement battery-operated sensors (or even sensors without battery) with battery replacement cycles of months or years. (Sallinen et al., 2007)

2.5 Satellite

Satellite communication can offer innovative solutions for remote control and monitoring of geographically dispersed assets (Emerson, 2006a; Cungor and Lambert, 2006). Due to extensive geographical coverage, it may be a good alternative, when communications infrastructure, such as telephone or cellular network, does not exist (Emerson, 2006a; Cungor and Lambert, 2006). However, satellite communication has some disadvantages, e.g. long delays (Cungor and Lambert, 2006), varying channel characteristics (depending on fading and weather conditions) (Hu, 2001), cost (Emerson, 2006a; Cungor and Lambert, 2006) and lack of existing standards (Emerson, 2006a).

Example of utilising satellite as a part of the monitoring system, in conjunction with WSN, can be found in (King, 2005). London-based company, BP, used battery-operated ultrasonic sensors to remotely monitor the fill levels of industrial customers' gas tanks. The radio signal from sensors was transmitted to low-earth orbit satellite and then further to BP to enable timely deliveries. The number of tanks was about 200 and the reported delivery efficiency improvement was over 33%.

2.6 Cellular Networks

In process automation, cellular technologies can be used to collect measurement data from remote locations via public cell-phone networks (Emerson, 2006a; Hoske, 2006). This enables more cost-effective and up-to-date information about asset status than sending a person to the site (Emerson, 2006a). In addition to providing primary network connectivity, the cellular connections can serve as backup for industrial automation devices, such as SCADA devices, programmable logic controllers (PLCs) and remote terminal units (RTUs) (Hoske, 2006).

Compared to satellite connection, cellular networks have several advantages, namely lower costs, existing standards and economics-of-scale (Emerson, 2006a). As a disadvantage, it is reported that cellular technologies are not able to meet strict Quality of Service (QoS) requirements needed for some real-time applications (Cungor and Lambert, 2006). However, opposite opinions exist. (Liu and Jäntti, 2006) proposes a hybrid communication scheme utilizing general packet radio service (GPRS) and circuit-switched data call (CSD) to improve reliability performance requirement of the system. The results implied that with the improvement scheme the reliability requirements could be met using commercial cellular networks (Liu and Jäntti, 2006).

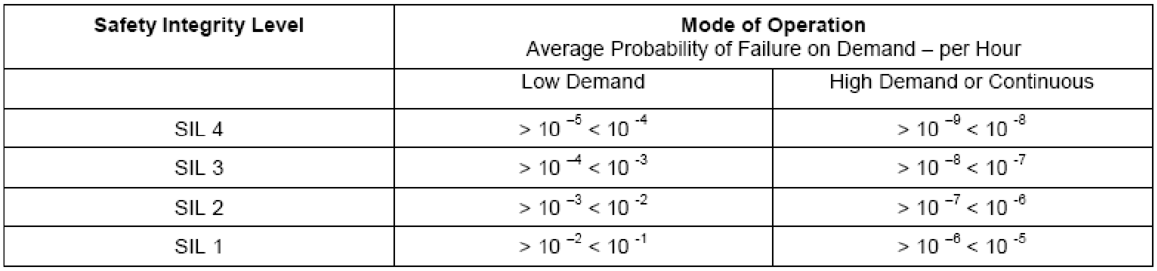
2.7 Additional Standards

In addition to standards mentioned above, some other standards may be of concern when developing wireless industrial applications. IEEE 1451, a family of Smart Transducer Interface Standards, describes a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks (IEEE 1451). For example, wireless communication protocol standards (e.g. 802.11, 802.15.1, 802.15.4) are being considered as some of the physical interfaces for IEEE P1451.5 (IEEE 1451). The aim for IEEE P1451.5 is to make possible to get the same sensor data from the wireless sensor implementing any of these three wireless protocols (IEEE 1451).

The International Electrotechnical Commission (IEC) 61508 standard for functional safety in programmable electronic systems defines the functionality of safety networks. The standard defines the requirements of a safety system to comply with the appropriate safety integrity level (SIL). (VAN, 2005)

Table 1 presents the IEC61508 safety integrity levels. The top-most is used for critical equipment, for example at nuclear power plants. SIL 3 is the highest level found in the traditional manufacturing and process applications. (VAN, 2005)

Table 1. IEC 61508 safety integrity levels (VAN, 2005).



Safety Integrity Level	**Mode of Operation** Average Probability of Failure on Demand – per Hour	
	Low Demand	High Demand or Continuous
SIL 4	$> 10^{-5} < 10^{-4}$	$> 10^{-9} < 10^{-8}$
SIL 3	$> 10^{-4} < 10^{-3}$	$> 10^{-8} < 10^{-7}$
SIL 2	$> 10^{-3} < 10^{-2}$	$> 10^{-7} < 10^{-6}$
SIL 1	$> 10^{-2} < 10^{-1}$	$> 10^{-6} < 10^{-5}$

European standard EN 954-1 was developed for safety machinery and is titled “Safety of machinery, Safety related parts of control systems” (VAN, 2005). For some wireless applications, especially related to control, it may be relevant.

Since 2003, ATEX directive has become mandatory for all electrical and mechanical equipment used in facilities with danger of exploitation. Any networked embedded devices needs to comply with the directive (Koumpis, 2005).

ISA 100 committee is working on establishing standards (ISA100.11a), recommended practices, technical reports, and related information that will define procedures for implementing wireless systems in the automation and control environment with a focus on the field level. The standard will likely adopt 6loWPAN (ABIresearch, 2007) and Wireless HART technologies (Pinto, 2007).

2.8 Technology Roadmap

Figure 5 presents a technology roadmap developed in RUNES project (see (RUNES)). The roadmap was discussed in (Koumpis, 2005). As a conclusion, it was stated that:

- Adoption of wireless systems to industrial automation will take longer period than in other sectors (e.g. building automation and control, medical care, disaster response, automatic meter reading)
- Companies dealing with automotive, food process, petrochemical and asset tracking will be the early adopters
- Adoption of wireless system to control applications will take considerably longer than adoption to monitoring applications
- Monitoring of hazardous / inaccessible areas was given priority in short-term by adopters of wireless technologies
- Many wireless systems in market today do not meet the local/national regulations, either because they transmit too much power or operate on non-licence free frequency area
- Any new networked embedded components should comply with the ATEX directive

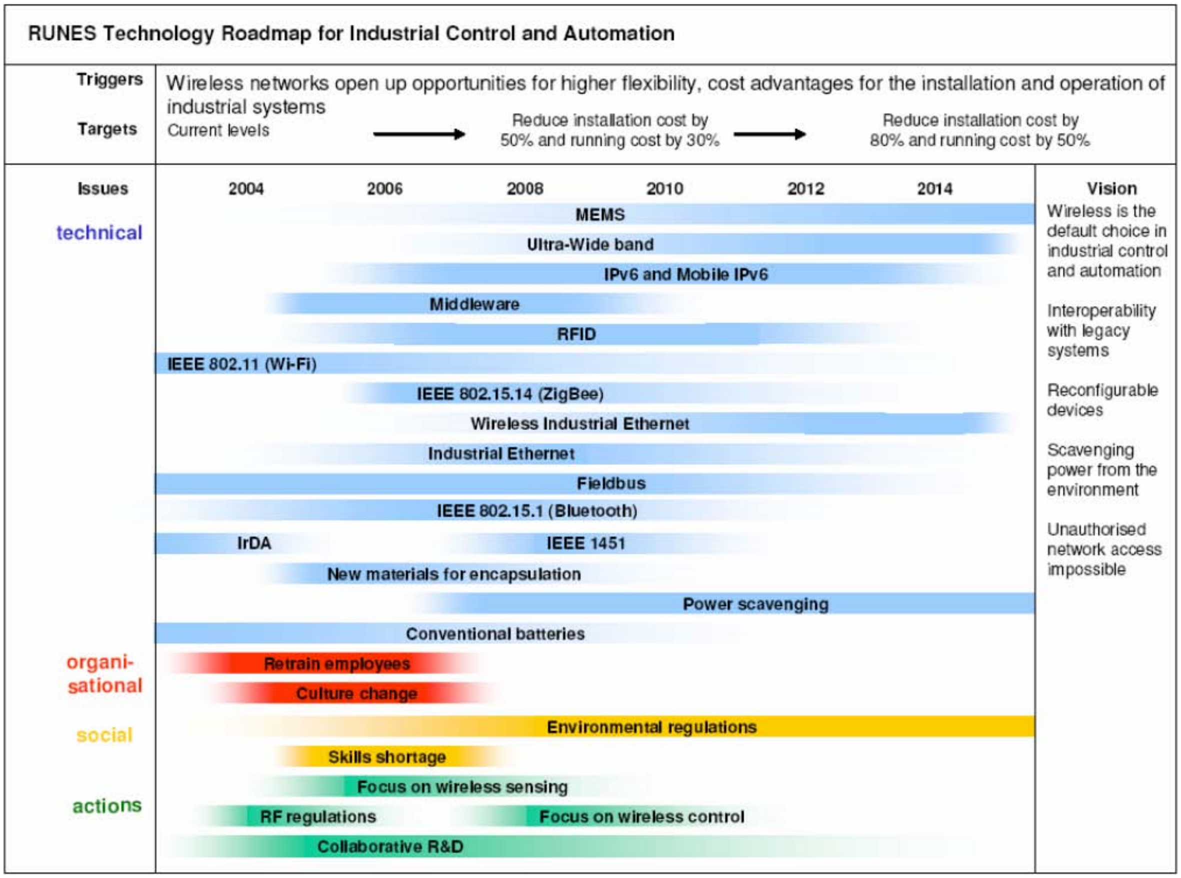


Figure 5. RUNES technology roadmap for industrial control and automation (Koumpis, 2005).

In the following Section, a brief introduction to wireless sensor networks is presented. Then, some characteristics for industrial environment with respect to wireless systems are introduced followed by industrial applications. Finally, some technical considerations are discussed.

3 WIRELESS SENSOR NETWORKS IN INDUSTRIAL ENVIRONMENT

3.1 Introduction to Wireless Sensor Networks

Wireless sensor networks (WSN) have been enabled by advancements in silicon chip technology, low-power micro-controllers, chip-based radios, ad-hoc networking protocols, and operating systems and languages for embedded systems. The WSN have a wide range of applications. These can be divided to: (Culler et al., 2004)

- Monitoring space
- Monitoring things
- Monitoring interactions with things with each other and the encompassing environment (monitoring complex interactions)

More detailed, the categories include, respectively: (Culler et al., 2004)

- Environmental and habitat monitoring, precision agriculture, indoor climate control, surveillance, treaty verification and intelligent alarms
- Structural monitoring, ecophysiology, condition-based equipment maintenance, medical diagnostics, and urban terrain mapping
- Wildlife habitats, disaster management, emergency response, ubiquitous computing environments, asset tracking, healthcare, and manufacturing process flow

The sensor nodes are physically small and they are typically provided with radio transceivers, microcontrollers, and batteries (Low et al., 2005). The nodes include wireless communications capability as well as sufficient computing resources for signal processing and data transmission (Aakvaag et al., 2005).

A node in sensor network consists of a microcontroller, data storage, sensor, analogue-to-digital converters (ADCs), a data transreceiver, controllers that tie the pieces together, and an energy source. A simple microcontroller may operate at 1 mW/ 10 MHz. When most of the circuits are turned off (in standby / sleep mode) the microcontroller power consumption is typically about 1 μW. These low-power microcontrollers have limited data storage, typically 10 kbytes of RAM for data and 100 kbytes of ROM for data storage. However, designers typically incorporate larger amounts of flash storage, for example a megabyte on a separate chip. (Culler et al., 2004)

Transreceivers are based on CMOS technology. The amount of energy needed to communicate wirelessly increases rapidly with distance and obstructions further attenuate the signal. WSN radios' energy consumption is about 20 mW and their range is typically measured in tens of meters. (Culler et al., 2004)

Depending on the surrounding environment, communication in WSN can be implemented in several ways (Aakvaag et al., 2005). Therefore, several network topologies are possible: star, cluster-tree and mesh. In different topologies, sensor nodes can act as a simple data transmitters and receivers or routers working in a multi-hop fashion (Aakvaag et al., 2005). IEEE 802.15.4 standard considers star and mesh topologies (Baronti et al., 2007). Figure 6 illustrates star, cluster-tree and mesh network topologies applied in ZigBee network.

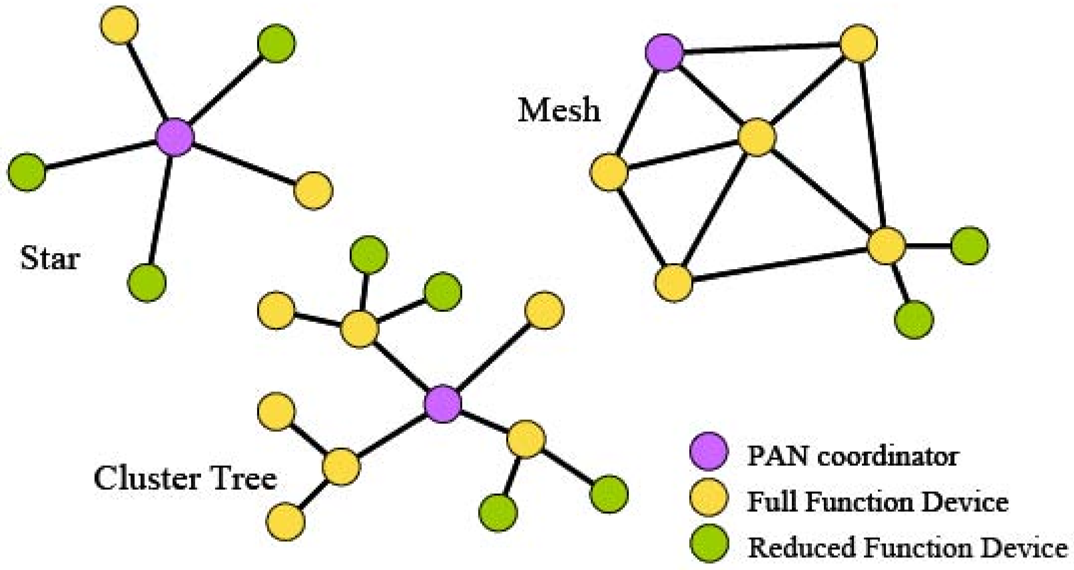


Figure 6. Different topologies in ZigBee network. Network topologies are general, but personal area network (PAN) coordinator, full function devices (FFDs) and reduced function devices (RFDs) are characteristic for ZigBee. FFD can act as a network coordinator or an end-device. Therefore, FFD is capable of relaying data, providing synchronisation or network join. The FFD can also take the role of personal area network (PAN) coordinator, administering network services. RFD can act only as end device. (Baronti et al., 2007)

The network tries to minimize the energy consumption either by eliminating communications or turning off the radio, when communications do not occur. This can be done either by: (Culler et al., 2004)

- Local processing of data in nodes
- Communicating, only if something of interest occurs
- Data aggregation (for example measuring average temperature for certain area
- Compression and scheduling
- Assigning certain tasks for special nodes
- Turning off radio, when uninteresting packet is received

In addition to limited energy resources, several other issues must be addressed in order to fully gain the advantage of WSN. These issues include: (Culler et al., 2004)

- Limited processing speed
- Limited storage capacity
- Limited communication bandwidth
- Wide variety in connectivity between nodes
- Harsh operating environments
- High degree of interaction between nodes (positive and negative)

The network must also be able to allocate limited hardware to multiple concurrent activities, for example sampling sensors, processing, and streaming data. Also, discovering the interconnections between the devices as well as routing data effectively from where it is produced to where it is used, is required. (Culler et al., 2004)

Each of the aforementioned factors complicates networking protocols. However, despite of the challenges, deploying and maintaining of the nodes must be inexpensive (Culler et al., 2004). Especially, because of the large number of nodes expected in some applications, the unit price of a node is an important parameter in the overall network cost (Aakvaag et al., 2005): according to (Rabaey et al., 2000), the unit price of a node should be less than 1 USD to achieve cost-effectiveness

3.2 Industrial Environment Characteristics

In industrial environments, the coverage area of WSN as well as the reliability of the data may suffer from noise, co-channel interferences, multipath propagation and other interferers (Low et al., 2005). For example, the signal strength may be severely affected by the reflections from the walls (multipath propagation) (Werb and Sexton, 2005), interferences from other devices using ISM bands (Werb and Sexton, 2005), and by the noise generated from the equipments or heavy machinery (Low et al., 2005). In these conditions, it is important that data integrity is maintained for operation-critical data, for example alarms (Low et al., 2005).

Interference signals can be classified in two different categories, broadband and narrowband. Broadband interference signals have constant energy spectrum over all frequencies and high energy. They are usually emitted unintentionally from radiating sources where as narrowband interference signals are intentional and have less energy. Both interferences have varying type of degradation effect on wireless link reliability. (Low et al., 2005)

Table 2 presents the general sources found in industry. Both broadband and narrowband interferences are considered.

Table 2. Interference sources. (Low et al., 2005)

Broadband interferences	***Narrowband interferences***
Motors	Cellular telephone
Inverters, Silicon-controlled rectifier (SCR) Circuits	Radio and TV transmitters
Electric switch contacts	Power-line hum
Computers, ESD	Signal generators
Ignition systems	Local oscillator, UPS system
Voltage regulators	Test equipment
Lightning electromagnetic pulses	Microwave&Ultrasonic equipment
Arc/vapor lams	Electronic ballasts
Pulse generators	Medical equipment
Thermostats	Microprocessor systems
Welding equipment	Pager transmitters
Frequency converters	High-frequency generators

Other types of interference sources are for example wide operating temperatures, strong vibrations, and airborne contaminants. It is important to study and understand the radio channel characteristics in order to predict the communications performance in these operating conditions (Low et al., 2005). Moreover, radio modulation techniques can be applied to reduce the interferences (Low et al., 2005).

Spread spectrum radio modulation techniques are applicable to reduce the interferences because of their multiple access, anti-multipath fading and anti-jamming capabilities. The two main spread spectrum techniques employed are direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSSS). They have different physical mechanisms and therefore, react differently in industrial settings. The choice between radio techniques is dependent on application (Low et al., 2005) and discussed more detailed in Section 3.4.6.

3.3 Industrial Applications

3.3.1 Introduction

According to survey results presented in (Hoske, 2006), the leading application for industrial networks (both wired and wireless) is supervisory control and data acquisition (SCADA). It is followed by diagnostics, testing, maintenance; both continuous and batch processing; motion control, robotic equipment; and machine control, CNC equipment (graphic). Furthermore, the applications include pump, fan, blower applications; continuous processing; packaging machines; materials handling equipment (elevators, cranes, hoists); and discrete product manufacturing. The most used means of communication were Ethernet TCP/IP, RS232 and 4-20 mA. Ten most used networks, communications and protocols did not include wireless alternatives.

However, as mentioned in Section 2.1, wireless technologies are reported to grow. A categorization for wireless sensor network applications is presented in (Low et al., 2005):

- Rare event detection
- Periodic data collection
- Real-time data acquisition
- Control
- Industrial mobile robots
- Real-time inventory management

WSN can be deployed for example to bearings of motors, oil pumps, engines, vibration sensors on packing crates, or many inaccessible or hazardous environments. For these environments, the wired solution may be impractical due to e.g. isolation required for cables running near to high humidity, magnetic field or high vibration environment. Also, for applications that have frequent re-location, wireless solution may be more feasible. (Low et al., 2005). APPENDIX 1 contains some application examples collected from the literature.

Characteristic for industrial applications is the existence of legacy communication systems (Shen et al., 2004). For example, fieldbuses are used to transport information across manufacturing or process equipment (Aakvaag et al., 2005). Figure 7 presents an example of such a communication scenario.

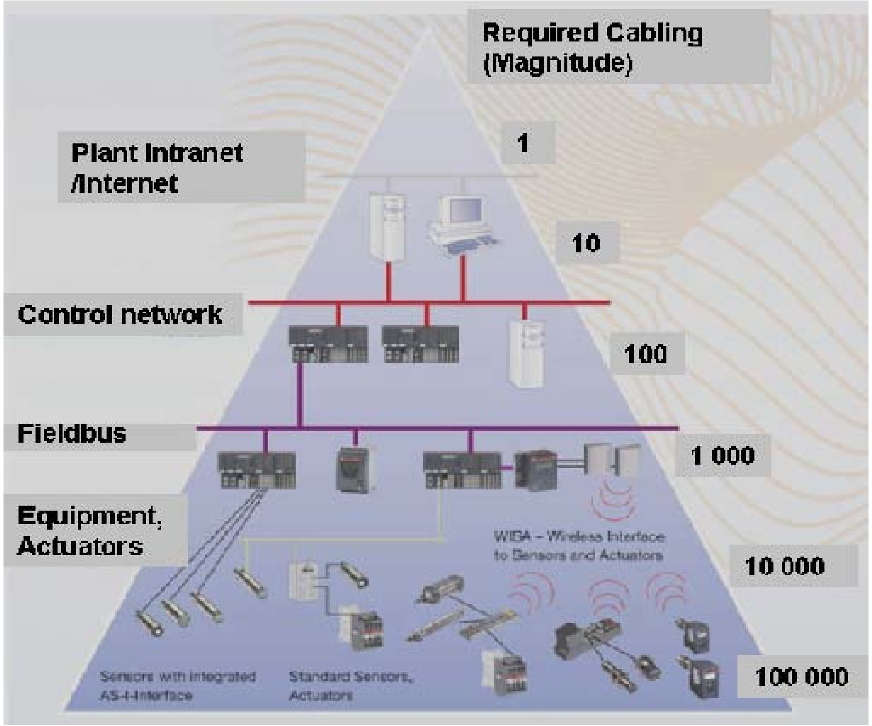


Figure 7. An example architecture of a plant automation system with wireless interface to sensors and actuators (WISA) provided by ABB. Complexity of architecture may pose challenges for managing the entity. (Virrankoski, 2007)

Compared to wired solutions in industrial applications, the wireless systems and WSN have several advantages. These include, for example:

- Flexibility in installing/upgrading network (Aakvaag et al., 2005)
- Reduced deployment and maintenance costs (Shen et al., 2004; Aakvaag et al., 2005)
- Decentralization of automation functions (Aakvaag et al., 2005)
- Better coping with regulatory and safety obstacles in running cables in constricted or dangerous areas (Shen et al., 2004
- Applicable for moving and rotating equipment (Low et al., 2005)
- Improved fault localization and isolation: for example critical tasks are often ensured with redundant wires, which may pose difficulties for fault location and isolation (Low et al., 2005).
- Incorporating short-range technologies to automation system (which has possible interfaces to wide area networks) forms a heterogeneous network, which may improve automation system efficiency (Low et al., 2005). Figure 8 presents a heterogeneous system in industrial automation.
- Exploitation of micro-electromechanical systems (MEMS): integrated wireless sensors with built-in communication capabilities offer a more robust design than attaching wires to small-sized devices. (US Department of Energy, 2002)

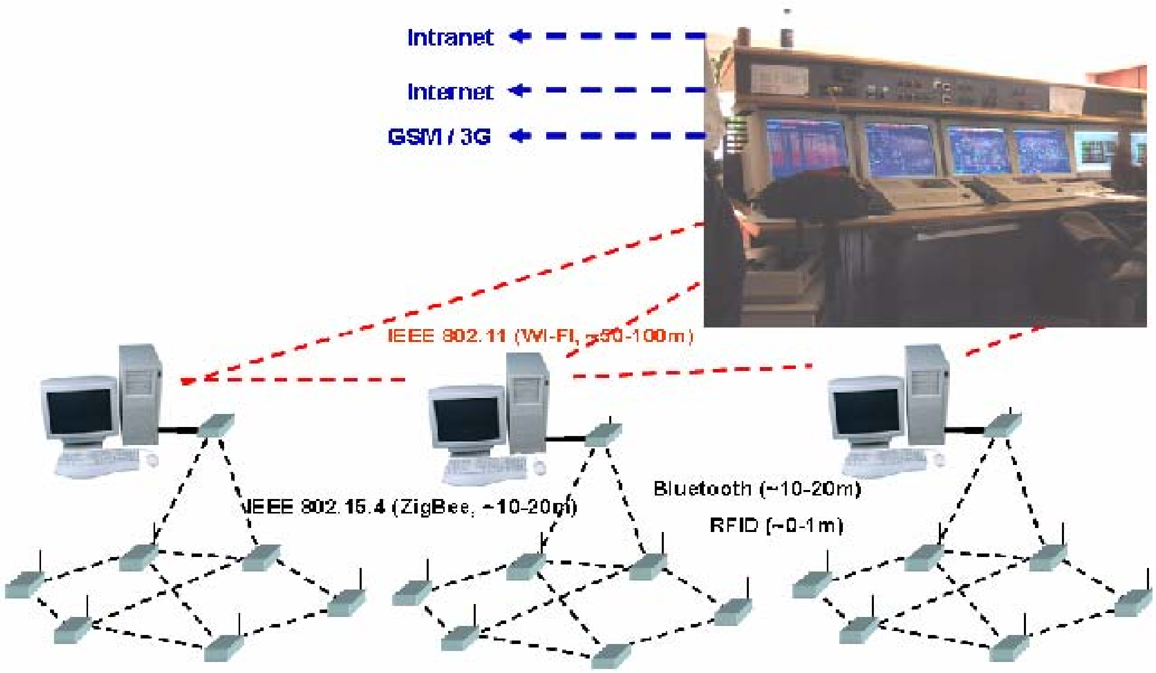


Figure 8. Heterogeneous system in an automation application. Different communication protocols are needed for based on wireless application scenario. Interworking of different technologies must be taken into account. (Virrankoski, 2007)

3.3.2 Classification of Applications

From industrial point of view, ISA SP100 workgroup introduced six classes for wireless communications, which include applications from each of the aforementioned categories. The classes were based on analysis of industrial, inter-device wireless communication applications (ISA-SP100.11, 2006). The classes are presented in Figure 9.

Class 5 defines items related to monitoring without immediate operational consequences. This class includes applications without strong timeliness requirements. The reliability requirement may, however vary. Some, like sequence-of-events logs, require high reliability; others, like reports of slowly-changing information of low economic value, need not to be so reliable since loss of a few consecutive samples may not be important. (ISA-SP100.11, 2006).

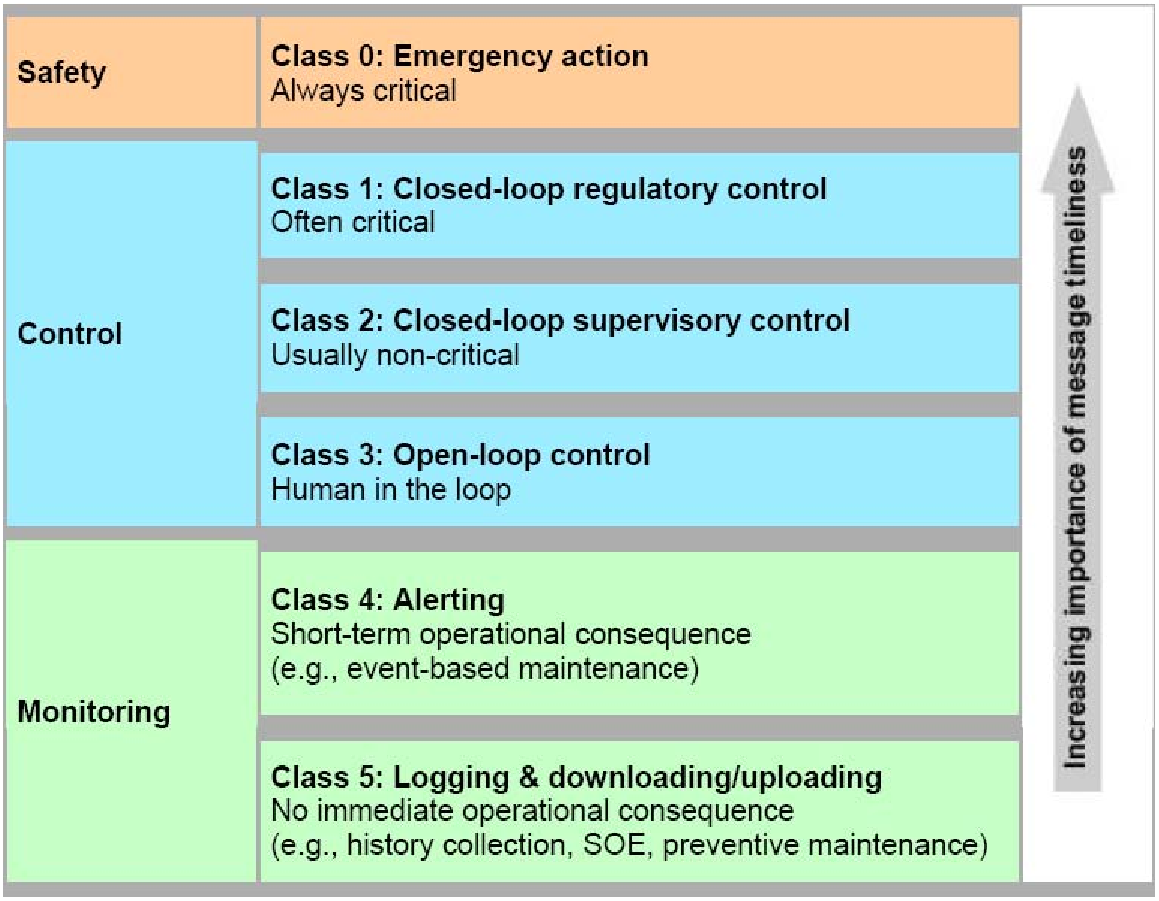
Class 4 defines monitoring with short-term operational consequences, which includes high-limit and low-limit alarms and other information that may require further checking or involvement of a maintenance technician. Timeliness of information in this class is typically low (slow), measured in minutes or even hours. (ISA-SP100.11, 2006).

Class 3 covers open loop control applications, in which an operator, rather than a machine, “closes the loop” between input and output. For example, an operator could take a unit offline, if required. Timeliness for this class is human scale, measured in seconds to minutes. (ISA-SP100.11, 2006)

Class 2 consists of closed loop supervisory control, in which applications usually have long time constants, with timeliness of communications measured in seconds to minutes. Examples in this category are batch unit and equipment selection. (ISA-SP100.11, 2006)

Class 1, closed loop regulatory control, includes motor and axis control as well as primary flow and pressure control. The timeliness of information in this class is often critical. (ISA-SP100.11, 2006)

Class 0 defines emergency actions related to safety, which are always critical to both personnel and plant. Most safety functions are, and will be, carried out by dedicated wired networks in order to limit both failure modes and vulnerability to external events or attacks. Examples in this category are safety interlock, emergency shutdown, and fire control. (ISA-SP100.11, 2006)



Safety	**Class 0: Emergency action** Always critical
Control	**Class 1: Closed-loop regulatory control** Often critical
	Class 2: Closed-loop supervisory control Usually non-critical
	Class 3: Open-loop control Human in the loop
Monitoring	**Class 4: Alerting** Short-term operational consequence (e.g., event-based maintenance)
	Class 5: Logging & downloading/uploading No immediate operational consequence (e.g., history collection, SOE, preventive maintenance)

Figure 9. Classification of industrial automation applications. (ISA-SP100.11, 2006)

Another way of classifying the communications in automation domain in general is presented in (VAN, 2005). The classification is based on guaranteed response times of an automation system and is as follows (additionally there is a “non real-time class”, which has not been considered here):

- Class 1, soft real-time. This category has scalable cycle time. Systems of this class are used in factory floor and process automation.
- Class 2, hard real-time: Cycle time in this category varies between 1…10 ms. Systems of this class are used for control applications.
- Class 3, isochronous real-time. This category has time/clock synchronisation and routing with time schedule. Cycle time varies from 250 µs…1 ms; jitter less than 1 µs. Systems of this class are used for motion control.

Either one of these classifications does not take into account all the real-time aspects presented in Section 3.4.2.

3.4 Design Considerations

3.4.1 Design Challenge

Developing a wireless sensor network for industrial applications requires a combination of expertise from several different disciplines (VAN, 2005; Bonivento et al., 2006; Howitt et al., 2006). According to (Howitt et al., 2006):

- Industrial expertise is essential for application domain specific knowledge.
- Sensor expertise is needed to understand issues associated with calibration, drift, digitalization, sampling and transducers.
- Wireless device and RF environment expertise is needed to address issues for technology suitability, electromagnetic compatibility, and electromagnetic interference in industrial environments.
- Network expertise is required for understanding the complex hierarchical network architectures which are required for industrial WSN.

3.4.2 Performance and Quality of Service

For industrial WSN, performance can be measured in terms of reliability, security, throughput, latency, adaptability and affordability. In aggregate, these measures can be used to define quality of service (QoS) (Howitt et al., 2006).

Reliability

Reliability addresses the ability of the network to carry out its functional requirement of carrying industrial application information over the network over a broad range of operational conditions (Howitt et al., 2006). Networks ability to deal with communication disruptions, unanticipated variations in traffic and variations in the operational environment should be considered (for issues causing disturbances refer to Section 3.2) (Howitt et al., 2006). The system should be able to react to these disturbances using a predictable”fail-safe” mechanism (Howitt et al., 2006), which is sometimes referred as “robustness of design”.

As mentioned before, WSN are often energy constrained and therefore reliability includes the ability of the network to maintain operational integrity under energy constraints such as dirty power, battery operation, or energy scavenging (Howitt et al., 2006). Operational power issues are discussed more detailed below.

Security

According to (Hamalainen et al., 2006), WSN share the common networking security threats presented in (Stallings, 2005), namely message interception, message modification, message fabrication, and interruption of communication and operation. Furthermore, attacks can be carried out by malicious outsiders or insiders (Shi and Perrig, 2004; Karlof and Wagner, 2003). According to (Shi and Perrig, 2004), it is desired that outsider attacks are blocked and in case of insider attack, the security gracefully degrades (is resilient). Different types of attacks are presented in Figure 10.

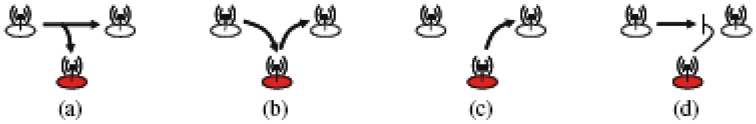


Figure 10. Different types of attacks in WSN: a) interruption b) modification c) fabrication d) interruption (Hamalainen et al., 2006).

WSN have special characteristics that enable new ways of security attacks (Hamalainen et al., 2006). Passive attacks are carried out by eavesdropping on transmissions and may include for example traffic analysis or disclosure of message contents (Stallings, 2005). Active attacks consist of modification, fabrication and interruption, which in WSN cases may include node capturing, routing attacks, or flooding (Hamalainen et al., 2006). It should also be noted, that even though WSN themselves are resource-limited, an attacker may have more powerful equipment available, such as laptop or PC, for making attacking more effective (Karlof and Wagner, 2003).

When designing the security of the wireless sensor network, both low-level (key establishment and trust control, secrecy and authentication, privacy, robustness to communication denial of service, secure routing, resilience to node capture) and high-level (secure group management, intrusion detection, secure data aggregation) security primitives should be addressed. It should also be noted, that due to resource limitations some of the previously proposed solutions may not work due to resource limitations. (Perrig et al., 2004)

As discussed in Section 3.3.1, WSN in industrial environments may be hybrid solutions. This, in turn, may provide another challenge. (Roman et al., 2005) separates the security of the wireless sensor network to two different categories. First, there is the security of the data acquisition network, which is a collection of sensor nodes with the task of measuring the physical data of its surroundings, and one or more base stations in charge of collecting data from the nodes and forwarding control information from the users. Second, there is the security of the data dissemination network which is a combination of wired and wireless networks providing an interface of the data acquisition network to any user.

A short review about some security technologies employed in wireless communications can be found in (VAN, 2005). A good review about ZigBee security issues (and others) is presented in (Baronti et al., 2007).

Throughput

Throughput defines the network's ability to carry out the offered traffic by industrial applications. It is impacted by the communication environment (Howitt et al., 2006).

When considering data rate required for application, it should be noted that although required bandwidth for sensor data may normally be low, dealing with multiple sensor data in small time interval may cause bandwidth requirement to increase (Pellegrini et al., 2006; Körber et al. 2007). Section 3.4.6 discusses the effect of different radio modulation techniques and their effect to throughput.

Latency, Timeliness, Jitter

Latency defines the time delay from sensor node to base station. Latency requirements are dependent on certain communication traffic, for example machine's servo control sensors have stricter requirements than sensors in supporting supply chain management may have. Latency is influenced by sensor node density, interrogation rates, network topology and number of simultaneous actions. (Howitt et al., 2006)

In addition to latency, other two concepts for defining real-time performance are timeliness and jitter. Timeliness defines the absolute deadline for the actions to be executed or completed. Jitter defines the time window in which action or co-ordinated actions have to be executed or completed. In the latter case it is also a fault if an action is completed earlier. Jitter can therefore be used to define requirement of synchronization. Concepts of timeliness and jitter are illustrated in Figure 11. (VAN, 2005)

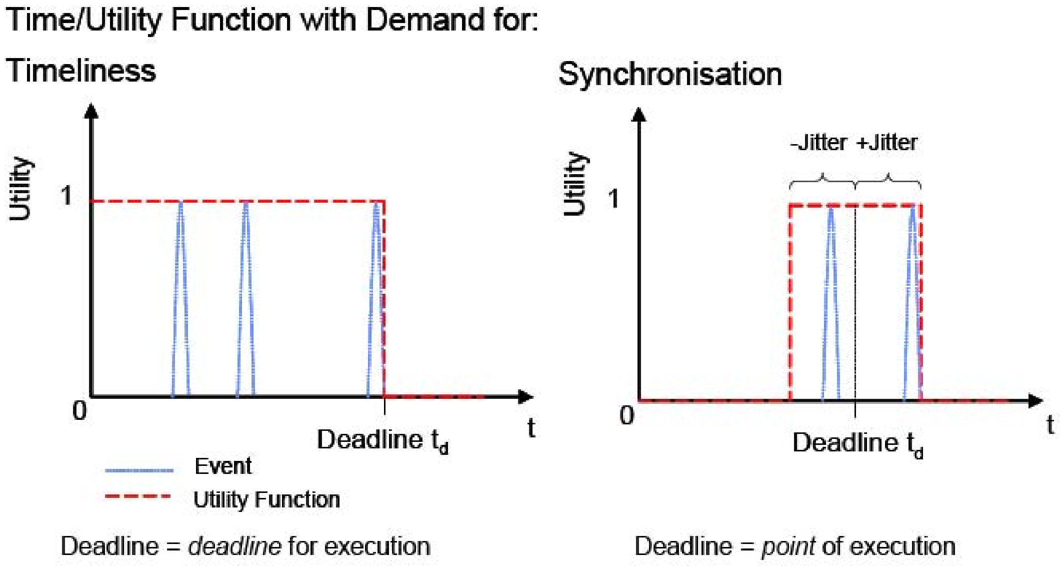


Figure 11. Concepts of timeliness and jitter. Time/utility functions are used to describe the utility of executing and completing a certain action as a function of the point of time when the action is executed and completed. The utility values describe the relative importance of an action. (VAN, 2005)

Adaptability

A major advantage of WSN is its ability to adapt to new configurations or tasks (Howitt et al., 2006). In industrial environment, adaptations may be required due to mobility of some sensor elements and scaling and/or reconfiguring the WSN to handle new process or modification to an existing process (Howitt et al., 2006). Configuration of WSNs may change also because of losses of key components, such as router nodes and gateways (ISA-SP100.11, 2006).

Also, physical industrial environment may change over time, which in turn causes changes to RF environment (Howitt et al., 2006). Additionally, there may be changes in traffic flow due to changes in sensor location or process utilization (Howitt et al., 2006). The WSN should be able to adapt to all these changes while maintaining the required levels of throughput, latency, reliability and security (Howitt et al., 2006). Proposals to improve WSN reliability especially in presence of changing RF environment can be found e.g. from (Jiang et al., 2006; Howitt et al., 2006)

Affordability

Affordability includes all the costs of ownership. These incorporate packaging requirements, modifications, maintainability, implementation costs, replacement and logistics costs, and training and servicing costs as well as the per-unit costs. (Howitt et al., 2006)

Coexistence

Interferences to the mission-critical data can have costly consequences in terms of money, manpower, and even lives of employees and public (Low et al., 2005). Therefore, the coexistence of WSN with the other systems operating in the same band should be examined (ISA-SP100.11, 2006). The coexistence should be considered both from system and to system –point of views, i.e. how does the system reduce its effects to other systems or reduce effects from other systems and interference sources to itself (ISA-SP100.11, 2006).

An example about coexistence impact analysis between 802.15.4 and 802.11b is presented in (Howitt and Gutierrez, 2003). As a conclusion, it is proposed that 802.15.4 should have little or now impact to 802.11b .

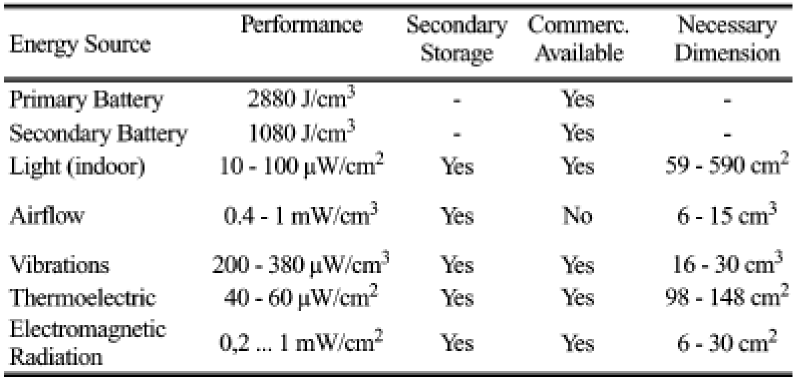
3.4.3 Operational Power

Energy consumption is an important design constraint in battery-powered wireless sensors. In order to save power, network nodes are kept in sleep mode for a significant fraction of time. A synchronization algorithm is required to ensure simultaneous sleep and awake times for nodes. The development environment should provide a MAC layer access to node sleep/awake states in order to reduce additional stack delays and enable precise synchronization. (Aakvaag et al., 2005)

Communication is the most energy intensive operation that the node performs (Culler et al., 2004): packet transmitting, receiving and listening consume energy (ISA-SP100.11, 2006). For example, in (Körber et al., 2007), data rate (Mbit/s) and energy per bit -ratio (µJ/bit) were used as selection criteria.

However, the use of batteries can be troublesome due to their limited lifetime, making periodic replacements unavoidable (Anton and Sodano, 2007). Energy scavenging devices are used to capture the ambient energy surrounding the electronics and convert it into usable electrical energy (Anton and Sodano, 2007). Some energy scavenging techniques’ characteristics are presented in Table 3. A survey about power scavenging systems is presented for example in (Paradiso and Starner, 2005).

Table 3. Characteristics of some energy scavenging techniques.(Körber et al., 2007)



Energy Source	Performance	Secondary Storage	Commerc. Available	Necessary Dimension
Primary Battery	2880 J/cm^3	-	Yes	-
Secondary Battery	1080 J/cm^3	-	Yes	-
Light (indoor)	10 - 100 µW/cm^2	Yes	Yes	59 - 590 cm^2
Airflow	0.4 - 1 mW/cm^3	Yes	No	6 - 15 cm^3
Vibrations	200 - 380 µW/cm^3	Yes	Yes	16 - 30 cm^3
Thermoelectric	40 - 60 µW/cm^2	Yes	Yes	98 - 148 cm^2
Electromagnetic Radiation	0,2 ... 1 mW/cm^2	Yes	Yes	6 - 30 cm^2

3.4.4 Scalability and Modularity

WSN should be both scalable and modular, i.e., support of both small and large numbers of sensors and actuators without affecting system performance (Körber et al., 2007). The characteristics of different radio communication components of the system should be carefully analysed (Ramamurthy et al., 2007). For example, Bluetooth can support only up to seven connections per device in a piconet setup (Ramamurthy et al., 2007). Additionally, when developing a security approach for wireless sensor networks, the scalability of the solution is important (Shi and Perrig, 2004).

3.4.5 Topology

According to (Horton and Suh, 2005), mesh networks are more scalable, offer better QoS, and it is shown analytically that they are more energy efficient than equivalent single-hop networks (Horton and Suh, 2005). They also introduce redundancy in topology, which makes them more robust against the failure of the single node, since messages may be routed through alternative paths (Shen et al., 2004; Horton and Suh, 2005). In star topology, if a signal is blocked by physical or RF interference, the network cannot recover, until the source of interference is removed (Shen et al., 2004).

However, (Körber et al., 2007) points out that energy awareness achieved by low or very low duty cycles causes a trade-off between quality of service and node lifetime and with respect to real-time applications this is not acceptable. Hence, (Körber et al., 2007) proposes star topology for industrial real-time wireless sensor/actuator applications.

A hybrid topology can combine the benefits of the both aforementioned networks by combining efficiency and flexibility of star and mesh topologies (Shen et al., 2004). In hybrid networks, star nodes are controlled by mesh nodes, therefore providing efficiency and flexibility (Shen et al., 2004).

3.4.6 Radio

As mentioned in Section 3.2, radio technologies can be used to reduce interferences. For this, spread spectrum radio modulation techniques are applicable because of their multiple access, anti-multipath fading and anti-jamming capabilities (Low et al., 2005). The two main spread spectrum techniques employed are direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) (Low et al., 2005). They have different physical mechanisms and therefore, react differently in industrial settings (Low et al., 2005). The choice between radio techniques is dependent on application and environment (Low et al., 2005).

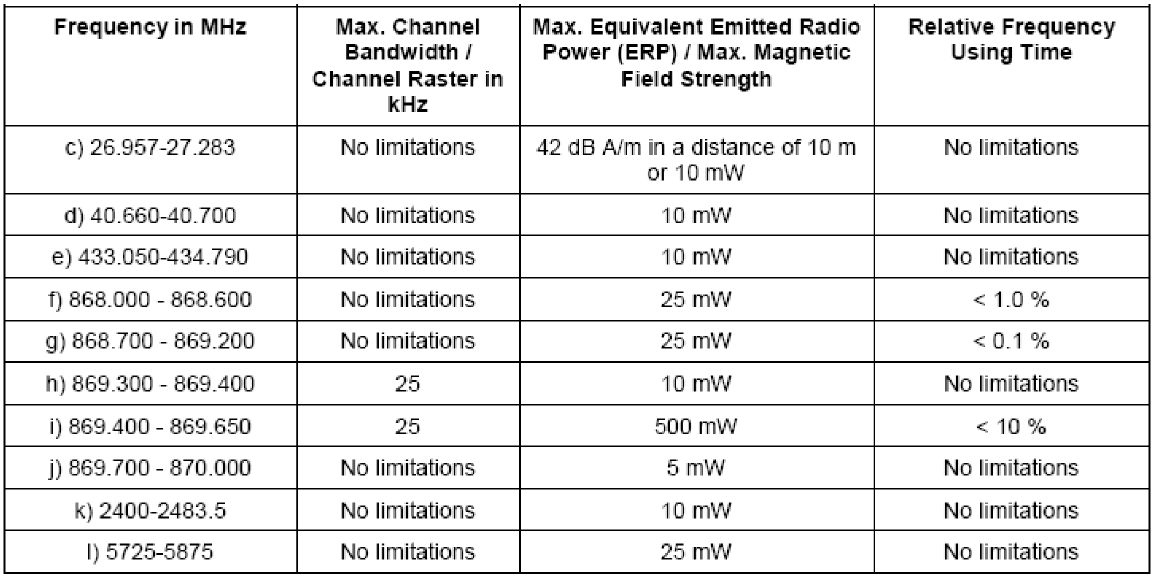
Due to the nature of frequency hopping in FHSS, other data packets still may reach the receiver even if one packet fails because of strong narrowband interference. Additionally, users may choose not to use certain frequencies, if there are known sources of interference. Therefore, FHSS is suitable for harsh environments, because only part of the spectrum is affected if packets jam at some hops. In general, FHSS scheme is less likely to collide with other transmissions since changing of transmitting frequency makes colliding in certain time frame more difficult than in DSSS scheme. (Low et al., 2005)

DSSS, for its part, can remove the interference completely, if the interfering signal power is within the jamming margin, especially in case of low two medium narrowband interference (Low et al., 2005). In case of heavy narrowband interference, though, FHSS can still perform, but DSSS fails (Low et al., 2005). To summarize, DSSS is ideal for systems that require high speed and are applied to environments with low or medium narrowband interference, whereas FHSS is suitable for applications that require low cost, lower data rate and applicability to high narrowband interference environment (Low et al., 2005).

Radio modulation can be incorporated with other strategies to improve link quality in industrial environments. These strategies include channel diversity, path diversity, temporal diversity an increased transmit power. (Low et al., 2005) Discussion about reduced radio link quality and countermeasures can be found in (Werb and Sexton, 2005)

The frequencies used for wireless communication in industrial automation are presented in Table 4. The frequencies can be used also by other wireless applications, e.g. RFID applications, WLAN applications or ISM applications. There is no guaranty for minimum radio transmission quality. (VAN, 2005)

Table 4. Frequencies used for wireless communication in industrial automation (VAN, 2005).

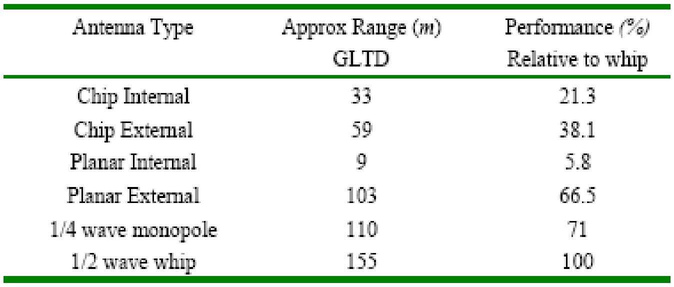


Frequency in MHz	Max. Channel Bandwidth / Channel Raster in kHz	Max. Equivalent Emitted Radio Power (ERP) / Max. Magnetic Field Strength	Relative Frequency Using Time
c) 26.957-27.283	No limitations	42 dB A/m in a distance of 10 m or 10 mW	No limitations
d) 40.660-40.700	No limitations	10 mW	No limitations
e) 433.050-434.790	No limitations	10 mW	No limitations
f) 868.000 - 868.600	No limitations	25 mW	< 1.0 %
g) 868.700 - 869.200	No limitations	25 mW	< 0.1 %
h) 869.300 - 869.400	25	10 mW	No limitations
i) 869.400 - 869.650	25	500 mW	< 10 %
j) 869.700 - 870.000	No limitations	5 mW	No limitations
k) 2400-2483.5	No limitations	10 mW	No limitations
l) 5725-5875	No limitations	25 mW	No limitations

In (Körber et al., 2007), a selection of radio technology for complementary or substitional system for a wired sensor/actuator bus is presented. A selected technology was a compromise of design flexibility, availability, data rate, supportability for large group of network nodes (at least 64), real-time capability, energy consumption (short wake-up time) and radio characteristics. Interestingly, 802.15.4-based radio was not selected because of it failed to provide support for guaranteed time slots for more than 7 nodes.(Körber et al., 2007)

Other issues to be considered are maximum transmission range and possible regulatory issues concerning radio technology in question (ISA-SP100.11, 2006). Additionally, antenna type and possible restrictions to it may be analyzed (ISA-SP100.11, 2006). An open-field test for different antenna types was carried out in (Buckley, et al., 2006). It was shown that the antenna performance is related directly to the size, type and orientation of the antenna under test. The results for different antenna types are presented in Table 5.

Table 5. Performance comparison of different antenna types. Good link threshold distance (GLTD), is defined as a distance, where 65% of transmitted packets is received successfully. (Buckley et al., 2006)



Antenna Type	Approx Range (*m*) GLTD	Performance *(%)* Relative to whip
Chip Internal	33	21.3
Chip External	59	38.1
Planar Internal	9	5.8
Planar External	103	66.5
1/4 wave monopole	110	71
1/2 wave whip	155	100

3.4.7 System and Software

General Software and System Considerations

According to (Dzung et al., 2005), the system must require minimum operator intervention. For WSN, this would mean a system that is self-organizing, self-configuring and self-healing (Shen et al., 2004). (Culler et al., 2004) addresses this issue also: manual configuration and managing of large WSN is impractical, and therefore, nodes must be able to organize themselves. Additionally, it should be possible to administrate and program the nodes as an ensemble rather than individual devices alone (Culler et al., 2004). Additionally, the architecture should support existing (legacy) fixed-installation systems and standards (in (Dzung et al., 2005), the smart sensors (IEEE1451) and Ethernet were mentioned as example).

Application software should be accessible through a simple API and be easily customized for both standards-based and customer-specific requirements enabling rapid development and network deployment (Shen et al., 2004). Moreover, the WSN should integrate seamlessly with the host PLC (Dzung et al., 2005) and legacy fieldbus systems (Shen et al., 2004; Willig et al., 2005).

An application utilising existing wireless fieldbus architecture was presented in (Pellegrini et al., 2006). In the proposed solution, the physical and data link layers were taken directly from existing WLAN/WPAN protocols and the application layer was adequately modified from the existing wired fieldbus system. Additionally, an adaptation layer between the application and radio data link layers was required. Figure 12 presents the architecture of the system bridged with wired fieldbus system. Wireless technologies in industrial automation and fieldbus systems are discussed also in (Willig et al., 2005.

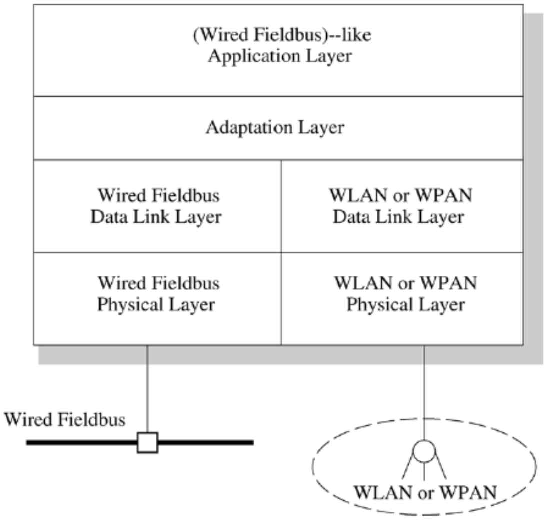


Figure 12. Wireless fieldbus bridged with wired fieldbus. The physical and data link layers of the wireless system are taken directly from existing WLANs / WPANs. The wired fieldbus-like application layer is modified from existing fieldbus systems. The adaptation layer adapts the application and data link layers.

After deployment in the field, network management and monitoring tools are essential (Shen et al., 2004). A graphical user display could, for example, display network connectivity and set node parameters (Shen et al., 2004). The management software could provide whole network performance analysis and other management features, such as, detecting failed nodes (e.g. for replacement), assigning sensing tasks, monitoring network health, upgrading software and providing QoS provisioning(Shen et al., 2004). Possibility of firmware updates should also be considered (ISA-SP100.11, 2006).

Operating System Considerations

According to (Horton and Suh, 2005), embedded software in nodes must have precise control over their hardware and OS should allow high level applications of direct and efficient control over low level HW, when necessary. An important property in this sense is the access to medium access control (MAC) layer in order to enable proper time synchronization, as mentioned in (Aakvaag et al., 2005). Without access to the MAC layer, the synchronization had to be implemented to the network (NTW) layer, which introduced an additional stack delay (Aakvaag et al., 2005). Taking into account the application classes presented in Section 3.3.2 and real-time requirements presented in Section 3.4.2, the additional stack delay may not be acceptable for all applications. The other alternative would have been to keep nodes awake all the time, which would not have been feasible in terms of energy consumption (Aakvaag et al., 2005).

A survey about MAC protocols can be found for example in (Demirkol et al., 2006). Note, that it is mentioned there that latency, throughput, and bandwidth utilization may be secondary in sensor networks, in industrial applications these maybe essential properties, depending on application (see for example (Körber et al., 2007) for reference).

An another example of where hardware control is needed is the power-saving feature. There may be a need to control a sensor (such as a turn vibration sensor on/off), turn the memory system off immediately after sending data or application may need direct access to radio RSSI to make routing decisions. (Horton and Suh, 2005) suggests that traditional layered abstraction for both networks and network stack leads to inefficiencies. Instead, one should seek for the balance between the precise hardware control and the ease of general purpose programming and efficiency (Horton and Suh, 2005).

4 CASE EXAMPLE – WIRELESS MONITORING OF A STEAM BOILER

4.1 Application

Section 4.1 is freely quoted from Juha Kemppainen: Master's Thesis

A steam boiler produces steam for a laboratory-scale chemical pulp process. The steam production process uses fuel oil and includes water storage tank, boiler, and pipelines. Feed water temperature is approximately 20 °C and after the boiler, steam temperature is approximately 200 °C. Four measurements are implemented to the steam boiler: three for temperature and one for the steam pressure. The measurements are presented in Figure 13.

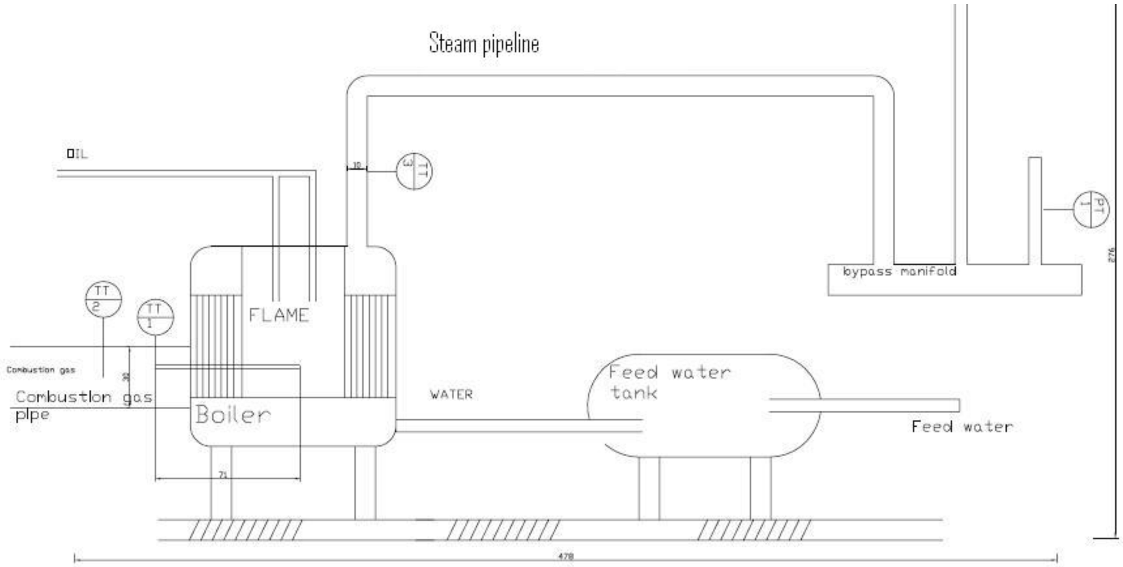


Figure 13. Steam boiler environment with measurements. T1, T2 and T3 are the temperature measurements and P1 is the pressure measurement.

Temperature is measured from the flame in the combustion chamber (required measuring range from the room temperature to approximately 1500 °C), from the combustion gas pipe (from the room temperature to over 300 °C) and from the surface of the steam pipe (from the room temperature to approximately 300 °C). The pressure, which normally is approximately 13 bar, is measured from the bypass manifold. During shutdowns and maintenance operations, however, the pressure may vary between 0-40 bars.

Lower temperatures from the combustion gas pipe and from the surface of the steam pipe are measured by Pt100-sensors. Since measurements are located closely to each other, the sensors are attached into one two-channel wireless transmitter node.

The higher temperature from the flame in the combustion chamber is measured with the S-type thermocouple and it has its own wireless transmitter node. For the thermocouple, mains power is required for the transmitter head.

Additionally, the pressure sensor has its own wireless transmitter node and requires mains power. Altogether, the equipment has three nodes and one gateway. The gateway uses OPC interface, which passes the measurement information to the LabVIEW^{TM} development system. Test environment has potential sources of disturbances such as thick cement walls, metal pipes, humidity and varying temperatures. The wireless sensor network is presented in Figure 14.

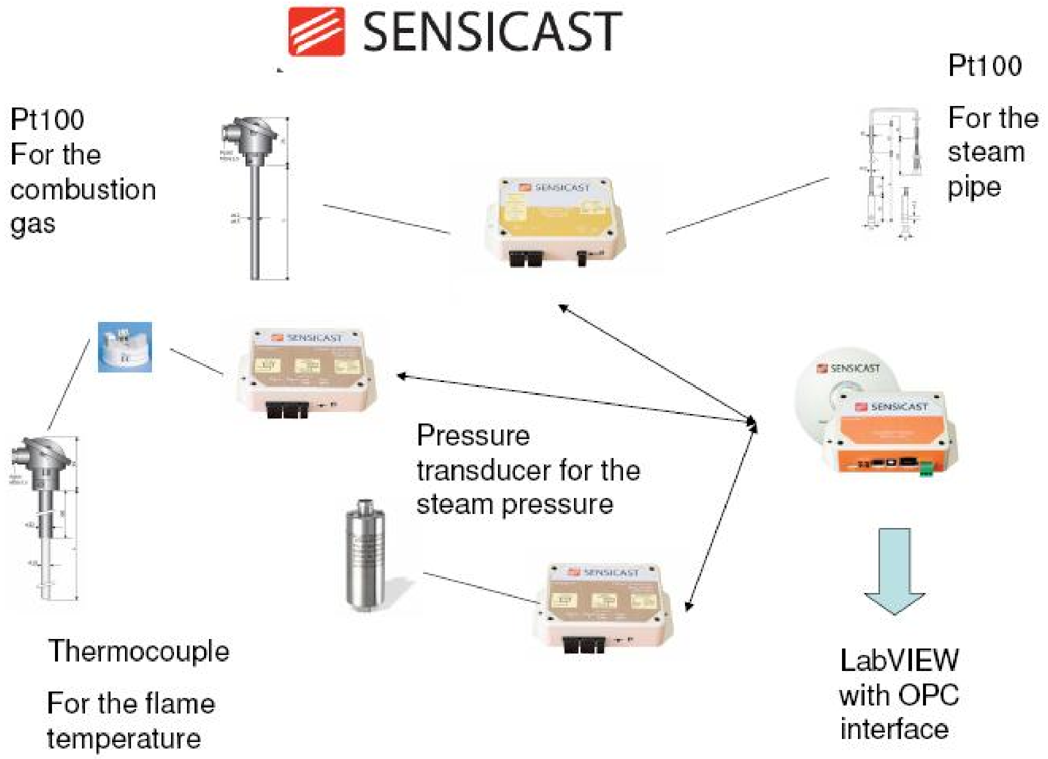


Figure 14. The WSN and sensors applied for monitoring the temperatures and the pressure of the steam boiler.

4.2 Use Case Scenario

A use case scenario was developed about the application example. The scenario is presented in Table 6. The template for the use case scenario was obtained from Tapio Frantti / VTT Technical Research Centre of Finland.

Table 6. Developed use case scenario.

Narrative Description:

An operator needs to monitor steam pressure and temperature, flame temperature and combustion gas temperature of a steam boiler. The monitoring is carried out both during operation and shutdown mode. During operation, the measurements can be utilised to control process operating temperature and pressure as well as to detect abnormal process conditions. Additionally, the data can be analysed for predictive maintenance purposes. During shutdown, the ambient temperatures are monitored to detect fire and prevent equipment from freezing.

Operator uses wireless sensor network to monitor process parameters. The WSN can be connected to the host PC via Ethernet/hub connection or over Local Area Network (LAN). The measured data is collected via OPC interface and displayed as trends in PC's monitoring software. Additionally, the data is stored for further analysis.

Use case:
Wireless_Monitoring_of_Temperature_And_Pressure_Of_A_Steam_Boiler

Description:
An operator monitors process parameters using wireless sensor network.

Actors:
-Operator (Primary)
-Wireless Sensor Network
-Local Area Network

Preconditions/Assumptions: -

Steps:
1. Configure the Wireless Sensor Network
1.1. Find out network structure
1.2.Configure connected measurements
1.3a)Configure Ethernet/hub connection between host PC and Bridge node
1.3b)Configure LAN connection between host PC and Bridge node
1.4 Start sending data via OPC interface

2. Display and store measured data in host PC
2.1 Start reading data via OPC interface
2.2 Display trends in monitoring application
2.3 Continuously store data for further use
2.4. Indicate abnormal situations for operator

Variations (optional):-

Non-functional requirements:
1. A/D-conversion should have accurate enough resolution
2. Node should have support for different types of sensor connections
3. Long battery life (high sampling rate may consume power significantly
4. Easy installation

Issues:-

Comments from the use case: External power was required for some sensors. Therefore, power wires were needed.

4.3 Requirements

A requirement analysis was performed for the application example. The original set of requirements was obtained from ESNA project. The requirements are presented in Table 7. Some requirements for the industrial real-time application were proposed to be added.

The added requirements are presented in Table 8. A set of requirements can also be found from (Willig, 2002).

Table 7. The original set of requirements.

Requirement	**Verbal value**	**Numerical value**	**Remarks**
Type of data VALUES: *event indication (on/off, something happened); slowly changing phenomenon such as temperature; rapidly changing phenomenon; streaming data (vibration, sound)*	Slowly Changing Phenomenon	1 meas / 2 min 6 meas/ 1 min	Shutdown Running
Sensing and control VALUES: only need to sense data; both sensing and control	Sensing		
Data rate VALUES: *very low (bytes / hour); low (bytes / minute); medium (bytes / second); high (kilobytes / second)*	Low to Medium		
Data delivery rate VALUES: *very low (1 / day) low (1 / hour) medium (1 / minute) high (1 / second)*	Medium to High	0.5/minute to 1/10s	
Sensing rate VALUES: *very low (1 / day) low (1 / hour) medium (1 / minute) high (1 / second) very high (1 / millisecond)*	Medium		
Acceptable latency(how long OK to wait for data) VALUES: *very high (day); high (hour); medium (minute), low (second); very low (millisecond)*	low	1-2 seconds	
Network scale (number of nodes) VALUES: 1-10; 10-100; 100-1000; 1000-		1-10	
Density (nodes / square meter) VALUES: *10 / m2 1 / m2 1 / 10 m2 1 / 100 m2*		1/m2	
Price sensitivity VALUES: *very high (0.1€) high (1€) medium (10€) low (100€) very low (1000€)*	low	100 €	
Localization precision VALUES: *0.01 m 0.1 m 1 m 10 m 100m*	Not applicable		
Harshness of environment(likeliness of hardware failure) VALUES: *rough (nodes might get destroyed) medium low (controlled laboratory experiment)*	rough		Nodes might get destroyed by high operating temperatures.
Expected lifetime VALUES: *years; one season; months; days; hours*	years		
Distance to monitoring entity VALUES: *other side of the world; kilometers; meters*	meters		
Mobility VALUES: *local; global*	local		
Security VALUES: *none; light; normal; heavy*	normal		No process control loop, therefore no need for high security.
Automatic system VALUES: *self connection; self routing; self adaptation; automatic fault recovering*	self connection, self routing, self adaptation, automatic fault recovering		

Table 8. Added proposals for requirements. When source is not marked in remarks, requirement is written by author.

Requirement	**Verbal value**	**Numerical value**	**Remarks**
Management /Configuration SW needed VALUES: *Yes; No*	Yes	-	Network setupe: need to configure e.g. used ports in nodes, sensor types and update rates. During operation: all these may be altered. Source: Shen et al., 2004
Application development SW needed VALUES: *Yes; No*	Yes	-	In example, firmware updates: nice-to-have.
Compliance with existing process automation standards and interfaces required VALUES: *Yes;No*	Yes	-	OPC compliance was essential for data gathering. Source: Shen et al., 2004
QoS VALUES: *Low / Medium / High*	Low	-	Includes Performance, QoS and adaptability issues (Section XX.) Source: Howitt et al., 2006
Support for heterogeneous network architecture needed VALUES: *Yes / No*	Yes	-	TCP / IP
Hardware Redundancy Needed VALUES*: Yes / No*	No	-	
Coexistence Values: *Yes / No*	No	-	No e.g. Wi-Fi links near. Source: Körber et al. 2007
Harshness of RF environment VALUES: *Low Interference / Medium Interference / High Interference*	Medium to High	-	Interference mainly time-variant (e.g. frequency converters) Source: Werb and Sexton, 2005
Support for Multiple Gateways Required? VALUES *Yes;No*	No	-	Source: ISA-SP100.11, 2006
Interoperability between devices (Nodes, Gateways) VALUES: *Yes;No*	No	-	Devices from one manufacturer. Source: Low et al., 2005
Safety Integrity Level (IEC 61508) VALUES: *SIL 1 / SIL 2 / SIL 3 / SIL 4*	SIL 1	-	Source: VAN, 2005
Data processing needed VALUES: *Yes /No*	Yes	-	Source: Virrankoski, 2007

5 DISCUSSION

5.1 General Considerations

Based on this review, it seems that there is a diverse, evolving field of wireless technologies suitable for process automation communications. As indicated in Sections 2 and 3; and in APPENDIX 1, in process automation, the resulting systems could often be hybrid by nature, incorporating existing automation systems and possibly heterogeneous wireless communication schemes. Therefore, interoperability of current and future wireless and wired applications may be a challenge, especially in the presence of rapidly evolving new technologies, industrial standards and proprietary solutions available.

Considering the wireless technologies presented in Section 2, the existing industrial automation wireless applications could be divided to two categories. First, a category, in which wireless communications is used as a backbone in communication architecture. In second category, wireless technology is applied to device level communication, delivering data from sensor to higher level in network hierarchy.

Employing wireless technologies in several levels of plant network hierarchy – from device level to remote connection – may introduce increased uncertainty in QoS indicators as the whole system perspective must be considered. This would, in turn, suggest distributed algorithms for some applications. For example, control applications are sensitive for varying delay in the feedback loop. Applying such a loop over wireless sensor network, wireless fieldbus and cellular link would provide increased uncertainties in terms of timeliness, jitter and latency, making the delay in feedback loop possibly more variable. Distributing the control to lower levels of network hierarchy might reduce the uncertainty.

At device level, based on use cases presented in APPENDIX 1, it seems that most of the current applications of wireless sensor networks in industrial automation have been focused on condition-based maintenance. Control applications are rare; the focus is mainly theoretical, although commercial application by ABB (wireless proximity switches) could be found. Additionally, remote monitoring approaches with complex network architectures, incorporating satellite and internet communications, could be found. Taking into account the manufacturing process example at aluminium plant and the event-based monitoring of relief valves, the applications support the proposed in the literature. Additionally, as presented in (Koumpis et al., 2006), applications related to monitoring are easier to find than those related in control.

Most of the wireless sensor network applications found during survey were based on 802.15.4-radio, with proprietary upper layer protocol stacks. For example, industrial applications using ZigBee are hard to find, but this may simply be because of the novelty of the technology. Quite recently, though, Mitsubishi announced a ZigBee-based WSN application for plant monitoring. Interestingly, in some cases it was mentioned that ZigBee is unable to cope with the requirements of industrial automation. (Dzung et al., 2005). and some discussion is ongoing about the ZigBee's applicability to industrial automation in internet publications. This suggests that the utilisation of ZigBee may also be application-specific, and its characteristics should be carefully considered based on requirements of application.

In general, it appears that most of the research in wireless sensor networks is based on communications technology and some less QoS intensive and harsh domains, such as environmental monitoring and building / home automation. Compared to that, relatively few articles could be found about industrial applications. Additionally, it seems that quite often the design of the applications starts from the network communications and wireless devices; instead, in process automation, the design should start from the process-point-of-view. One should consider e.g. process dynamics, required sampling rate (defined by the Nyquist criteria) and required accuracy for measurements. Similar approach is suggested also in (Bonivento et al., 2006).

5.2 Monitoring of the Steam Boiler: Experiences and Conclusions

Setting up the wireless sensor network for steam boiler monitoring was relatively straightforward and required very little previous knowledge about WSN, or networking in general. The selected network was self-organizing, so network was immediately functional when management software was installed and devices were turned on. Clearly, self-organization was considered as a beneficial and possibly mandatory requirement, which probably eases the technology adoption for industrial customers. Also the management software was considered to be very useful, at least in the setup phase and in problem solving (later, own application was developed for monitoring and data collection).

The only problems encountered in setup phase were related to Windows low-level application interfaces. The language version mismatch caused errors, preventing OPC-interface from working correctly. Later, another problem was detected: the host PC was unable to receive the messages from WSN gateway, when extended to monitor over LAN. The fault had not been previously experienced by the manufacturer's customers, so it might have been characteristic / configuration problem in the test environment. The solution was to separate both the host PC and WSN to their own network segment. However, this solution prevents the full usage of LAN, which may not be acceptable for industrial clients. These two issues in relatively simple environment lend support for importance of interoperability considerations.

Despite the wireless communication channel, lots of power wiring was needed. This was because of the amplifying and signal processing required by the S-type thermocouple and excitation power required by the pressure sensor. In order for the system to be truly wireless, these power wires should be replaced by wireless alternatives. However, the power need is beyond the capacity of current energy scavenging technologies. For improved energy efficiency, also advances in sensor technology (e.g. adaptation of MEMS to industrial measurements) to save power may be required. Indeed, when discussing the power usage and energy efficiency of the wireless system, one should consider whole system, rather than just a piece of it.

As suggested in the literature, it was noticed, that when designing a wireless sensor network for an application, the specification of the measurements (measuring ranges, operating temperatures, etc.) and knowledge about process and sensors is essential. Based on the requirements and knowledge, it is possible to draw requirements for the wireless sensor network. For example, when selecting the system provider, it could be noticed, that all the manufacturer's did not have accurate enough (12-bit was required) A/D-conversion for the pressure and temperature measurements needed to be implemented.

5.3 Future Work

Due to diversity of wireless technologies and hybrid nature of industrial implementations, interoperability may be an important issue to be investigated. A possible solution to tackle some interoperability problems could be the use of some design principles from software defined radio (SDR) and reconfigurable systems. Traditionally, SDR is considered as flexible end device reconfiguration by replacing radios implemented completely in hardware by those that are reconfigurable or even reprogrammable in software to a large extent. Reconfigurable systems extent the concept to take into account required network support and reconfiguration of application and services. The use of SDR in WSN has been proposed in (Ali et al., 2006) and in (Silverstrim et al., 2006).

It may also be useful to further deepen the knowledge about the different categories of industrial applications (see Section 3.3.2). The classification of applications could be supplemented for example by QoS issues and other relevant design criteria (presented in Section 3.4). This classification might be useful in e.g. deriving requirements, designing WSN architecture as well as selecting technology for an industrial automation application.

In order to gain advantage of the additional information the WSN provide, data processing methods may need to be addressed. Especially, data stream mining might be applicable in dealing with large amount of sensor data. The applications used in data processing should take into account the characteristics of the wireless sensor networks.

Based on the review, there seems to be some opposing opinions about interferences in industrial environments. According to some authors, the interferences may cause problems with wireless channel, while the others claim that these interferences are negligible. Therefore, systematic field experiments, taking into account different interference sources and proposed countermeasures might be needed.

6 CONCLUSION

This review firstly presented shortly the emerging and employed wireless technologies in process automation. Some standards, which may be relevant to industrial wireless systems, were then introduced. Wireless sensor networks and interferences in industrial environments, application classification and design criteria, were discussed a bit more detailed. Finally, a case example utilised in studying WSN applicability for process monitoring, was presented.

The review indicates that industrial implementations of wireless systems are often hybrid by nature, incorporating existing (legacy systems) and heterogeneous networks. Wireless technologies were used as a backbone in the network, or at device level, delivering data from sensor to upper level in network hierarchy. Compared to other domains, wireless industrial automation applications have stricter requirements for certain design criteria, e.g. QoS. Additionally, process automation applications should be designed from the process point-of-view, rather than the communication network.

Wireless sensor network could be utilised in monitoring of a steam boiler, although the solution was not truly wireless, due to required power cabling. In order to enable truly wireless sensor networks, the energy efficiency needs to be improved significantly, which may require advancements in several technology areas, for example in sensor technology and wireless communications. Interoperability showed to be an important design criteria also in case example.

Based on review, it was proposed, that the in future work, interoperability in hybrid networks and more detailed application classification taking into account the design criteria of industrial applications should be addressed. Also a systematic understanding of interferences in industrial environment should be acquired. Finally, the use of data processing techniques, e.g. data stream mining, to take advantage of the information provided by the WSN should be studied.

REFERENCES

Aakvaag, N., M. Mathiesen and G. Thonet (2005). Timing and Power Issues in Wireless Sensor Networks – an Industrial Test Case. In: *Proceedings of the 2005 International Conference on Parallel Processing Workshops*, 419-426.

ABIresearch® (2007). Key Developing Industrial Wireless Sensor Networking Standard Looks to IP. http://www.abiresearch.com/abiprdisplay.jsp?pressid=934 (30.10.2007).

Ailisto H., T. Matinmikko, J. Häikiö, A. Ylisaukko-oja, E. Strömmer, M. Hillukkala, A. Wallin, E. Siira, A. Pöyry, V. Törmänen, T. Huomo, T. Tuikka, S. Leskinen and J. Salonen (2007). Physical Browsing with NFC Technology. http://www.vtt.fi/vtt_show_record.jsp?target=julk&form=sdefe&search=57624 (30.10.2007).

Akan, Ö.B. and I.F. Akyildiz (2005). Event-to-Sink Reliable Transport in Wireless Sensor Networks. *IEEE/ACM Transactions on Networking*, **13**, 1003-1016.

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci (2002). A Survey on Sensor Networks. *IEEE Communications Magazine*, **40**, 102-114.

Ali, M., S. Umar, A. Dunkels, T. Voigt, K. Römer, K. Langendoen, J. Polastre and Z.A. Uzmi (2006). Medium Access Control Issues in Sensor Networks. *ACM SIGCOMM Computer Communication Review*, **36**, 33-36.

Anton, S.R. and H.A. Sodano (2007). A Review of Power Harvesting Using Piezoelectric Materials (2003-2006). *Smart Materials and Structures*, **16**, 1-21.

Baronti, P., P. Pillai, V.W.C. Chook, S. Chessa, A. Gotta and Y.F Hu (2007). Wireless Sensor Networks: A Survey on the State of the art and the 802.15.4 and ZigBee Standards. *Computer Communications*, **30**, 1655-1695.

Bonivento, A., L.P. Carloni and A. Sangiovanni-Vincentelli (2006). Platform-Based Design of Wireless Sensor Networks for Industrial Applications. In: *Proceedings of Design, Automation and Test in Europe, 2006*, **1**, 1-6.

Buckley J., K. Aherne, B. O'Flynn, J.Barton, A. Murphy and C. O'Mathuana (2006). Antenna Performance Measurements Using Wireless Sensor Networks. In: *Proceedings of the 56th Electronic Components and Technology Conference, 2006*, 1652-1657.

Cisco. Capacity Coverage & Deployment Considerations for IEEE 802.11g. http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_white_paper09186a00801d61a3.shtml (30.10.2007).

Cleaveland, P. The Explosive Growth of Wireless Communications Requires Well-Informed Decisions to Avoid Confusion. *IMPO*. http://www.impomag.com/scripts/ShowPR~PUBCODE~032~ACCT~0000100~ISSUE~0604~RELTYPE~PR~PRODCODE~0000~PRODLETT~A.asp (30.10.2007).

Culler, D., D. Estrin, and M. Srivastava (2004). Overview of Sensor Networks. *Computer*, **37**, 41-49.

Culler, D.E. and J. Hui. 6LoWPAN Tutorial. http://www.archrock.com/downloads/resources/6LoWPAN-tutorial.pdf (30.10.2007).

Cungor, V.C. and F.C. Lambert (2006). A Survey on Communication Networks for Electric System Automation. *Computer Networks*, **50**, 877-897.

Demirkol, I., C. Ersoy and F. Alagoz (2006). MAC Protocols for Wireless Sensor Networks: A Survey. *IEEE Communications Magazine*, **44**, 115-121.

Dzung, D., C. Apneseth, J. Endersen and J.-E. Frey (2005). Design and Implementation of a Real-Time Wireless Sensor/Actuator Communication System. In: *10th IEEE Conference on, Emerging Technologies and Factory Automation, 2005*, 443-442.

Emerson (2006a). Technology Selection. http://plantweb.emersonprocess.com/university/Library_Downloadable_Courses.asp#wir (30.10.2007).

Emerson (2006b). Wi-Fi Networks. http://plantweb.emersonprocess.com/university/Library_Downloadable_Courses.asp#wir (30.10.2007).

Eriksson L., and H.N. Koivo (2005). Tuning of Discrete-Time PID Controllers in Sensor Network Based Control Systems. In: *Proceedings 2005 IEEE International Symposium on Computational Intelligence in Robotics and Automation*, 359-364.

Gonia, P. and R. Budampati (2006). Wireless Network for Secure Industrial Applications. http://www1.eere.energy.gov/industry/sensors_automation/pdfs/meetings/0606/hw-wireless_gonia_0606.pdf (30.10.2007).

Hancke, G.P. and B. Allen (2006). Ultrawideband as an Industrial Wireless Solution. *Pervasive Computing, IEEE*, **5**, 78-85.

Horton, M. and J. Suh (2005). A Vision for Wireless Sensor Networks. In: *2005 IEEE MTT-S International Microwave Symposium Digest*, 361-364.

Hoske, M.T. (2006). Industrial Networks. *Control Engineering*, http://www.controleng.com/article/CA6347555.html (19.10.2007).

Howitt, I. and J.A. Gutierrez (2003). IEEE 802.15.4 Low Rate – Wireless Personal Area Network Coexistence Issues. In: *2003 IEEE Wireless Communications and Networking*, **3**, 1481-1486.

Howitt, I., W.W. Manges, P.T. Kurugati, G. Allgood, J.A. Gutierrez and J.M. Conrad (2006). Wireless Industrial Sensor Networks: Framework for QoS Assessment and QoS Management. *ISA Transactions*, **45**, 347-359.

Hu Y. (2001).: Satellite-Based Internet: A Tutorial. *IEEE Communications Magazine*, **39**, 154-162.

Hämäläinen P., M. Kuorilehto, T. Alho, M. Hännikäinen and T.D. Hämäläinen (2006). Security in Wireless Sensor Networks: Considerations and Experiments. In: *Embedded Computer Systems: Architectures, Modeling and Simulation*, 167-177.

IEEE 1451. Introduction to IEEE P1451. http://ieee1451.nist.gov/ (30.10.2007)

IDG Communications (2005). GM Cuts the Cords to Cut Costs. *Techworld.* http://www.techworld.com/mobility/features/index.cfm?featureid=1530 (30.10.2007).

IML Group plc (2007a). Wireless Networking in Process Automation: Building New Applications in 2007. *Control Engineering Europe*, February 2007, 36-39.

IML Group plc (2007b). Wireless Hart Specification Released. *Control Engineering Europe*, June/July 2007, 8.

Intel. Sensor Network Operation. http://www.intel.com/research/exploratory/sensornetwork_operation.htm# (31.10.2007)

ISA-SP100.11 (2006). Call for Proposal: Wireless for Industrial Process Measurement and Control. http://www.isa.org/filestore/ISASP100_11_CFP_14Jul06_Final.pdf (30.10.2007).

Jiang, P., H. Ren, L. Zhang, Z. Wang and A. Xue (2006). Reliable Application of Wireless Sensor Networks in Industrial Process Control. In: *Proceedings of the 6th World Congress on Intelligent Control and Automation*, 99-103.

van de Kar, E., Z. Lukszo and G. Leus (2006). Wireless Networks in the Process Industry: Opportunities for Ultrawideband Applications. In: *Proceedings of the 2006 IEEE International Conference on Networking, Sensing and Control, 2006*, 607-612.

Karlof, C. and D. Wagner (2003). Secure Routing in Wireless Sensor Networks: Attacs and Countermeasures. In: *Proceedings of the 2003 IEEE International Workshop on Sensor Network Protocols and Applications*, 113-127.

Kinnunen, L. (2007). Wireless Automation Provides both Opportunities and Challenges. *Automaatioväylä*, **23**, 26-28.

King, J. (2005). BP Pioneers Large Scale Use of Wireless Sensor Networks. *Computerworld*, http://www.computerworld.com/newsletter/0,4902,99962,00.html (19.10.2007).

Koumpis, C. (2006). Wireless in Industrial Applications.
http://host.quid5.net/~koumpis/talks/2006-10-26_IET_Reading.pdf (30.10.2007).

Koumpis, K., L. Hanna, M. Andersson and M. Johansson (2005). Wireless Industrial Control and Monitoring Beyond Cable Replacement, *Profibus International Conference, June 2005, Coombe Abbey, Warwickshire*, 1-7.

Körber H.-J., H. Wattar and G. Scholl (2007). Modular Wireless Real-Time Sensor/Actuator Network for Factory Automation Applications. *IEEE Transactions on Industrial Informatics*, **3**, 111-119.

Liu, Y. and R. Jäntti (2006). A Study Towards Enhanced Reliability Performance of Remote Control and Monitoring Application Over Commercial Wireless Communication Networks. In: *International Conference on Wireless Communications, Networking and Mobile Computing, 2006*, 1-4.

Low, K.S., W.N.N Win, and J.E. Meng (2005). Wireless Sensor Networks for Industrial Environments. In: *International Conference on Computational Modelling, Control and Automation, 2005 and International Conference on Intelligent Agents, Web Technologies, and Internet Commerce*, **2**, 271-276.

Mannion, P. (2006). Handset Forms Sensor Gateway. *Electronic Engineering Times*, http://www.eetonline.com/issue/fp/showArticle.jhtml;jsessionid=WUC44CIYYW0N4QSNDLRCKH0CJUNN2JVN?articleID=193105229&_requestid=912996 (30.10.2007).

Millenial Net. Wireless Networking for Remote Monitoring.
http://www.millennial.net/industries/ia_remotemonitoring.php (31.10.2007)

Paradiso, J.A. and T. Starner (2005). Energy Scavenging for Mobile and Wireless Electronics. *Pervasive Computing*, **4**, 18-27.

de Pellegrini, F., D. Miorandi, S. Vitturi and A. Zanella (2006). On the Use of Wireless Networks at Low Level of Factory Automation Systems. *IEEE Transactions on Industrial Informatics*, **2**, 129-143.

Perrig, A., J. Stankovich and D. Wagner (2004). Security in Wireless Sensor Networks. *Communications of the ACM*, **47**, 53-57.

Pinto, J. (2007). Industrial Wireless Standards. http://www.isa.org/Content/ContentGroups/News/20071/August37/Industrial_wireless_standards.htm (30.10.2007).

Porcino, D. and W. Hirt (2003). Ultra-Wideband Radio Technology: Potential and Challenges Ahead. *IEEE Communications Magazine*, **41**, 66-74.

Rabaey J., J. Ammer, J.L. da Silva Jr. and D. Patel (2000). PicoRadio: Ad-hoc Wireless Networking of Ubiquitous Low-Energy Sensor/Monitor Nodes. In: *Proceedings of the IEEE Computer Society Workshop on VLSI*, *2000*, 9-12.

Ramamurthy H., B.S. Prabhu, R. R. Gadh and A.M. Madni (2007). Wireless Industrial Monitoring and Control Using a Smart Sensor Platform. *IEEE Sensors Journal*, **7**, 611-618.

Roman, R., J. Zhou and J. Lopez (2005). On the Security of Wireless Sensor Networks. In: *Computational Science and Its Applications – ICCSA 2005*, 681-690.

RUNES. http://www.ist-runes.org/introduction.html (29.10.2007).

Sallinen, M., E. Strömmer and K. Känsälä (2007). Lyhyen kantaman tiedonsiirto mullistaa teollisuuden tiedonsiirron. *Automaatioväylä*, **23**, 32-35.

Sensicast (a). Montoring Giant Furnaces. http://www.sensicast.com/uploadedFiles/Resource_Center/Monitoring_Giant_Furnaces.pdf (31.10.2007).

Sensicast (b). Sensinet® Improves Efficiency in Compressed Air Systems While Reducing Operating Costs in Manufacturing Facilities. http://www.sensicast.com/uploadedFiles/hv.case.study.ver.6bb_casestudy.pdf (30.10.2007).

Sensicast (c). Sensinet® Wireless Temperature Monitoring Solutions Increases Throughput in Aluminium Plant. http://www.sensicast.com/uploadedFiles/CS-Alum.10.06_casestudy.pdf (31.10.2007).

Sereiko, P. (2007). Building the Perfect Beast. http://www.isa.org/InTechTemplate.cfm?Section=Article_Index1&template=/ContentManagement/ContentDisplay.cfm&ContentID=59875m (31.10.2007)

Sifakis E. (2006). Routing Protocols for Wireless Networked Sensing and Control Systems. http://etd.nd.edu/ETD-db/theses/available/etd-05252006-114853/unrestricted/SifakisE052006.pdf (31.10.2007)

Shen, X., Z. Wang and Y. Sun (2004). Wireless Sensor Networks for Industrial Applications. In: *Fifth World Congress on Intelligent Control and Automation, 2004*, **4**, 3636-3640.

Shi, E. and A. Perrig (2004). Designing Secure Sensor Networks. *IEEE Wireless Communications*, **11**, 38-43.

Silverstrim, J.E., W.E. Holland and K. Colling (2006). Method and Apparatus for Multi-Waveform Wireless Sensor Network. http://www.patentstorm.us/patents/7119676-claims.html (30.10.2007).

Sun, Y., Y.Q. Bian, P. Strauch and A.R. Nix (2007). Study of Radio Resource Sharing for Future Mobile WiMAX Applications with Relays. In: *IEEE Mobile WiMAX Symposium, 2007*, 91-97.

Stallings, W. (1995). Network and Internetwork Security: Principles and Practice. Prentice-Hall, USA (1995).

US Department of Energy (2002). Industrial Wireless Technology for the 21st century. http://www.energetics.com/rep_products.asp?Product=90 (30.10.2007).

VAN (2005). State of the Art and Trends in Safety, Security, Wireless Technologies and Real-Time Properties. http://www.van-eu.eu/deliverables (29.10.2007).

Virrankoski R. (2007). Langaton tiedonsiirto tehdasautomaatiossa. http://www.smartsystems.fi/konferenssimateriaalit.html (30.10.2007)

Welander, P. (2007). Industrial Networking. *Control Engineering*, **54**, 59. http://proquest.umi.com/pqdlink?Ver=1&Exp=07-09-2012&FMT=7&DID=1255353221&RQT=309&cfc=1 (30.10.2007).

Werb, J. and D. Sexton (2005). Improved Quality of Service in IEEE 802.15.4 Mesh Networks. *International Workshop on Wireless and Industrial Automation, San Fransisco, California, March 7, 2005*, 1-6.

Wiberg, P.-A. and U. Bilstrup (2001). Wireless Technology in Industry – Applications and User Scenarios. In: *Proceedings of the 2001 8th IEEE International Conference on Emerging Technologies and Factory Automation (2001)*, **1**, 123-131.

Willig, A. (2002). Investigations on MAC and Link Layer for a Wireless PROFIBUS over IEEE 802.11. http://edocs.tu-berlin.de/diss/2002/willig_andreas.pdf (29.10.2007).

Willig, A., K. Matheus and A. Wolisz (2005). Wireless Technology in Industrial Networks. In: *Proceedings of the IEEE*, **93**, 1130-1151.

Yeager, D.J., A.P. Sample, J.R. Smith, P.S. Powledge and A.V. Mamishev (2006). Sensor Applications in RFID Technology. In: *International Conference on Actual Problems of Electron Devices Engineering*, 449-452.

Zeng, W., H. Wang , H. Yu and A. Xu (2006). The Research and Application of UWB Based Industrial Network. In: *The Third Industrial Conference on Ultrawideband and Ultrashort Impulse Signals*, 153-155.

Condition-Based Maintenance, General Use Case

Narrative Description:

Physical structure, such as machine, motor, airplane wing, bridge or building has typical modes of vibration, acoustic emissions and response to stimuli. Variations in these behaviours can indicate wear, fatigue, or other mechanical challenges. For example, a bearing will often squeak and shudder before it seizes up. (Culler et al., 2004)

Often, an operator is required to gather data manually/with a computing device from the sensors attached to production equipment. The logs are then carried out to central computer, which analyses the data and e.g. for the signs of wear. The time between visits at a particular machine may be months. WSN offers alternative approach to condition monitoring: performing local processing at each device and transporting the data continuously to operations staff. (Culler et al., 2004)

Some example sampling rates for condition monitoring: about 100 Hz for vibration analysis and several kHz for acoustic analysis, which are considerably higher than in environmental monitoring. Higher sampling rate requires more energetic sampling activity and greater care in how network performs sampling. Buffering data needs greater amounts of storage and the system may perform more extensive local processing on data chunks sampled intermittently. (Culler et al., 2004)

Instead of transmitting large amount of raw data, the sensor nodes can perform signal analysis, communicating only the modes of vibration and anomalies. Sensor nodes could also monitor control networks to find out what is active when the sample is taken or even to determine when to sample. Because reducing costs of obtaining and processing data reduces overall costs, improving timeliness of analysis can improve plant performance (Culler et al., 2004).

Use case:

Condition_Based_Maintenance_General

Description:

Preventive maintenance is carried out to reduce unwanted downtime by condition-based maintenance.
Sources: (Culler et al., 2004)

Actors:

Operator (Primary), Wireless Sensor Network, Local Area Network, Production Equipment

Preconditions/Assumptions:

Steps:

a)
1. Measure defined physical stimuli from production equipment
2. Send data continuously to sink
3. Transfer data e.g. to control room PC over LAN
4. Display data in monitoring application.
5. Analyze data for anomalies.

b)
1. Measure defined physical stimuli from production equipment
2. Analyze data locally
3. If an anomaly is detected, send alert (and data) to sink
4. Transfer data e.g. to control room PC over LAN
5. Display alert (and data) in monitoring

Variations (optional):

Non-functional requirements:

1. External power may be required for some sensors
2. A/D-conversion should have accurate enough resolution
3. Node should have support for different types of sensor connections
4. Long battery life (high sampling rate may consume power significantly)

Issues:

Comments from the use case:

Condition-Based Maintenance, Monitoring Compressed Air System

Narrative Description Compressed air systems degrade over time and tend to come leaky and inefficient, which is compensated by increasing line pressure. If the inspections are run seldom (according to (Sensicast, (b)), typically once a year), the system works inefficiently and use excessive electricity for long periods of time. (Sensicast, b) Wireless Sensor Network has been implemented to monitor compressed air system in a paper plant /Sensicast/. Monitored parameters were for example temperature, line pressure, airflow, and compressor energy usage. Monitoring software was used to display data and detect trends leading to system degradation. The monitoring and reporting interval was set to one minute. Hence, knowledge about small changes in system was available accurately. The system was reported to increase compressed air systems efficiency by 50%. (Sensicast, b)
Use case: Monitoring_Compressed_Air_System
Description: Increase compressed air system's efficiency by monitoring operating parameters and detecting degradation. Source: (Sensicast, b)
Actors: Operator, Wireless Sensor Network, Compressed Air System
Preconditions/Assumptions:
Steps: 1. Measure defined physical stimuli from production equipment 2. Send data continuously to sink 3. Display data in monitoring application. 4. Analyze data for anomalies.
Variations (optional):
Non-functional requirements: 1. External power may be required for some sensors 2. A/D-conversion should have accurate enough resolution 3. Node should have support for different types of sensor connections 4. Long battery life (high sampling rate may consume power significantly)
Issues:
Comments from the use case:

Condition-Based Maintenance, Vibration Monitoring of a Robot in a Manufacturing Cell

Narrative Description

A manufacturing cell is a stage of automation line in an industrial plant. In this scenario, robots equipped with drilling tips work with metal surfaces. Monitoring the state of the drilling tip is considered to be important because they wear out and need to be replaced before damaging both the piece under construction and the robot itself. (Bonivento et al., 2006)

Typically, the monitoring is carried out by different vibration sensors placed on the robot. If a certain threshold of vibration intensity is exceeded, the equipment is stopped in order to safely perform maintenance. The monitoring task is carried out by a PLC unit, which queries periodically each cluster for information on the vibration intensity for the robots. (Bonivento et al., 2006)

Use case:

Vibration_Monitoring_Manufacturing_Cell

Description:

Detect tool wear by monitoring vibration in production equipment.
Sources: (Bonivento et al., 2006)

Actors:

Operator (Primary), Wireless Sensor Network, Production Equipment

Preconditions/Assumptions:

Steps:

1. PLC queries WSN for vibration patterns
2. WSN measures vibration patterns
3. WSN sends information to PLC
4. PLC: Anomaly detected?
4.1 No ➔ Continue production
4.2 Yes ➔ Stop production equipment

Variations (optional):

Non-functional requirements:

1. External power may be required for some sensors
2. A/D-conversion should have accurate enough resolution
3. Node should have support for different types of sensor connections
4. Long battery life (high sampling rate may consume power significantly)

Issues:

Comments from the use case:

Condition-Based Maintenance, Detecting Vibration in Water Purication Equipment

Narrative Description

A trial deployment of a wireless sensor network to monitor the health of semiconductor fabrication equipment is presented in (Intel). Specifically, the network monitors the vibration signature of water purification equipment, providing data for preventive maintenance operations.

Currently manual monitoring is used to predict failures and schedule maintenance or replacement to avoid costly manufacturing downtime. Deploying wireless sensor networks would provide more frequent and more reliable data, reduce equipment downtime and eliminate costly manual equipment monitoring. (Intel)

Use case:

Vibration_Monitoring_Water_Purification

Description:

Monitor vibration signature of water purification equipment for preventive maintenance operations.
Sources: **(**Intel)

Actors:

Operator (Primary), Wireless Sensor Network, Production Equipment

Preconditions/Assumptions:

Steps:

1. Query for vibration patterns to WSN
2. WSN measures vibration patterns
3. WSN sends information to sink
4. Anomaly detected?
4.1 No ➔ Continue purification
4.2 Yes ➔ Perform maintenance activities

Variations (optional):

Non-functional requirements:

1. External power may be required for some sensors
2. A/D-conversion should have accurate enough resolution
3. Node should have support for different types of sensor connections
4. Long battery life (high sampling rate may consume power significantly)

Issues:

Comments from the use case:

Condition-Based Maintenance, Monitoring Steel Furnace

Narrative Description:

In /Sensifur/, a wireless sensor network was used to monitor temperature fluctuations in water jackets of steel furnaces. In the monitoring environment, there are extreme temperatures and harsh chemical, metallurgical, and mechanical processes. At some point of the steel making process, electrical current often arcs to the sides of the furnaces, heating its walls and sometimes overloading its temperature control mechanism. If the cooling system would fail, the production equipment as well as the lives of the operating personnel would be endangered. (Sensicast, a)

Wireless solution was selected, because the installation of the sensors had to be carried out quickly, and high heat and difficult positioning made the use of wired sensors impossible. Temperature sensing nodes were installed between the inner and outer walls of the furnace. They were reported to be able to withstand the heat from melting steel, wide temperature variations, powerful magnetic fields, water spray, and vibration. (Sensicast, a)

The wireless technology routes data around any temporary obstacles that might occur. Frequency hopping was employed to select the best channel for clear communication. OPC interface was utilised in delivering data directly to the control system. (Sensicast, a)

Use case:

Monitoring_Steel_Furnace

Description:

A wireless sensor network is used to monitor the cooling system of the steel furnace.
Source: (Sensicast, a)

Actors:

Operator (Primary), Wireless Sensor Network, Plant’s control system

Preconditions/Assumptions:

Steps:

1. Measure temperature data
2. Try to send temperature data to sink
2.1 a) If sending fails, try another route / channel
2.1 b) If sending was successful, continue monitoring task

Variations (optional):

Non-functional requirements:

1. External power may be required for some sensors
2. A/D-conversion should have accurate enough resolution
3. Node should have support for different types of sensor connections
4. Long battery life (high sampling rate may consume power significantly)
5. Perform reliably in extremely harsh conditions (strong magnetic and electrical fields, large masses of steel interrupting communications, wide temperature variations, water sprays, vibrations)

Issues:

Comments from the use case:

Condition-Based Maintenance and Diagnostics, Pulp and Paper Mills

Narrative Description

An example about using wireless sensor networks for diagnostic and preventative maintenance purposes at pulp and paper mills is presented in (Shen et al., 2004). The rolling machines at the mills are massive, complex mechanisms. Even small variations in the speed, temperature or alignment of the rollers can have serious effects on quality or operation. (Shen et al., 2004)

WSN could be utilised in investigating and resolving unanticipated circumstances such as variations in output quality, unusual vibration or noise, or other signs for potential problems. Examples about measured quantities are temperature, speed, pressure, and vibration. Technicians could attach the required sensor nodes to the areas of interest in the machine or process line. The nodes could use wireless RF communications to relay data to portable or handheld device. The wireless measurement system should be quickly installed and rapidly removed once problems are identified and resolved. (Shen et al., 2004)

Use case:

Pulp_And_Paper_Mills

Description:

WSN is utilized to solve quality problems and for preventive maintenance operations at pulp and paper mills.
Source: (Shen et al., 2004)

Actors:

Operator (Primary), Wireless Sensor Network, Portable / Handheld Device, Production Equipment

Preconditions/Assumptions:

Steps:

1. Attach nodes to area of interest
2. Form wireless sensor network
3. Measure specified quantity
4. Transmit data to portable / handheld device

Variations (optional):

Non-functional requirements:

1. External power may be required for some sensors
2. A/D-conversion should have accurate enough resolution
3. Node should have support for different types of sensor connections
4. Long battery life (high sampling rate may consume power significantly)
5. Rapid installation and removal of WSN

Issues:

Comments from the use case:

Condition Based Maintenance, Monitoring Pump Wear

Narrative Description In (Aakvaag et al., 2005), an experimental network developed by ABB and Metso is presented. The WSN was implemented at a mining company, Metso supplying automation equipment and ABB delivering the automation system. At the facility, there are 200 pumps, which were reported to have uneven and unpredictable wear of rubber parts. On average, a wear part had to be replaced three times a year. Metso was working on "smart wear parts", which would detect tear and wear in rubber and then deliver acquired information from pumps to central location for integration. (Aakvaag et al., 2005) The wear sensing unit consisted of two parts: RFID tag and a radio-equipped unit. The RFID tag would transmit pump identification and wear data across to radio unit. (Aakvaag et al., 2005) The, developed solution, EmberNet, was a multi-hop network using an ad-hoc on-demand distance routing (AODV) algorithm. The network consisted of seven nodes, which would exchange data once per minute, and a gateway node. The application programming interface API supported two types of packets, broadcast and unicast, from which broadcast was used. The broadcast method sent packet three times (time between retransmissions was 100 ms) in order to ensure successful transmission (the number of retransmissions could not be altered, which was a limitation for the system). Maximum radius (maximum number of radio hops that a packet can propagate from originator) was utilised to prevent network from flooding. (Aakvaag et al., 2005)
Use case: Monitoring_Pump_Wear
Description: Wireless Sensor Network is used to detect wear and tear in rubber parts of pumps. Sources: (Aakvaag et al., 2005)
Actors: Operator (Primary), WSN, Production Equipment
Preconditions/Assumptions:
Steps: 1. Measure wear data 2. Transmit data to gateway node 3 times (broadcast) 3. Go to sleep mode, wait for the next measurement period.
Variations (optional):
Non-functional requirements: 1. A/D-conversion should have accurate enough resolution 2. Node should have support for different types of sensor connections 3. Long battery life (high sampling rate may consume power significantly) 4. Rapid installation and removal of WSN
Issues:
Comments from the use case:

Control Applications, Wireless Networked Control Systems

Narrative Description

Wireless Networked Control Systems, WNCS, consists of sensors, actuators and controllers, which are connected over a wireless communication channel. The sensing nodes take measurements related to a phenomenon and route these measurements to the actuator/controller; second, actuators and controllers in charge of receiving sensed data and sending a control command to the plant. The system must satisfy timeliness requirements in order to avoid instabilities. Compared to wireless sensor networks, they usually require sending more data packets of smaller size. However, in some cases, the time frame for sending packets may be small, which may increase periodic data rate. Additionally, wireless sensor networks usually have one base station or data sink while wireless networked control systems have many actuators/controllers which behave like data sinks. (Sifakis, 2006)

Wireless communication channel for control applications brings new challenges in the form of higher bit error rates and communication latencies. These characteristics may lead to decreased phase margins, which can destabilize the system. (Sifakis, 2006)

Use case:

Wireless_Network_Control_Systems

Description:

Wireless Networked Control Systems perform sensing and control over wireless communication channel.
Sources: (Sifakis, 2006)

Actors:

Controller (Primary), WNCS, Plant Equipment

Preconditions/Assumptions:

Steps:

Variations (optional):

Non-functional requirements:

Issues:

Comments from the use case:

Steps not included due to general nature of use case.

Control Applications, A PID Controller in a Feedback Loop

Narrative Description

In (Erikkson and Koivo, 2005), a new tuning method is developed for discrete-time PID controllers in networked control systems where time-varying delays are present. The control system is comprised of a process, a discrete-time PID controller, an actuator and a wireless sensor network.

Although many processes have multiple inputs and multiple outputs (MIMO), they are often controlled with single input-single output (SISO) controllers. Therefore, data fusion needs to be applied over multiple sensor readings. (Erikkson and Koivo, 2005)

The use of sensor networks in process control is based on fact that there is no need for expensive cabling of sensors, and free mobility. There is also more freedom if the monitored process is far away from the controller or if the process is very wide, and it is difficult or impossible to use wired coupling. However, multiple sensors are required for redundancy and for guaranteeing reliable operation of the whole measurement system. (Erikkson and Koivo, 2005)

Use case:

PID_Control_System_In_Wireless_Feedback_Loop

Description:

PID control system is used in wireless feedback loop
Source: (Erikkson and Koivo, 2005)

Actors:

Controller(Primary), Wireless Networked Control System, Process, Actuator

Preconditions/Assumptions:

Steps:

1. Data is acquired from multiple sensors.
2. Data is transmitted over wireless communication channel to e.g. sink/host PC.
3. Data fusion is carried out to fuse multiple sensor readings.
4. Fused data is transmitted to controller over wireless channel.
4. Controller calculates control signal and transmits the signal to actuator using wireless communication channel.

Variations (optional):

Only one potential case of multiple sensors described in steps.

Non-functional requirements:

1. Low battery consumption
2. QoS (strict with timeliness, jitter ➔ variable delays cause instability in control loop)
3. Sensor nodes should have support for different sensor connections

Issues:

Comments from the use case:

Control Applications, Wireless Sensor/Actuator Network in Robotic Installation

Narrative Description

(Dzung et al., 2005) describes design and implementation of a real-time wireless sensor/actuator communication system. Requirements for industrial automation applications using production machines and robotic installations are also presented (in addition to the general requirements of high reliability and low and predicable data transfer): (Dzung et al., 2005)

- Fast response time (generally less than 10-15 ms for real-time applications)
- Serve large number (up to 120) of sensors/actuators located in a cell of several meters radius
- guarantee high reliability of data transmission even in unfriendly environment of factories, where radio propagation may be affected by many obstacles and where various sources of interfering signals must be expected
- have low power consumption

Fast response times were achieved. The system was tested in factory environment and products based on it are commercially available (ABB, wireless proximity switches). According to authors, the design criteria related to response times as well as number of sensors / actuators differ by orders of magnitude from the design goals of existing wireless systems such as Bluetooth or ZigBee. (Dzung et al., 2005)

Use case:

WSAN_Production_Machines_Robotic_Installations

Description:

Wireless Sensor and actuator network (WSAN) is utilised in real-time wireless sensor/actuator communication system (wireless proximity switches).
Source: (Dzung et al., 2005)

Actors:

Controller (primary), WSAN, Production Equipment

Preconditions/Assumptions:

Steps:

1. Node transmits proximity data from to base station (BS)
2. Base station maps the wireless links to fieldbus addresses and connects links to automation controller (PLC)
3. Base station sends the data to PLC
4. PLC sends control command to BS (e.g. based on data)
6. Control command is send to actuator from BS (wirelessly)

Variations (optional):

Non-functional requirements:

1. A/D-conversion should have accurate enough resolution
2. Node should have support for different types of sensor connections
3. Fast response times
4. High number of nodes to be served
5. High reliability
6. Low power consumption

Issues:

Comments from the use case:

Remote Monitoring, Monitoring For Tank Levels of Natural Gas By-Products

Narrative Description

The process of extracting natural gas produces by-products, such as such as hydrocarbons, oil and water, which are stored in tanks in the gas fields and trucked off site on a scheduled basis. Utilising wireless communication channels for measurements (pressure, temperature, flow and level) was considered to enable the trucks to make pickup based on need rather than timed schedule. (Millenial Net)

A self-sufficient, self-powered wireless sensor network was employed to collect and communicate vital operational data to a remote monitoring centre via satellite to an Internet backbone. The solution was reported to enable moving away from scheduled maintenance to just-in-time, as-needed basis. Additionally, gathered data could be utilized in improving the gas extraction process. (Millenial Net)

Use case:

Remote_Monitoring_Natural_Gas

Description:

WSN is utilised to enable just-in-time basis maintenance pickups from remote tanks.
Source: (Millenial Net)

Actors:

Operator (Primary), Satellite Network, Internet, WSN, Production Equipment

Preconditions/Assumptions:

Steps:

1. Sensor node detects high level for some by-product measurement.
2. Data is sent via satellite to internet backbone
3. Data is displayed at the monitoring application and maintenance is delivered.

Variations (optional):

Non-functional requirements:

1. Ability to withstand changes in weather conditions
2. Long battery life

Issues:

Comments from the use case:

Remote Monitoring, Monitoring LPG Level

Narrative Description A London-based company is also remotely monitoring its industrial customers' LPG tank fill levels, using battery-powered ultrasonic sensors that transmit information by radio signal to a low Earth orbit satellite, which relays the data to the company information system. The technology is operational on about 200 tanks in England and is being deployed across Europe. WSN was utilised to gauge how much LPG remained in large tanks to enable just-in-time deliveries. (King, 2005)
Use case: Remote_Monitoring_of_Tank_Levels
Description: WSN is utilised in tank level monitoring to enable just-in-time deliveries. Source: (King, 2005)
Actors: Operator (Primary), Satellite, WSN, Refinery Equipment
Preconditions/Assumptions:
Steps: 1. Sensor measures the LPG level in the tank 2. Data is transmitted to sink via wireless communication channel 3. Data is transmitted to remote office via low-Earth satellite. 4. Tank level data is displayed at the monitoring software.
Variations (optional):
Non-functional requirements: 1. Ability to withstand changes in weather conditions 2. Long battery life
Issues:
Comments from the use case:

Other Applications, Monitoring Aluminium Rolls in Cooling Phase

Narrative Description

A company's uses a cold rolling process to produce rolled aluminium goods. As a result of the rolling process, metal is heated to 225 degrees and is let cool to 100 degrees at the cooling stations, which cover an area about a football field. An overhead crane manually monitors the temperatures of about 100 rolls to determine when they are cool enough to move. The measurement process was considered to be time-consuming, because the operator had to climb down from an overhead crane to perform the measurements. (Sensicast, c)

A wireless temperature monitoring system was deployed in the plant, which automatically monitors the temperature of the rolls in the cooling stations every minute. The data is wirelessly transmitted to a computer in the cab of the crane. The need for manual measurements could be eliminated. And an increase of 2.3 million kilograms in annual throughput was observed due to the improvement. (Sensicast, c)

Use case:

Monitoring_Aluminium_Rolls_In_Cooling_Phase

Description:

WSN is utilised to improve temperature monitoring at a aluminium factory.
Source: (Sensicast, c)

Actors:

Operator (Primary), Wireless Sensor Network, Aluminium Rolls

Preconditions/Assumptions:

Steps:

1. Temperature monitoring sensor node is attached to aluminium roll.
2. Network accepts a new node to the network.
3. Node measures a temperature of an aluminium roll.
4. Temperature is transmitted over wireless communication channel to the gateway in the overhead crane.
5. Data is transferred to PC and displayed at the monitoring software.
6. Once the roll is cooled down, remove the sensor node and dismiss the node from the network.

Variations (optional):

Non-functional requirements:

1. Rapid installation and removal of WSN
2. Nodes should withstand high temperatures

Issues:

Comments from the use case:

Other Applications, Relief Valve

Narrative Description:

Petroleum companies are among the largest worldwide consumers of control and automation products, and therefore, a potential applier of wireless automation technology. In an oil refinery, a relief valve is a purely mechanical device used to protect equipment from overpressure, when refining process is out of balance. (Sereiko, 2007)

A typical refinery covers over 8 hectares and can have between seven and 10 different processing areas where hydrocarbon emissions may occur. Each of these areas is about 100 square meters and can contain over 200 relief valves. (Sereiko, 2007)

There may be several reasons for gas pressure to builds up in the refinery setting. When the pressure goes above a predetermined, safe level of pressure the relief valve opens and gas vents to the atmosphere. When the pressure drops back to acceptable level, the relief valve closes. Regulatory limitations provide thresholds for the emissions, and if those are exceeded, the refinery must pay fine. Therefore, it is economically feasible to monitor the emissions. (Sereiko, 2007)

Wireless sensor networks are applicable for monitoring the emissions, because they do not require cabling, which would be costly due to large area covered by oil refinery. The measurements would be based on acoustic emission, produced by the hissing sound, which gas makes as it escapes from the valve. Furthermore, after capturing the information is solved, the emission information could be utilised in plant’s control system to further enhance efficiency of the project. (Sereiko, 2007)

Use case:

WSN_Relief_Valve_Monitoring

Description:

WSN is utilised in monitoring of relief valves.
Source: (Sereiko, 2007)

Actors:

Operator (Primary), WSN, Relief Valve, Data Storing Equipment

Preconditions/Assumptions:

Steps:

1. Valve opens.
2. Sensor node detects hissing sound produced by gas escaping from the valve. Node starts timer.
3. Sensor node detects end of the sound and stops timer.
4. The duration of gas emission is routed e.g. to PC via mesh network and stored in database.

Variations (optional):

Non-functional requirements:

1. Ability to withstand changes in weather conditions
2. Long battery life

Issues:

Comments from the use case: