Wireless Automation

Scholl, Gerd
Professur für Elektrische Messtechnik
Helmut-Schmidt-Universität, Universität der Bundeswehr, Hamburg
Holstenhofweg 85
22043 Hamburg

Abstract – Resource conserving weight, material and energy savings, achievement of compliance with new environmental and safety requirements, cost-efficient retrofitting of already existing monitoring and control systems, improvement of labor productivity, inventory optimization, mobile operation and tracking, remote control and maintenance or alleviation and acceleration of awkward or laborious installations are only some reasons boosting wireless technologies in automation applications. Highly matured low-power CMOS technologies with an ever-increasing performance and steadily shrinking chip-sizes enable the integration of microelectronic components and systems into machines, tools, sensors and actuators. Compared with, e.g. the mobile phone market, the market for machine-to-machine communication is much more conservative and diversified. A single wireless solution cannot deliver all the benefits in every situation and must be tailored to the requirements of the different market segments, which can roughly be subdivided into transportation and logistics, building automation, factory and process automation and infrastructure plants. Thus, the wireless automation market offers opportunities for creative ideas for highly specialized applications but also requires industry standards to guarantee systems interoperability and to increase quantities. Even a discussion of only a subset of the various solutions already available on the market goes far beyond the scope of this paper. Therefore, this article is focused on processs and factory automation, outlining newest trends and developments in the field.

1. INTRODUCTION

While proprietary wireless technologies have been used for automation applications in a limited fashion since the 1980s, users were reluctant to adopt wireless technologies originally determined for office or consumer applications. Main concerns were high security and safety requirements, battery lifetime, interoperability and scalability, interference of radio signals with other radio services and electromagnetic radiation, emitted from e.g. spot welding robots, induction heaters or inverter controlled motors. In recent years automation and wireless-technology suppliers are addressing these and other concerns. Analysis of inter-device industrial wireless communications by the International Society of Automation (ISA) resulted in a partitioning of industrial communication systems into three categories: monitoring, control and safety. Two of theses categories, monitoring and control, are further subdivided into two and three classes, respectively, so that in total six safety levels are defined, where class 0 denotes the highest safety level (emergency action) and class 5 stands for the lowest safety level (monitoring without immediate operational consequences). For all safety levels wireless products are already available. Examples for extremely robust wireless data transmission systems are [1-5]. By modifying the eleven-chip Barker spreading sequence employed in 802.11b Wi-Fi modules a very high interference immunity against other Wi-Fi systems also operating in the 2.45 GHz ISM band could be achieved. Depending on the application a wireless PROFIsafe data transfer, which is the extension of the standard PROFIBUS or PROFInet to address special requirements for safety related information, can be realized with various Wi-Fi standards, Bluetooth, DECT or upbanded DECT radio solutions [1]. In [2] a highly robust wireless data transmission is achieved on the basis of chirp spread spectrum technology. With a bandwidth of 64 MHz and a symbol length of 1μs the processing gain is 64 or 18 dB, which allows to detect very weak signals even in strong interference situations or noise. A frequency hopping spread spectrum technology with up to 830 individual hop-channels for industrial applications was developed by [3]. Fail-safe point-to-point wireless transmission via PROFInet was realized using two redundant wireless links in the 2.45 GHz and/or 5 GHz ISM-bands [4]. Even in a heavily interference-prone environment wireless technologies can be integrated into an industrial communication system employing leaky wave cables [4] or slotted waveguides [5]. Today, Wi-Fi and Bluetooth are well established for secure and robust factory and process automation applications [1-10]. Wi-Fi systems can provide an excellent backbone for data concentration and networking. They also allow wireless access to field devices for configuration and testing, linking of communication segments for rapid commissioning, communication with dynamic stations as stacker trucks, conveyor lines or trolleys, and also give mobile workers access to up-to-date control and

maintenance data, wherever they are. As Bluetooth uses tiny, inexpensive, short-range radio transceivers, this technology is ideally suited to be embedded into sensors or actuators connecting them to a programmable logic controller (PLC). Other applications are serial cable replacement or wireless access points [7-9]. A Bluetooth piconet can have up to eight devices, typically, but also wireless systems, where up to 250 Bluetooth modules can be clustered, are already available [10]. A multi-hop Bluetooth tree-network can be automatically established using the standard serial port profile so that almost any commercially available Bluetooth device can be integrated into the network. The first commercially available wireless sensor network solution for low-data rate home, building and industrial automation applications was ZigBee. The ZigBee 1.0 specifications was ratified in December 2004 followed by releases ZigBee 2006 and Zigbee 2007/PRO with improved functionalities in December 2006 and October 2007, respectively. Zigbee provides the network and applications layers on top of the IEEE standard 802.15.4, defining the physical and data link layer of the International Standard Organization (ISO) Open System Interconnection (OSI) protocol reference model [11]. Also at the end of 2007 the HART Communication Foundation (HCF) announced the HART 7 specification including WirelessHART, a standard specifically designed for process measurement and control applications.

The next section is focused on process automation, reviewing the basic features of ZigBee [12] and WirelessHART [13]. Section three deals with factory automation. First, WISA [14], the wireless interface for sensors and actuators is outlined, an innovative combination of a low-latency wireless sensor/actuator control network with magnetic field powered sensors. Then the latest results of a feasibility study, carried out in the public funded project EnAS [15], concerning energy-autonomous wireless sensor/actuator communication will be presented.

2. PROCESS AUTOMATION

Compared with office applications industrial applications have stricter timing requirements and higher security concern, i.e. the maximum allowable delay for end-to-end communication must be guaranteed and the protocol stack should support extensive security services. As wireless communication in an industrial environment is exposed to interference, especially when operated in the 2,45 GHz ISM-band, frequency of operation should be adjusted dynamically and channels, where interference is persistent or communication is blocked, should be ignored. The network should also be easy to install, flexible, scalable, self-organizing and self-healing. Other requirements are: cost and time saving installation, low maintenance costs, engineering and diagnosis tools should be based on standards already known by the technical staff, simple integration of additional sensors or actuators into the existing sensor network and an efficient power management for long-term operation.

Due to the limited space available and as both specifications, ZigBee as well as WirelessHART, include several hundred pages, only the main features can be highlighted here.

ZigBee and the IEEE standard 802.15.4 [16] provide the network infrastructure for wireless sensor network applications. 802.15.4 defines the physical and MAC layers, and ZigBee defines the network and applications layers. Wireless HART also relies on the the physical layer of 802.15.4, but specifies additionally to the transport and applications layers its own data-link layer. More than 26 million wired HART devices are already installed in the field. To ensure compatibility protocol stacks of HART and WirelessHART are compatible in the transport and application layers, allowing the user to employ the same engineering tools and practices he already knows. WirelessHART is a contention-free, time-synchronized protocol with an accuracy of 1 ms across the entire network. The basics for network synchronization were developed by DustNetworks [17]. Time division multiple access (TDMA) is used to provide collision free and deterministic communications. All devices must support superframes, which are formed by a sequence of time slots, each having a length of 10 ms. Typically, a communication transaction between two devices are assigned to a given time slot. To enhance reliability, channel hopping is combined with TDMA so that each slot may be used on multiple channels at the same time by different nodes. All devices in the network share an identical channel list indicating which channel can be used.

The life of a ZigBee network begins when a router uses the radio-signal-strength-indicator (RSSI) to look for an interference-free channel, and then sets itself up to be the network coordinator. The frequency-static nature in an interference-prone industrial environment was a blocking point for fast adoption of this technology in process automation. Therefore, the Zigbee 2007/PRO renditions also offer frequency agility, i.e. upon some criteria provided by the application, the network manager may direct the network to leave the current operating channel and move to another one. WirelessHART also allows the network administrator to restrict the channel hopping network-wide to selected channels in the RF band, denoted as blacklisting. 802.15.4 networks use two types of devices: Reduced-Function Devices (RFDs) and Full-

Function Devices (FFDs). FFDs contain the complete set of MAC services and typically operate as network coordiator or routers in a ZigBee network. They are typically line-powered, so placement is limited to locations with easy power access. RFDs or end devices contain a reduced set of the MAC services and can can only communicate with a FFD. Every ZigBee network must contain a network controller. The network controller, always a FFD, initializes the network, manages the process of joining and leaving of other network devices, and acts as Zigbee Trust Center, if security is enabled. Three topologies are supported by ZigBee: star, mesh and star-mesh hybrid (cluster-tree).

For easy network installation and expansion WirelessHART only specifies one single type of network device, so that each device in a self-organizing multi-hop mesh network can act as router for other nearby devices, passing messages along until they reach their destination. Also star and hybrid network types are possible. The complete network is organized by the network manager, who is responsible for e.g. initializing and maintaining network communication parameter values, scheduling, management of dedicated and shared network resouces, collection of system performance and diagnostic information, and provision of mechanisms for devices joining or leaving the network. The network manager maintains a complete list of all devices and has full knowledge of the network topology resulting in a collection of routing graphs, where each edge of the graph represents a possible transmission link between two devices. Each graph is denoted by a unique graph ID to identify the route through the mesh network. As the network is established multiple redundant communication paths are formed and continuously verified. To ensure path diversity each device should have at least two neighbours in each routing graph. In real plant settings, typically 30% of the devices communicate directly with the gateway and 50% are one hop away. The remaining 20% may be 3-4 hops [18]. Source routing is a second method for routing information between two devices. The source specifies a single route to the destination without providing any path diversity. Therfore, source routing is only used for testing and trouble shouting.

The ZigBee security architecture includes security mechanisms at two layers of the protocol stack, the Network (NWK) and the Application Support Sub-layer (APS). MAC layer security is provided by 802.15.4 using the 128-bit Advanced Encryption Standard (AES-128) supporting a variety of security suites, which can be classified into three categories: no security, encryption only with AES in Counter mode (AES-CTR), authentication only with AES in Chipher Block Chaining (AES-CBC-MAC), and encryption and authentication using Counter with CBC-MAC (AES-CCM). The network layer makes use of the CCM* mode of operation, a minor modification of the CCM mode used by the MAC layer with option to have encryption-only or authentication-only modes. Frame integrity can be secured by a Message Integrity Code (MIC) consisting of 0, 32, 64 or 128 bits. At a minimum, a ZigBee network should be secured with a Network Key shared between all nodes for protection of all network frames. Link keys are secret session keys for end-to-end encryption. Master keys are used as an initial shared secret between two devices to generate link keys. The central component of the ZigBee security architecture is the ZigBee Trust Center (ZTC). The ZTC, usually the network coordinator, is responsible for device authentication upon a joining request, maintenance and distribution of network keys, and configuration management.

WirelessHART specifies security services for the data-link and network layer. For authentication and encryption the CCM* is used in conjunction with the AES-128 block cipher to generate and compare a 32 bit MIC. Messages are verfied on an end-to-end and hop-to-hop basis. Key generation and management is done by the Security Manager and key distribution is serviced by the Network Manager. Four types of keys are employed: public keys to generate MICs by the joining devices, Network Keys to authenticate messages on a one-hop basis, unique Join Keys are used during the network joining process to authenticate the joining device, and Session Keys to authenticate end-to-end connections between two network devices. White lists prevent unauthorized devices from joining the network.

Well-engineered WirelessHART products are already available [17-23] and are continuously penetrating into the market. An example for many successful WirelessHART networks already installed in the field is Emerson's Smart Wireless solution to improve wellhead and heat exchanger monitoring on the StatoilHydro offshore platform (Fig. 1a) employing a self-organizing mesh field network. Statoil Hydro needed to remotely monitor wellhead and heat exchanger in harsh, difficult to reach areas. The wellhead is crowded with metal pipe work, metal walkways above and below, together with other metal obstructions (Fig. 1b). The Smart Wireless network on the platform includes 22 wireless pressure transmitters replacing traditional gauges. Ten pressure transmitters are mounted on a wellhead to measure annular pressure, twelve pressure transmitters monitor inlet pressure and pressure drop over the exchanger heater. Despite the metal-rich harsh environment the devices found the gateway and established the mesh as they were powered up. Total installation took less than 2 days.

Fig. 1a. Grane offshore platform, operated by StatoilHydro in the Norwegian Sea off the coast of Bergen, Norway.

Fig. 1b. Installation of a wireless pressure transmitter in the Grane platform.

3. FACTORY AUTOMATION

In [24] guidelines were derived for radio-based communication in industrial automation. Together with customer interviews and a market research carried out in the German public funded project EnAS [25], which is focused on the development of wireless energy autonomous sensor/actuator networks in production environments, the following conclusions can be drawn. The number of devices, i.e. sensors and actuators, being interconnected at the device level is usually high (up to 120 in a cell with a diameter of several meters). Typically short messages are exchanged, mainly in a cyclic manner. Furthermore, strict real-time boundaries have to be met, generally 10 ms between status change at the sensor node and actuator activation; reliability should be comparable with wired systems, i.e. packet error probability should be in the order of 10^{-9}. Additional requirements are: energy autonomous sensor operation, as the user only has full benefit of the wireless system if not only communication lines but also power lines are cut; coexistence with other wireless standards; scalability and modularity; usage of standard commercial off-the-shelf components and modules due to small market volumes of specialized automation applications; and the wireless system should also be applicable for the global market with no or only minor modifications.

Up to now these requirements for wireless device level communications can only be met by the WISA system [14] and feasibility of the system has already been proven with many installations in the field. An excellent description of the system is given in [25] so that only the main features of WISA, comprising the communication system, power supply, and sensor interface, are presented here.

Sensor/actuator communication is based on a standard Bluetooth radio transceiver with a channel spacing of 1 MHz and a symbol rate of 1 Mbit/s. The protocol stack has been modified to achieve a high transmission reliability, to meet the requirement of short cycle times and to support a large number of sensors and actuators. For wireless sensor/actuator control a network controller or base station with a high-performance full-duplex RF-frontend has been developed. A well-elaborated F/TDMA scheme is employed to guarantee infererence- and contention-free medium accesss. The parameters were chosen for a communication load of 120 sensor/actuator modules (SAMs) per base station. For frame and slot synchronisation by the sensors/actuators the downlink signal is always available. Uplink information from the sensors/actuators to the base station is organized in four parallel uplink channels. Total frame length for one communication cycle is 2 ms. Antenna diversity and switching is employed to meet the challenges of a time-variant, frequency-selective radio channel and the requirement for an extremely low packet error rate. To achieve low-power consumption sensor modules leave sleep mode only when a change in the sensor state occurs. SAM information can wirelessly be transmitted to the base station within 2 ms in a best-case scenario and in 15 ms in a worst-case scenario with strong interference. The hopping sequences are chosen so that several WISA cells can operate on the same factory floor without the need for inter-cell coordination.

The power supply unit is connected to primary wire loops generating a varying magnetic field with a frequency of 120 kHz. With two power-supply units, each connected with a pair of primary loops installed around a machine or part of a plant, a volume of up to 3x3x3 m^3 can be enclosed. Also ring-, line- and point type wireless energy supply concepts can be realized.

Today three different field devices for wireless automation are available: wireless proximity switches, wireless sensor pads, and wireless sensor/actuator pads. Wireless proximity switches and wireless sensor pads transmit their sensor information via modified Bluetooth-radio. With compact secondary wire-loops they source energy out of the magnetic field. Also wireless sensor/actuator pads employ a modified Bluetooth-radio for communication with the base station, but they are supplied conventionally with 24V DC. Advantages are obvious: short commissioning times, fast and cost-effective adaptions and retrofit, and highest flexibility.

In September 2005 a cable winding machine was equipped with 156 wireless sensors and 14 power loops (Fig. 2). The sensors are distributed in a metal-rich, strongly time-variant environment over a distance of approximately 50 m and are wirelessly connected to several base stations. The winding machine runs 24 hours a day and 7 days a week. A violation of the time limit for SAM sensor/actuator communication would result in an expensive machine shutdown. A second machine with 80 sensors is running since February 2007.

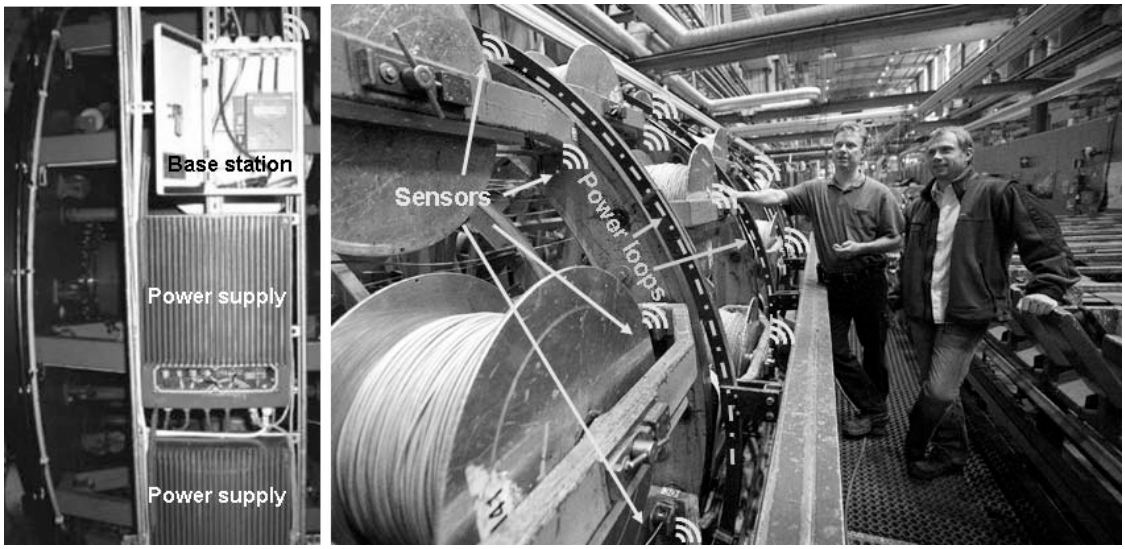

Fig. 2. ABB-WISA installation for wireless monitoring and control of a cable winding machine

The AS-Interface (AS-i) is a simple and cost-effective network solution connecting simple I/O devices to the upper fieldbus levels. A fully loaded AS-i Version I network with one master and 31 slaves has a maximum response time of 5 ms per I/O. With our wireless prototype system [26] we wanted to investigate if a performance similar to a wired AS-i could also be achieved. For the network controller we have chosen an approach based on a Xilinx Spartan 3 field programmable gate array (FPGA), as is shown in Fig. 3, offering both, a price-competitive solution and a high degree of freedom for implementing module functionalities either in soft- or hardware. To achieve multi-frequency operation, the network controller is realized with four low-power radio frequency transceiver units, denoten bei Rx/T#1 -Rx/T#4. Each RF transceiver is controlled by a finite state machine (FSM#1 - FSM#4) that can be subdivided into two sub-modules, RF-Ctrl and SPI-Ctrl, respectively. SPI-Ctrl serves for time-parallel configuration and data transfer to and from the RF transceiver units. SPI-Ctrl also automatically reads data from the Dual-Port RAM, if new information is available. RF-Ctrl checks RF transceiver status informations and generates all instructions for RF transceiver control, i.e. adjust to new frequency, transmit, receive or initialize. Substituting a RF radio module by a radio module operating with another RF modulation format or standard only requires to modify the RF-Ctrl finite state machine. Dual-Port RAM Ctrl coordinates RAM access by FSM1#1 - FSM#4 and their submodules. Different medium access algorithms and logical link control are realized in a software module running on the embedded MikroBlaze controller. Communication between network controller and distributed SAMs are visualized in Fig. 4, where the spectrogram of sensor/actuator communication embedded between three 802.11g-WLAN bands is shown. Measurements were taken with a Tektronix RSA 6100A real-time spectrum analyzer. A complete communication cycle, i.e. communication down from the network controller to the SAMs and back from the SAM to the network controller can be realized in 1.5 ms. Our measurements and simulation results have shown that packet error probability due to fading, shadowing and interference should be less than 10^{-3}. Therefore we expect that with 3 retries within 5 ms in the down- and uplink a packet error probability as low as 10^{-9} and thus a performance comparable with a wired AS-i can be achieved.

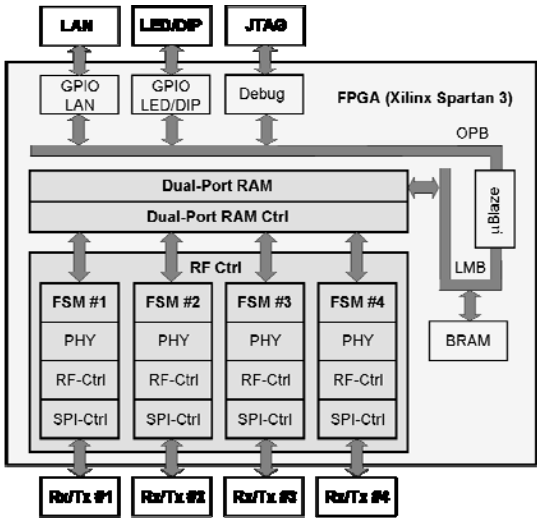

Fig. 3. Architecture of the network controller.

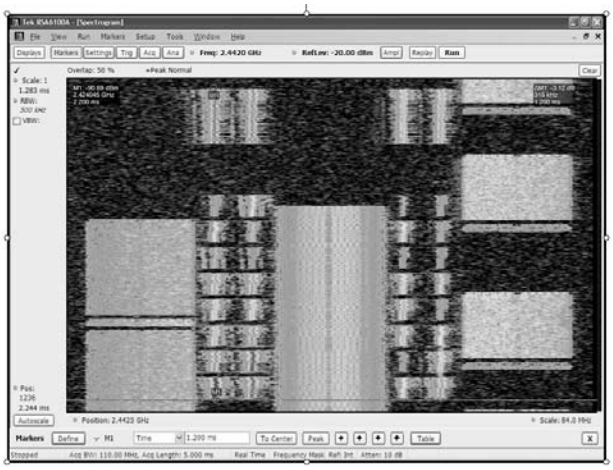

Fig. 4. Spectrogram of sensor/actuator-communication between three Wi-Fi bands.

ACKNOWLEDGEMENT

The author would like to thank Bernd Kärcher, FESTO AG, for a very fruitful cooperation in the EnAS project, and Guntram Scheible, ABB STOTZ-KONTAKT GmbH, and Ralf Küper, Emerson Process Management GmbH & Co. OHG, for their support in preparing this article.

REFERENCES

[1] Schildknecht AG, “Wireless Data Primer,” http://www.schildknecht.info.
[2] Nanotron Technologies, “nanoNET Chirp Based Wireless Networks,” White Paper, Version 1.04, Feb. 2007.
[3] Phoenix Contact, “Truted Wireless – in Detail,” Application Note 103146_C00_en, Jan. 2007.
[4] Siemens AG, “Industrial wireless communication: reliable, rugged, secure,” Scalance W Brochure, Oct. 2007.
[5] Vahle Electrification Systems, http://www.vahle.de.
[6] Sensicast, http://www.sensicast.com.
[7] Wago, http://www.wago.com.
[8] Phoenix Contact, http://www.phoenixcontact.de.
[9] connect Blue, http://www.connectblue.com.
[10] Stollmann Entwicklungs- und Vertriebs GmbH, “BlueCluster+,” http://www.stollmann.de.
[11] H. Zimmermann, “OSI reference model – The ISO model of architecture for Open Systems Interconnections,” IEEE Transactions on Communications, vol. 28, no. 4, April 1980, pp. 425 – 432.
[12] The Zigbee Alliance, http://www.zigbee.org
[13] HCF – Hart Communication Foundation, “HART 7 Specification,” Sept. 2007
[14] R. Steigmann, J. Endresen, “Introduction to WISA and WPS,” White Paper, ABB Stotz-Kontakt, Aug. 2004
[15] Governmental Funded Project, ”Energieautarke Aktoren und Sensoren (EnAS),” http://www.energieautark.com.
[16] J.A. Gutiérrez, E.H. Callaway, and R.L. Barrett, “Low-Rate Wireless Personal Area Networks, Enabling Wireless Sensors with IEEE 802.15.4,” IEEE Standards Information Network, 2004.
[17] Dust Networks, “Technical Overview of Time Synchronized Mesh Protocol,” http://www.dustnetworks.com.
[18] HART Communication Protocol, “Control with WirelessHART,” HCF_LIT-127, Revision 1.0, Jun. 2008.
[19] Emerson Process Management, http://www.emersonprocess.com
[20] A.N. Kim, F. Hekland, S. Petersen, P. Doyle, “When HART Goes Wirless: Understandig and Implementing the Wireless HART Standard,“ IEEE Int. Conf. On Emerging Techn. and Factory Autom.,” 09/2008, pp. 899 – 907.
[21] Endress+Hauser, “Wireless Adapter and Fieldgate,“ http://www.endress.com
[22] Pepperl+Fuchs GmbH, “A request becomes reality,” http://www.pepperl-fuchs.com.
[23] G. Lohmann, “Bereit für die breite Anwendung, Wireless HART als offener Standard für die Funkkommunikation in der Prozessautomation,” P&A Spezial Wireless-Kommunikation, May 2008.
[24] Guidelines of the VDI/VDE, GMA, Radio-based Communication in Ind. Automation, Beuth Verlag, Berlin, 2003.
[25] G. Scheible, D. Dzung, J. Endresen, and J.-E. Frey, “Unplugged but connected – Design and Implementation of a Truly Wireless Real-Time Sensor/Actuator Interface,“ IEEE Industrial Electronics Magazine, vol. 1, issue 2, 2007, pp. 25-34.
[26] R. Heynicke, D. Krüger, H. Wattar, and G. Scholl, “Modular wireless fieldbus gateway for fast and reliable sensor/actuator communication,” IEEE Int. Conf. On Emerging Technolgies and Factory Automation, Sept. 2008, pp. 1173 – 1176.