8th IEEE International Conference on Industrial Informatics

INDIN 2010

July 13-16, 2010

Osaka University Nakanoshima Center, Osaka, JAPAN

IEEE

ICS

EXPO'70

Osaka Convention & Tourism Bureau

Sessions Co-Chairs

Date	Duration	Session	Co-Chairs
July 14	09:15-10:30	TT1-1	Stefan Mahlknecht, Charlotte Roesener
		TT2-1	Tokuro Matsuo, Hirosato Seki
		TT8-1	Hiroshi Yajima
		TT4-1	Jose Barata, Hiroshi Morihisa
	10:45-12:00	TT1-2	Seung Ho Hong, Jan Haase
		TT2-2	Tokuro Matsuo, Chi Man Pun
		TT15-1	Hajime Mizuyama, Gia-Shie Liu
		TT12-1	Yoshiyuki Karuno, Takahiro Yakoh
		SS11-1	Benjamin Klöpper, Jörg Donoth
		TT9-1	Norihisa Komoda, Hiroshi Tsuji
		TT4-2	Mauro Onori, Hiroshi Morihisa
	14:50-16:30	SS1-1	Valeriy Vyatkin, Andrei Lobov
		TT2-3	Tokuro Matsuo, Jung-Hua Wang
		TT12-2	Tetsuya Ohtani, Takahiro Yakoh
		TT7-1	Masaharu Akatsu, Matsuki Yoshino
	-16:55	TT15-2	Hajime Mizuyama, Gia-Shie Liu
		SS11-2	Jörg Donoth, Benjamin Klöpper
		TT6-1	Paulo Leitao, Jose Machado
July 15	09:00-10:40	SS1-2	Kayoko Takatsuka, Valeriy Vyatkin
		TT9-2	Kazuhisa Seta
		TT3-1	Jose Martinez Lastra, Josep M. Fuertes
		TT14-1	Francois Jammes, Tsuyoshi Motegi
		SS9-1	Alois Zoitl, Friederich Kupzog
		TT10-1	Satoru Tezuka, Hiroshi Yoshiura
		TT8-2	Hiroshi Yajima, Takahiro Yakoh
	13:30-15:10	SS1-3	Yasutaka Fujimoto, Knut Åkesson
		TT9-3	Kazuhisa Seta
		TT3-2	Josep M. Fuertes, Jose Martinez Lastra
		SS7-1	Tatsushi Nishi, Nobutada Fujii
		SS9-2	Friederich Kupzog, Alois Zoitl
		TT10-2	Dimitrios Serpanos, Jiann-Der Lee
		SS5-1	Narayan C. Debnath, Baisakhi Chakraborty
	15:30-16:45	SS1-4	Valeriy Vyatkin, Cesare Fantuzzi
		TT9-4	Kazuhisa Seta, Takaaki Yamada
		TT14-2	Tsuyoshi Motegi, Francois Jammes
		SS7-2	Yoshitaka Tanimizu, Yoshiyuki Karuno
		SS8-1	Jong-Ok Kim, Kazuhiko Kinoshita
		SS2-1	Francisco Restivo, Claudia-Melania Chituc
		SS5-2	Narayan C. Debnath, Baisakhi Chakraborty

Date	Duration	Session	Co-Chairs
July 16	09:00-10:40	SS6-1	Po-Hsun Cheng, Sung-Huai Hsieh
		TT9-5	Keinosuke Matsumoto, Masanori Akiyoshi
		SS12-1	Nobutada Fujii, Takeshi Takenaka
		SS4-1	Hiroaki Nishi, Friederich Kupzog
		SS8-2	Kazuhiko Kinoshita, Yosuke Tanigawa
		TT13-1	Takahiro Hara, Jan Haase
		SS10-1	Hideki Tode, Won-Joo Hwang
	13:30-14:45	TT5-1	Elizabeth Chang, Tatsuya Nakae
		TT9-6	Keinosuke Matsumoto, Masaki Samejima
		SS12-2	Takeshi Takenaka, Nobutada Fujii
		SS4-2	Friederich Kupzog, Hiroaki Nishi
		SS8-3	Yosuke Tanigawa, Jong-Ok Kim
		TT11-1	Yoji Taniguchi, Tatsuya Nakae
		SS10-2	Won-Joo Hwang, Hideki Tode

A Smartcard based approach for a secure energy management node architecture

Stefan Mahlknecht
Markus Damm
Christoph Grimm
Vienna University of Technology
mahlknecht, damm, grimm@ict.tuwien.ac.at

Abstract- Future buildings and neighborhoods are expected to combine a manifold of Energy using Products ("EuP") ranging from electrical lighting to HVAC with locally available renewable energy sources and energy storages. Until now, advanced techniques for energy management are not yet applicable in an economically reasonable way in the smaller entities like in energy-positive buildings and neighborhoods. The EC FP7 project SmartCoDe is trying to enable a low cost application for demand side management and smart metering in private homes and small commercial buildings and neighborhoods. A new system architecture for secure wireless energy management nodes that specifically considers the requirements of Energy using Products in homes/offices is developed. The focus is the development of an inexpensive wireless System in Package (SiP) solution that allows to build up a fine grained infrastructure of wireless connected Energy using Products. The proposed architecture is a smartcard based solution which is scalable, highly secure, cheap and does not complicate node integration.[1]

I. INTRODUCTION

Today's energy grids are required to guarantee reliable operation of energy-positive buildings and neighborhoods. But stochastic energy sold back to the grid is of little (also financial) value because its availability cannot be guaranteed or predicted. This is a serious problem for both participation of energy-positive buildings in future energy markets, because the "predictable" energy achieves much higher prices, and for the power network operators which have to deal with rising peak demands. An intelligent management of energy in a local grid would enable customers to participate in the energy market and even contribute to the stability of the power grid. The problem is that such an energy management requires fine grained infrastructure and expensive hardware. Today, this limits applicability of energy management to large consumers in the industrial and commercial sector.

The goal is to allow all manufacturers of Energy using Products (EuP) to add energy management functionality (and maybe additional features such as remote control, etc.) for very little additional cost, and thereby address a new and huge market in homes and offices. The local energy management will enable local entities to participate in the energy market as an intelligent, managed "sub-grid" that can even contribute to a demand side management if necessary, and thereby reducing the required "spinning reserve". One approach of the project SmartCoDe is to timely schedule the use of energy or switch EuPs into standby if the customer process currently allows that.

To implement this functionality, a wireless sensor/actor node is developed (the "SmartCoDe node"). It will be a low cost System in Package (SiP) solution that can be integrated into arbitrary EuPs or into smart power outlet retrofitting older products. The SmartCoDe nodes will send the relevant data of the EuPs they are attached to to a central energy management unit, which in turn can control the EuPs via the SmartCoDe nodes, e.g. by switching it off or diming it down.

As the project is in an initial stage, the focus of this paper is to present state of the art and an initial solution comprising a novel system architecture for a low cost SmartCoDe node.

The remainder of this paper is organized as follows: After a review of the related work in Section II, we discuss the requirements regarding the energy management scenario described above in Section III. In Section IV, we outline the basic design decisions derived from the requirements. After discussing the SmartCoDe node architecture in Section V we conclude.

II. STATE OF THE ART

Bringing Energy Management further "down" to the consumer has been an industry and research topic since many years. Existing solutions however stop at at large customers mainly from industry. There were and are numerous attempts of scaling down the technological concepts so that home owners might also participate in this idea, but so far virtually all of them did not achieve a significant market penetration because of the usual barriers: System costs, necessary technological features and complex setup or maintenance.

The idea of a high volume, low cost chip for energy management is, for instance, addressed by the "DigitalStrom" initiative founded by ETH Zürich in Switzerland [1]. The focus of this initiative is, however, rather directed towards tackling the problems of achieving an inter-industry acceptance and generating a market for its energy

[1] The work presented in this paper has been carried out in the SmartCoDe project, co-funded by the European Commission within the 7th Framework Programme (ICT-2009-247473).

management chip; it is not about providing a technologically secure and scalable solution. While Digitalstrom is focusing on carrier-less power-line communication, SmartCoDe will focus on highly secure wireless communication as it is much more scalable and powerful compared to a narrowband power-line technology for single homes.

Demand side management (DSM) has been investigated in a number of research projects and test programs. One approach that follows a single-chip integration strategy for demand side management is part of the large U.S. "GridWiseTM" initiative, where research in the area of smart energy grids is conducted [2]. In the corresponding subproject the "GridFriendlyTM Appliance Controller" (GFA Controller) has been implemented as an FPGA solution [3]. This controller is supposed to be integrated in a large number of consumer products and performs grid frequency measurements. However, the approach is restricted to pure demand side management and does not provide additional features for communication and more intelligent power management.

Research at TU Vienna/ICT in the area of demand side management and smart power grids in several funded research projects has revealed that general technical and economical feasibility is given, but concrete concepts yet have to be developed [4]. TU Vienna/ICT has contributed to the field by providing a modeling approach for electrical load management [5] and by developing and implementing an economically and technically feasible concept of balance energy provision by electrical loads [6].

However, the big challenge in the above mentioned approaches for energy management is the need for cheap communication and data processing as well as data security and ease of installation in household and office buildings.

Home and building automation networks are on the market since more than one and a half decades. But due to the high price tag and the lack of flexibility of the technology, a large market penetration has never been achieved.

LonWorks [7] is a very powerful technology allowing much flexibility, and mostly used in professional building installations. The disadvantage of this technology is its complex installation and the requirement for training network integrators in order to be able to handle such networks with devices from many different vendors.

Konnex (formerly EIB) [8] is a European field bus mainly installed in high quality homes since more than a decade, but like LonWorks it has similar drawbacks and lacks the inherent support for energy management profiles.

An interesting alternative to wired field bus systems would be Power Line Communication (PLC). Simple solutions like X10 [9] remain popular in the home environment because of the inexpensive availability of components. However, the poor scalability and the lack of any security make them hard to be used in a commercial environment.

Other power line technologies that use sophisticated modulation techniques have been introduced in the last few years under the HomePlug power line alliance [10]. The technology is far too expensive to connect hundreds or thousands of low cost devices in a commercial building.

Considering cost optimization, Wireless Sensor Networks (WSN) are a promising approach, even though reliability and security are a significant challenge considering very low cost devices. One of the furthest developed standard is 802.15.4/ZigBee [11], followed by newer approaches such as WirelessHart [12] or ANT [13] or many other proprietary wireless systems. Although these wireless communication networks provide some robust networking, they can utmost be part of an easy to integrate and low cost overall system solution.

Beside the basic underlying communication technologies, functional profiles are one of the most important contributions to interoperability. Situated above the application layer, they define the syntax (coding, data types) and the meaning of variables and functions of a networked device. Building automation technologies are, compared to other domains, pretty sophisticated when it comes to interoperability and profiles. However, profiles for energy management are rare. Two notable exceptions are the ZigBee Smart Energy Profile and the BACnet Load Control Object. These two specifications are both recently published and manufacturers are invited to use them for their products. The two profiles however are very different. The BACnet Load Control Object consists of a 4-state finite state machine which can be used by an EuP to express its capabilities of managing loads. The big advantage of this profile is its simplicity and high abstraction level. It can potentially be used to represent individual devices as well as aggregates of them (house, neighborhood, etc.), but it lacks the capability of a finer granularity. It also lacks additional features like meter reading, payment and smart devices. The ZigBee Smart Energy Profile is an attempt to provide what is missing with BACnet. It is significantly more complex and specific when it comes to energy management applications like prepayment or programmable communicating thermostats (PCTs).

Both specifications, however, lack one important feature: an abstract but detailed representation of the "customer process". The customer process is the schedule or the physical mechanisms that stands behind the energy consumption patterns now and in future. These patterns are influenced by customer behavior, time, environmental parameters, device programs and schedules and the nature of the process itself (time constants, etc.). All existing solutions which share this important information with an optimizing algorithm are either not abstract (i.e. easy) enough or not detailed enough.

III. REQUIREMENTS

To enable the application of advanced energy management techniques in energy-positive buildings and neighborhoods, infrastructure and methods are needed that specifically fulfill the following requirements:

- *Low additional costs.* Most households are not willing to spend money for energy management features of their heating, ventilation and air condition (HVAC), electric lighting or white goods. According to our internal market studies, an acceptable price for an embedded system that provides energy management capabilities is in the range of 3$ to 10$ (see [14] for actual numbers). This is also a price that is economically reasonable considering costs and benefits. However, existing hardware for demand response management is by far more expensive.
- *No New Wires.* The low additional cost requirement implies that no new wires can be installed. In most households and offices there are no automation networks like LonWorks or BACNet [15] available which connect each individual consumer and can be reused for energy management. Therefore, only wireless communication or power line communication would be applicable. Due to the advances in wireless communication and the still many challenges in power line communication (see section II), the project focuses entirely on a wireless solution.
- *Small size.* To allow for the integration of energy management solutions in almost all kinds of household appliances, the integrated solution must be small in size. Size however is also the key to cost: the higher the integration (i.e. a very small chip with no additional discrete components in the best case) the lower the manufacturing costs. To allow integration into as many appliances as possible, advanced energy management must have a very small footprint (e.g. 1cm*2cm*2cm).
- *Information Security.* The ability to remotely take influence on EuPs requires high information security. Integrity and authenticity of all data and commands are the most important requirements, followed by confidentiality and sophisticated access control. The system must offer robustness against malicious attacks and intrusion.

IV. SMARTCODE NODE DESIGN APPROACH

In order to fulfill the requirements of low cost, small size, flexible communication infrastructure, and high security, the following approach has been taken:

- Integration of all SmartCoDe node hardware into an integrated circuit, i.e. a "System in Package" (SiP). Integration allows reaching even ambitions goals considering the costs, assuming high volume market such as the electric lighting market (several Mio. p.a.). External components will be unavoidable as 220/110V inputs (i.e. for a power supply) and outputs must be managed, however the goal must be an architecture with material costs of less than 1 U$.
- Communication between all energy generators, storages and energy consumers ("SmartCoDe nodes") and a central energy management unit via RF interfaces over single- or multi-hop 868/915MHz or 2.4GHz ISM Band communication interfaces. This allows for dependable networks using multiple routes.
- Integration of highest-grade security features from existing "SmartCard" designs (a.k.a. crypto-cards) to guarantee information authenticity and privacy, either embedded or in form of a separate replaceable smart card.
- Optional passive RFID or NFC [16] interfaces for node installation addressing and node replacement. Alternatively, a plug-in smart card (i.e. in the form of a micro SD Card) can be used to deploy entire networks in a plug and play manner. This would also simplify network commissioning and trust establishment apart from adding security.

Not every SmartCoDe Node will be equipped with the same hardware functionality, so variants will be proposed that address different device classes to optimize for cost and functionality. The benefit of the approach is that it tackles security issues and installation issues as a central point in the overall system architecture, while still focusing on the highest level of integration including high voltage subsystems typically not found in SiP based solutions.

V. PROPOSED NODE SYSTEM ARCHITECTURE

A single SmartCoDe Node consists of a high voltage and a low voltage subsystem, where the low voltage system may be further subdivided into the smart card chip die and the SmartCoDe core chip integrating all communication interfaces as well as basic firmware (System ROM) common to all SmartCoDe nodes.

There are three basic variants proposed in order to optimize for cost within the given class of application. The full featured variant can be used together with any type of EuP. For more cost sensitive devices or smart devices which provide already basic functionality like energy consumption information or a low voltage supply, certain functional blocks can be omitted. For instance, smart consumer devices which are SmartCoDe enabled in the future can share certain functional blocks of the SmartCoDe node architecture which are already built into the device. Examples are the already available power supply and a possible control interface where information on power consumption or state of the device can be exchanged with the SmartCode node. In this way no separate voltage and current measurement circuit is needed

lowering the additional cost of the devices energy management functionality.

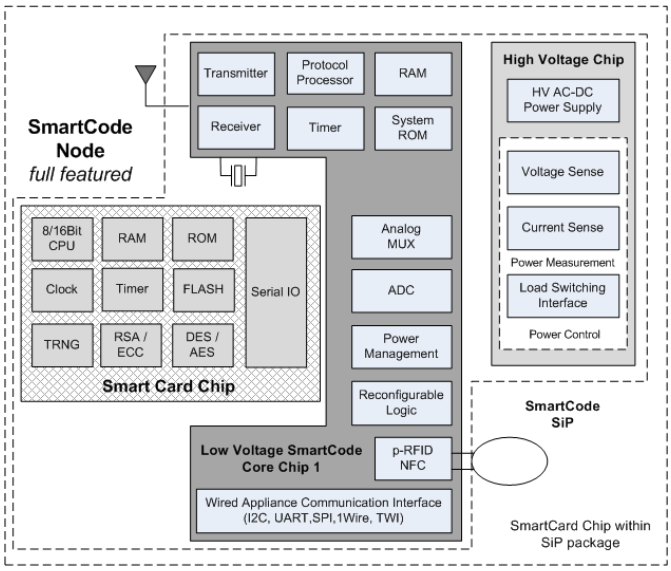

Fig. 1. Fully extended System Architecture of a SmartCode Node, with plug-in Smartcard and Wireless ultra short range passive configuration and maintenance interface.

On the other hand, low cost devices such as lamps or generic power plugs where anything can be connected to, need a high voltage power measurement and supply unit. For cost reasons, we propose a variant shown in Figure 2 without a smart card where specific smart card functionality is integrated directly in the SmartCoDe core Chip. Within the course of the project we are going to analyze whether this second variant saves significant cost as it still requires a wired level secure interface (solved with a NFC or RFID interface) to establish a trusted relationship between device and network. This is typically done by an operator or the user when installing a device within a network.

There is another way of establishing a trusted relationship in the third variant of the proposed architecture (Fig. 3.). A smart card is delivered separately to the device, similar to cell phones, where the phone is delivered separately from the SIM card. When the user establishes a trusted relationship between the phone and the network, it plugs in the SIM card and the device can join the network. In the same or similar way it can work for any EuP as well. As it might not be feasible for every EuP to provide a connector for a smart card (which could be in the physical form of a micro SD-Card), the variant in Fig. 1 does not provide a plug-in smart card, but have the smart card integrated within the SiP. In Fig. 2 a separate smartcard is omitted and basic security is provided within an upgraded version of the core chip. For both variants an NFC Interface allows to configure at close proximity any network configuration and security settings. The SmartCoDe node comes without any network parameters and private network keys stored when delivered. For the establishment of at trusted relationship the extremely short range wireless NFC interface is used to exchange the relevant network information automatically with a programming device or even with a standard NFC enabled cell phone and a respective application program.

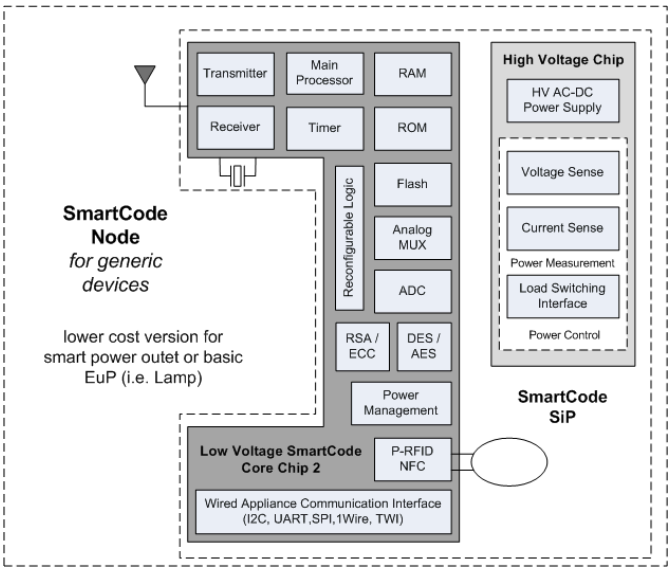

Fig.2: Smart Card less system architecture with encryption hardware within the SmartCoDe Core Chip eliminating a third die in the SiP package.

NFC [16] is a novel standard for short range (up to 10-20 cm) peer to peer communication in the 13MHz ISM Band and already integrated in many cell phones, allowing for simplified e-payment and other applications in the near future. Not all devices might allow for such an interface as the antennas are large, but at least very cheap as less than 10 cent priced passive RF-ID tags prove.

Our proposal of three basic variants of the given node architecture would give enough flexibility to accommodate most application use cases. Another very interesting use case of NFC in private homes is that any user with a trusted NFC enabled phone could approach any SmartCoDe enabled device and query its energy usage or statistics or even control the device. This could be very interesting for consumer electronics or white goods where connection is established only at close proximity giving intruders from outside little chance to access a device.

The integration of smart card level security (typically used for banking cards or digital passports) already at the design stage as an inherent system component allows for using processor and memory resources of the smart card chip for the protocol and application profiles as well as node addressing and storage of keys in a highly secure environment.

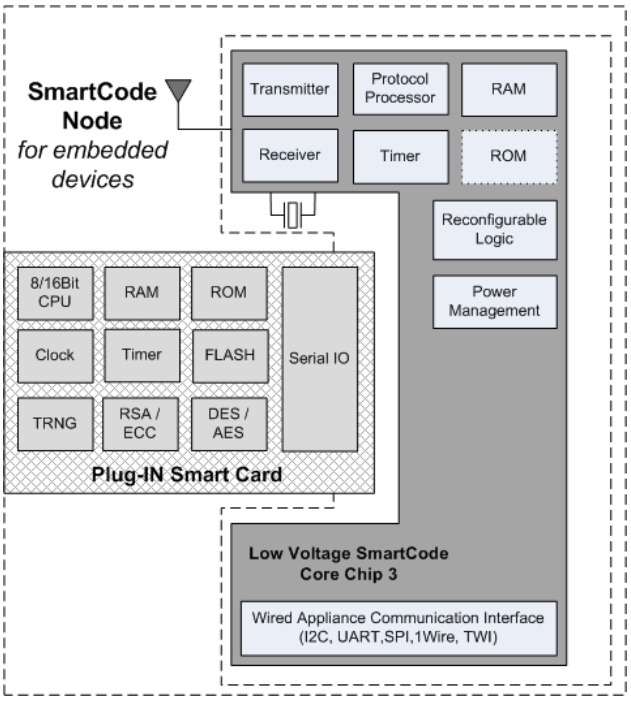

Fig.3: Plug-in Smart Card version for smart devices to be integrated directly into smart EuP which provide a basic communication interface for exchanging power states power consumption and controlling the device.

The specific SmartCoDe architecture for embedded devices (Fig. 3) has the advantage that the additional cost for the device manufacturer is minimal as only the SmartCoDe Core chip has to be integrated on the motherboard as well as a low cost Smart Card connector and antenna to prepare the EuP for a SmartCoDe enabled network. Only if the user wants the additional SmartCoDe functionality a Smart Card for the given device class is purchased and plugged into the device which then automatically joins the network.

VI. CONCLUSION

This paper presented system requirements and an architecture for a novel highly integrated SiP solution of a modular, low cost and highly secure energy management node. It has the capability to not only run energy management applications, but also feature rich automation applications for homes and neighborhoods. It also solves the problem of trust establishment between the device and the device owner or network maintainer. Network and node configurations can be automatically generated during installation time and plugged-in or transferred to the device via NFC at time of installation.

In this paper the details of the architecture for the different variants are omitted as the project started recently and some design decisions still are to be verified. One of these decisions is the use of a respective wireless solution for the radio communication between nodes and the network topology as well as network configuration and maintenance. We are investigating in using 802.15.4 / ZigBee compliant standards as well as other more downsized solutions which may lead to an alternative standard used in future energy management solutions.

The drawback of the added cost for the security functionality (Smartcard) is offset by the possibility to scale the SiP solution for the different devices needs as well as by the fact that CPU and memories of the Smartcard (ROM, RAM, and EEPROM) will be used for communication protocols and application profiles. The added value of a secure node will enable a much larger market acceptance as security is a major concern especially in wireless applications and professional energy management in buildings.

REFERENCES

[1] Official Homepage of the DigitalStrom Alliance www.digitalstrom.org
[2] Official Homepage of the ZigBee Alliance: www.gridwise.org
[3] Hammerstrom, D. J. et al. (2007). Pacific Northwest GridWiseTM Testbed Demonstration Projcts, Part II, GridFriendlyTM Appliance Project, Pacific Northwest National Labora-tory, Project Report
[4] Palensky, P. et al. (2006). Integral Resource Optimization Network – Study, Project report En-ergiesysteme der Zukunft, Project No. 808570, BmVIT
[5] Kupzog F., Roesener C. (2007). A closer look on load management, 5th International IEEE Conference on Industrial Informatics (INDIN 2007), Vienna, Austria
[6] Kupzog, F. et al. (2008). Integral Resource Optimization Network – Concept, Project report Energiesysteme der Zukunft, Project No. 810676, BmVIT
[7] D. Dietrich, D .Loy, H.J. Schweinzer; "Open Control Networks LonWorks/EIA 709 Technology"; Kluwer Academic Publishers, 2001
[8] D. Dietrich, W. Kastner, T. Sauter; "EIB Gebäudebussystem", Hüthig Buch Verlag GmbH, Heidelberg, 2000
[9] More information on X10: http://en.wikipedia.org/wiki/X10_%28industry_standard%29
[10] The official Homepage of the Homeplug Alliance: www.homeplug.org
[11] The official Homepage of the ZigBee Alliance: www.zigbee.org
[12] More information on WirelessHart: http://www.hartcomm.org/
[13] More information on ANT: http://www.thisisant.com/
[14] Friedrich Kupzog: "Energiesysteme der Zukunft". Final report of Project 810676/7837: „Integral Resource Optimization Network Concept". TU Vienna, Institut für Computertechnik, March 2008.
[15] ANSI/ASHRAE Standard 135-1995: BACnet—A, Data Communication Protocol for Building Automation and Control Networks
[16] Madlmayr G., Ecker J., Langer J. & Scharinger J.: *Near Field Communication: State of Standardization*, Proceedings of the International Conference on the Internet of Things 2008, Zürich 2008; ETH Zürich