Linking Control Networks and Wireless Personal Area Networks

Stefan Mahlknecht, Peter Palensky
Inst. of Computer Technology
Vienna University of Technology
Gusshausstr. 27/E384, A-1040 Wien
AUSTRIA

Abstract – **Automation networks tend to become smarter and more consumer-oriented. New technologies, initially not intended for automation purposes, offer new possibilities and increased functionality for control and monitoring applications. This paper gives an overview of how intercommunication between to entirely different networks such as fieldbus systems, used for automation networks and wireless personal area networks (WPANs), embedded in modern consumer electronic devices for small and wireless ad-hoc networks can lead to new services. The major challenge is the integration of WPANs into existing and proven automation applications. This introductory paper emphasizes on inter-communication, services at the application layer level and on how to leverage from the different features of these networks to extend the functionality and allow new services. The approach presented here is universal and can be applied to any automation system. In section V we present some results of the implementation of selected services.**

I. INTRODUCTION

Many modern consumer electronic devices like mobile phones, personal digital assistants (PDAs), laptop computers and printers are or will be equipped with a WPAN [1] network interface. A combination of the WPAN concept and existing fieldbus-based automation networks [2] would allow new types of services. Previously separated WPANs can be connected as well as WPAN devices and fieldbus nodes can participate in a common application. Within the InFiPAN[1] project the potential benefits of such an intercommunication are investigated. This paper will give an overview of the possibilities of this intercommunication and starts with an explanation of what WPANs and fieldbus systems are.

WPANs are wireless ad-hoc networks with a limited range of typically some tens of meters (10-100m). The commercial focus lies on consumer electronic devices and cable replacement. The media is radio transmission, although it could also be based on an infrared channel. The most important WPAN is Bluetooth [3], standardized under IEEE802.15. It has a raw bit rate of 1 Mbps and a data rate of max. 721 kbps.

State of the art fieldbus systems (a.k.a field area networks) [4][5] are typically based on a wired communication channel. They are low latency and medium to low bandwidth networks that are deployed in industry but also in modern buildings where they reach almost every corner of the same. The majority of fieldbus systems use twisted pair channels.

[1] Intercommunication between Fieldbus and Wireless Personal Area Networks, a project at the Institute of Computer Technology www.ict.tuwien.ac.at/infipan

Combining the capabilities of WPANs and fieldbus systems leads to a broad range of new services and can increase the flexibility of fieldbus systems. Taking an example from the area of home and building automation, wireless enhanced mobile electronic devices such as PDAs, cellular phones or notebook computers could have access to the control network or even use its infrastructure for intercommunicating with other WPAN peers. It would be possible to locate a person within the building through the persons WPAN enhanced cellular phone and to regulate the climate and lighting automatically according to a personalized level of comfort.

The following sections present different flavors of interconnecting WPANs to fieldbus systems. Based upon the typical services and types of nodes present in such a heterogeneous network, an appropriate access point architecture that allows wireless and wired control nodes and consumer devices to intercommunicate, will be proposed.

II. PROBLEM ANALYSIS AND RELATED WORK

Connecting two different types of networks can happen in a variety of ways. The interface between the two networks can happen on almost every layer of the ISO/OSI reference model [6], which results in repeaters, routers, bridges or gateways. Depending on the similarity of the two protocol stacks one might get along with a bridge or the like. At the fieldbus level a number of ways to integrate wireless nodes have been proposed [7][8][9]. These proposals show the connection of wireless sensors to wired fieldbus systems, but they do not show the different types of mappings from and to consumer electronic devices.

In our case, the protocol stacks are different as can be. The communication media are wireless and wired, the protocol stacks have different syntaxes and the individual services are either very specialized or simply not existent on the other network.

Fieldbus systems, historically coming from industrial automation, usually have a fully defined protocol stack from layer 1 to layer 7. Above that, application layer services and applications are standardized and defined. WPANs typically only define the lower layers of the ISO/OSI model and stay open for the upper layers. Another problem is the different qualities of services (QoS). A fieldbus might have a transmission service that is based on priorities or real-time restrictions for alarm messages, while this can not be found on a classical WPAN. Our main focus lays on common applications. Both technologies should participate in and contribute to one high level application service. Decotignie

presents in [9] different types of interconnection between wireless and wireline fieldbus systems but does not discuss the necessary application services.

Lilakiatsakun and Senevirante [10] discuss the connection of different WPANs via a scatternet architecture in the context of home networks. This represents a totally wireless solution which has many drawbacks regarding network topology construction, routing issues, range restrictions and delay through multiple hops. Our approach also aims to interconnect different WPANs, but we think that in many applications a wired infrastructure such as a fieldbus or a LAN will be better suitable for such purposes. Also Saito [11] discusses connections between wireless and wireline networks, but only focuses on a multimedia environment in the home, while we focus on generic automation applications. Coming from the top level or application level view of such a common automation system we can find two main aspects, namely

- WPAN devices should participate in the fieldbus application and vice versa, and
- separate WPANs should be interconnected via the fieldbus and separate fieldbus segments via WPAN.

Having a look at the usage scenarios and typical services in industry tells how such a heterogeneous network system looks like (Fig. 1). The main services for which wireless consumer electronic devices will be deployed in factories are data logging and supervisory functions. Wireless sensors and actuators will most probably first be installed for non safety critical applications where real-time is not of a big issue.

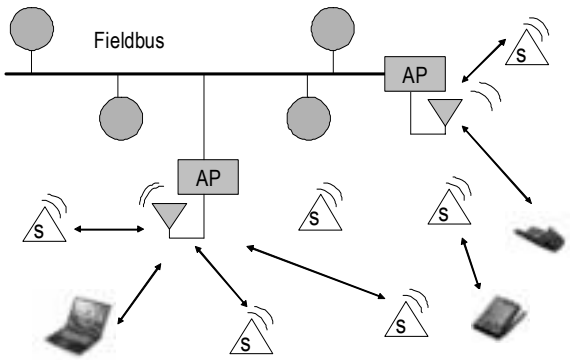

Fig. 1: Heterogeneous network architecture

Fig. 1 differentiates between different types of devices. On one hand there are sensors and actuators that may be mobile and communicate through a mix of wireline and wireless communication. On the other hand we have wireless consumer electronic devices that may take part to a WPAN and at the same time offering and using services to and from the fieldbus (e.g. access control, location information, environment control, data monitoring, and extension of the WPAN to reach other distant WPANs)

The central point in this architecture are a set of Access Points (AP) that have the task to map the different services offered by WPAN nodes and the fieldbus itself in both directions. Existing proposals of access points [??] do not define an appropriate way of mapping services of consumer electronic devices onto automation networks. It has to be made clear that many services on one side of an access point are not available on the other side and that a generic and transparent gateway application will not be a feasible solution. Later sections describe this issue in more detail.

III. SYSTEM ARCHITECTURES

Taking the above considerations into account, four different types of communication between fieldbus systems and WPANs are identified:

a.) WPAN to Fieldbus

WPAN devices and their services and capabilities are "exported" to the fieldbus in order to be used by the members of the same. This type of communication is described in [11] where an approach is shown how to connect Bluetooth enabled sensors in a power efficient and plug & play fashion to an existing fieldbus. Of course one could implement this type of communication through repeaters, bridges or routers by taking the wireless link just as a transport layer and implementing the upper fieldbus layers on the wireless nodes, but these solutions have many drawbacks as shown by Mahlknecht [12] and Dunbar [13].

WPAN to Fieldbus communication is best achieved through a network of "access points" that are connected to the fieldbus system as depicted in Fig. 2.

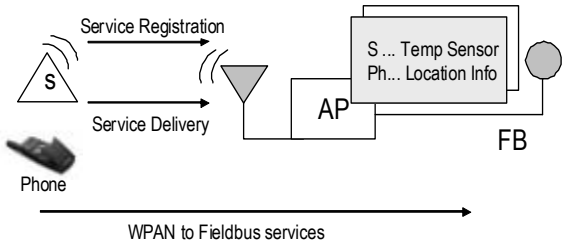

Fig. 2: WPANs deliver services

These access points represent the wireless devices and nodes to the fieldbus network. Depending on the fieldbus this might happen as additional entries in a global and distributed data structure (process image) or as one or more "virtual" fieldbus nodes. Fig. 2 shows one simple data structure on the fieldbus side that represents two wireless nodes and their services.

Since WPANs are normally relatively small (<10nodes) a point to multipoint connection with a master slave architecture with one access point per WPAN is the most appropriate solution.

Access points may consist of an embedded system with fairly high computational power and memory resources and no power constraints. In contrast to access points, wireless sensors are often battery powered and have few resources, therefore only the sensor data and essential management messages should be transferred over the wireless link. This can be done by the OBEX (Object Exchange) Protocol that is

specified in Bluetooth and defines how generic objects are exchanged between devices.

b.) Fieldbus to WPAN

Similar to a.) an application layer gateway can be used to offer fieldbus nodes and their services to wireless devices. The services of the fieldbus system are offered to the WPAN in a WPAN-like style (Fig. 3.). Again, the massively different technologies and domains of applications are the main challenge.

Automation network nodes might contain complex application layer services like a data logger or a room controller, all of them well defined in object-oriented profiles and standards like given in Haakenstad [14], LonMark [15] and Profibus [16]. Virtually every "sophisticated" fieldbus has such "functional profiles" that give the rules on how to get the desired service (like reading out a temperature log) and how to interpret the retrieved information.

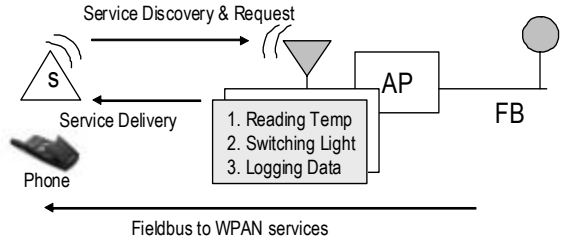

Fig. 1: WPANs request services

A wireless PDA does not know anything about fieldbus profiles. Even if the PDA is somehow capable to browse the data structures of the fieldbus nodes (by understanding the syntax), it would not comprehend the semantics. This can easily be shown by looking at the protocol stacks. A LonWorks node for instance uses data types (engineering values like degrees Celsius) and data structures (like the standard profile of the temperature node) far above layer 7 while a WPAN device probably ends at layer 3. So there seems to be no easy way to translate the contents of the fieldbus service F1 into a WPAN service W1 because W1 simply does not exist or the respective protocol stack has a deep gap. The missing bridge for this semantical gap is an abstract representation of fieldbus services, preferably based on some existing standard. Classical network management frameworks and "middleware" offer a way to implement data structures in an object-oriented way like it was done for functional profiles, but they appear to be either too inflexible (SNMP, simple network management protocol) or too heavy weighted (CORBA, common object request broker architecture). Recent players like SOAP [17], HAVI [18] and OSGI [19] look more promising. They were especially designed for operating distant services, for representing electronic devices and for implementing gateways to control nodes. The WPAN devices, however, still lack the ability to use these new technologies.

Instead of developing a powerful SOAP client application together with forcing all access points to "talk" SOAP to the WPAN, the wireless consumer goods offer an alternative way. An increasing number of devices come with flexible platforms like Java-enabled web-browsers. So if the access points simply use java applets and web-pages to represent the fieldbus services, the wireless client is not bothered with new technologies - everything is encapsulated within the web content. This second alternative is less interoperable and less elegant than the first one because the access points can (and will) use proprietary methods to transport data and to visualize services, as long as the (human) user of the wireless device can somehow "read" and operate it. A machine-parseable service representation would be better.

Therefore the pragmatic way is preferred: representing the fieldbus as an XML/SOAP content that can eventually be operated by a future standard browser or a special application.

c.) WPAN to WPAN

Connecting different WPANs via a Fieldbus is a very interesting option. As depicted in Fig.4, the goal is to physically extend the WPAN network to form a virtual WPAN that spans a much wider area. Actually coverage is restricted to the radio range of a single access point and the respective radio range of the mobile device. To mention an example, a Bluetooth enabled laptop in a conference room could print something on a printer that is on the other end of the floor and thus not reachable by Bluetooth over a point-to-point link.

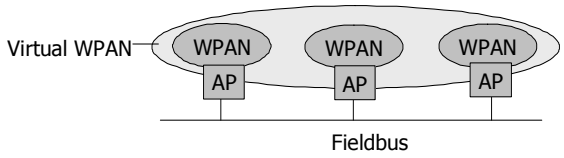

Fig. 2: Virtual extended WPAN

To allow local WPAN devices to communicate transparently with its remote peers, a tunnelling protocol must be implemented at the access points. It has to be investigated for each fieldbus whether enough bandwidth, upper delay bounds and jitter can be guaranteed for the different WPAN services. Alternatively an existing local area network (LAN) could be used as a backbone and transport medium for the virtual WPAN.

d.) Fieldbus to Fieldbus

Connecting two interoperable fieldbus segments via a wireless personal area network is the more exotic aspect of how Fieldbus systems and WPANs can be connected. Generally, for most applications it does not make much sense, because a simple wire would do the same job. Only special cases like galvanic separation or redundant network segments could lead to such architecture. Therefore this type of intercommunication is not covered here.

V. ACCESS POINT ARCHITECTURE

Based on the above definitions the access points are responsible for three tasks:

a.) representing the WPAN as virtual fieldbus objects

b.) representing the fieldbus as WPAN-accessible data

c.) tunnelling data from WPAN to WPAN

The first two points are done via application layer gateways. Both gateways (fieldbus to WPAN and WPAN to fieldbus) face the same needs:

- service and node discovery/lookup: This can be done via protocols like UPnP/SSDP (universal plug-and-play/simple service discovery protocol) [20] or JINI [21]. See Moyers et al. [22] for further examples like SLP (service location protocol). Bluetooth for instance uses its own service discovery protocol (SDP). Some fieldbus systems allow such a discovery, others do not. In that case the network management tool of the fieldbus system must register the fieldbus services in the access point by providing a config-file or something similar.

- data abstraction: a measurement value is not only a float number but rather an engineering value with a physical unit, accuracy, time stamp, etc. Also the encoding and addressing method must be translated.

- service abstraction: Classical SCADA (supervisory control and data acquisition) services like on-line data, data logging and alarm messages are to be translated for the WPAN system, and the location information of a mobile phone must be converted into fieldbus-like data structures.

When different applications need to interoperate, profiles play an important role. Profiles of fieldbus nodes need to be mapped to profiles of the wireless nodes and vice versa, as far as they are existent. The task of the access points is to register nodes plus their services and to map them onto profiles of the other side. Beside these two gateways the access point also contains the tunneling infrastructure of point c.), as depicted in Fig. 5. The image also shows the discovery protocols FSDP (fieldbus service discovery protocol) and WSDP (WPAN service discovery protocol) as being parts of the protocol stacks. This is not necessarily the case as for some fieldbus systems these protocols would be based upon the stack. Plug-and-participate on the lower protocol levels and automatic service discovery, identification and registration are a must-have. There will be no way for access points that need intensive system administration.

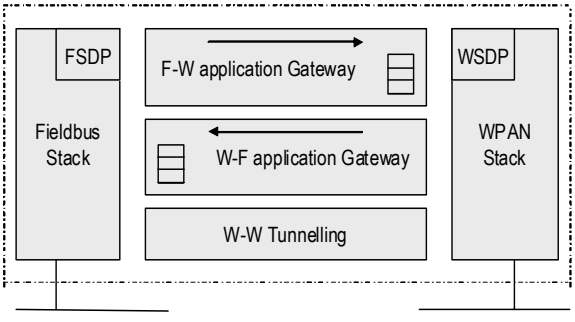

Fig. 3: Access point architecture

One problem of the gateway approach is its non-transparency. New services demand new profiles and new data structures, so the gateway is usually application-specific. One way out of this organizational problem is to define a generic standard profile for a specific automation domain. This profile or representation needs to be as generic as possible to cover all services that might appear. It also needs to be as specific as possible in order to release the clients of this profile from interpreting and parsing data that is too abstract.

An important aspect of the access point concept is localized services. Imagine a person that wants to control a device at its current location by using a mobile phone. The access point needs to be aware of the location of the WPAN device and the location of the fieldbus devices. In this way only the relevant services for the operator could be shown. The operator won't be interested in getting a list of all the services offered by the entire automation system.

Connecting two different types of networks can happen in a variety of ways. The interface between the two networks can happen on almost every layer of the ISO/OSI reference model [6], which results in repeaters, routers, bridges or gateways. Depending on the similarity of the two protocol stacks one might get along with a bridge or the like. In our case, the protocol stacks are different as can be. The communication media are wireless and wired, the protocol stacks have different syntaxes and the individual services are either very specialized or simply not existent on the other network.

V. IMPLEMENTATION OF SELECTED SERVICES

The "wireless group" at the Institute of Computer Technology in Vienna is currently evaluating and implementing the ideas of this article. At time of writing two services that interconnect wireless and wired control networks have been implemented:

- A wireless access control system that works with any Bluetooth enabled phone or other mobile device.

- Generic remote control service for automation applications designed for Bluetooth enabled phones.

Both projects were realized with the same type of hardware platform, shown in 6.

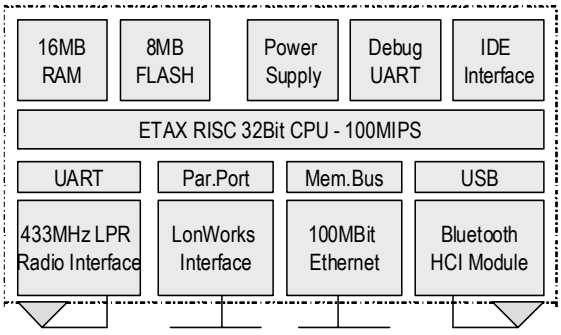

Fig. 4: Hardware block diagram of the generic Access Point

On this platform also many other functions and services outlined in this paper could be implemented. Fig. 6 shows a hardware block diagram of the access point.

This versatile platform is based on the so-called "Etrax" chip from Axis Communications [23], a highly integrated SOC hosting a standard Linux operating system. It offers two wired and two wireless communication interfaces. For the wireless part, Bluetooth is the typical WPAN representative while the low power radio interface is more suitable for battery operated sensors. Bluetooth is no option for the types of sensors that we intend to use, due to the excessive power consumption and the costs. Concerning the wired interfaces, an Ethernet MAC was already available on the Etrax chip and will be used for high speed backbone connections and connections to possible office networks or the Internet. Already nowadays, fieldbus systems are very often deployed in local clusters that are interconnected via an IP-based backbone which tunnels the fieldbus packets [24]. Therefore having both interfaces, namely LonWorks and Ethernet on the gateway can provide much greater flexibility at very little additional costs. Management and administration of the access point node can be done over any of the wired or wireless interfaces.

Our first implemented service - the wireless access control system - is a WPAN to fieldbus service delivery as explained in section III.a. The access control system consists of the here presented access point and works with any commercially available Bluetooth enabled cellular phone. The results obtained in the wireless access control project can be summarized as follow:

- True ad-hoc networking proved to be feasible providing access control information to a fieldbus actuator.
- Multiple access request by different users at the same time can are supported by the access point.
- Constrained resources at the Bluetooth link did not allow to run other services while the access control system was active. Only this single Bluetooth to Fieldbus service can run at a time. A solution to this problem would be to have more than one Bluetooth interface at an access point.
- For the cellular phones, no additional software was needed. The access control system relied solely on the features of the Bluetooth stack and its services like device discovery, service request and authentication information.

The generic remote control service belongs to the fieldbus to WPAN service explained in section III.b. The results obtained in the remote control project are:

- A client application was required on the cell phone for the user interface and the Bluetooth connection. Although we could have used an already available WAP or XML browser with the user interface designed as a content, the mobile phones were not able to use the Bluetooth link as IP network connectivity instead of the GSM link.
- Java is still not an option for many client applications since at time of writing there is no Java API available on cellular phones that allows to control the Bluetooth interface. For our implementation the Nokia 7650 was used because it was the only available cell phone with the capability of programming Bluetooth in a C/C++ language. We expect that it will be only a matter of time until extended Java APIs are available that enable the usage of all the features of mobile devices.

VI. OUTLOOK AND FUTURE RESEARCH

This paper discussed the principles and architectural structures of intercommunication between WPANs and fieldbus systems. This combination will very likely achieve significant relevance in future.

Recently a simple and yet useful family of products appeared on the market. EnOcean [25] delivers wireless communication technology that work without a battery - the desired energy is produced at the sensor (i.e. by pressing a button). This does not necessarily fall into the problem of intercommunication between different types of networks, but it is a further technology that makes wireless devices more attractive for any automation application.

The general driving factor for combining WPANs and fieldbuses, however, is the growing number of WPAN enabled consumer electronic goods. These devices will determine how the intercommunication will take place. Currently IP-technology and JAVA seem to be basis for it.

Still open is the topic of data and service representation. There are first ideas to exploit XML for this topic like given by Wollschlaeger [26] and Birkhofer [27], which will be subject of further research.

Another important aspect is system security. Fieldbus systems naturally have low or no security at all, while modern WPANs (such as Bluetooth) do. On the other hand, a wireless transport media is more vulnerable to attacks than wired ones [28]. See Palensky and Sauter in [29] for a discussion on security for fieldbus gateways with the premise of an open and unsafe transport. The most challenging aspect of security for WPAN/fieldbus systems is to stay compliant with the security mechanisms that the WPAN already might have. Combining two different security concepts seems to be almost impossible, so probably applying the WPAN concept to the fieldbus network might be the easier way and will be subject of further research and papers.

Based on the realized gateway we intend to realize many of the here discussed services in further research projects and exploit the different options for implementing them.

VII. REFERENCES

[1] IEEE 2002. Standards of the IEEE 802.15 Working Group, www.ieee802.org/15

[2] Schickhuber, G. and O. McCarthy, "Distributed fieldbus and control network systems", *Computing & Control Engineering Journal* 97, pp.21 –32, Feb. 1997.

[3] J. Bray and C.F. Sturman, *Bluetooth1.1 Connect Without Cables*, Prentice Hall, 2nd Ed., pp. 622; 2002

[4] D. Dietrich, D. Loy and H.J. Schweinzer, *Open Control Networks LonWorks/EIA 709 Technology*, Kluwer Academic Publishers; 2001.

[5] T. Sauter, D. Dietrich and W. Kastner, *EIB Installation Bus System*, Publicis Verlag, Munich; 2001.

[6] A.S. Tanenbaum, "Computernetzwerke" *Pentice Hall Verlag GmbH*, Deutschland, 1997

[7] L. Rauchhaupt, J. Hähnliche, "Opportunities and problems of wireless fieldbus extensions", *Proc. FeT99, Magdeburg 1999*, pp.48-54, September 23-24.

[8] D. Buchholz et al., "Wireless in-Building Network Architecture and Protocols", *IEEE Network Magazine* 1991, pp.31-38.

[9] J. Decotignie, H. Dallemagne and A. El-Hoiydi "Architectures for the interconnection of wireless and wireline fieldbusses", *Proceedings of IFAC-4th FET 2001*, pp. 285-290.

[10] W. Lilakiatsakun and A. Senevirante, "Wireless Home networks based on a Hierarchical Bluetooth Scatternet Architecture", *Proceedings of the Ninth IEEE Int. Conference on Networks 2001*, pp. 481-485.

[11] T. Saito, , I. Tomoda, Y. Takabatake, K. Teramoto, and K. Fujimoto , "Wireless gateway for wireless home AV network and its implementation", *IEEE Transactions on Consumer Electronics, Aug. 2001*.

[12] S. Mahlknecht, "Virtual Wired Control Networks: A Wireless Approach with Bluetooth", *IEEE Africon* 2002, Vol 1, pp. 269-272.

[13] M. Dunbar, "Plug & Play Sensors in Wireless Networks", *IEEE Instrumentation and Measurement Magazine*, Mar. 2001, pp. 19-23.

[14] L.K. Haakenstad, "The open protocol standard for computerized building systems", *Proceedings of the 1999 IEEE International Conference on Control Applications*, 2, pp. 1585 -1590.

[15] LonMark Organisation, "LonMark Application Layer Interoperability Guidelines and Profiles", www.lonmark.org.

[16] Profibus 2001, Profibus profiles, www.profibus.com.

[17] T. Jepsen, "SOAP cleans up interoperability problems on the Web", *IT Professiona 2001* , 3.

[18] HAVI Organization, "HAVI, the A/V digital network revolution", *White Paper*, www.havi.org.

[19] M. Condry, , U. Gall, P. and Delisle, "Open Service Gateway architecture overview", *Proceedings of the 25th Annual Conference of the IEEE IECON '99 Industrial Electronics Society*., 2, pp.735-742.

[20] B.A. Miller, T. Nixon, C. Tai, M.D. Wood, "Home networking with Universal Plug and Play", *IEEE Communications* Magazine 2001, 39/12, pp. 104 -109.

[21] G.G. Richard, "Service advertisement and discovery: enabling universal device cooperation", *IEEE Internet Computing 2000*, 4, pp.18 –26.

[22] S. Moyer, D. Maples, S. Tsang and A. Ghosh, "Service portability of networked appliances", *IEEE Communications Magazine 2002*, 40/1, pp.116 -121.

[23] Axis Communications AB: http://developer.axis.com

[24] S. Soucek, "Control Network Data over IP Networks: A Tunneling Approach using EIA-709.1", *Ph.D. Thesis, University of Technology, Vienna, 2002*.

[25] EnOcean, "Wissenschaft in Unternehmen: Strom zum Nulltarif", *Spektrum der Wissenschaft Juli 2002*, p.98.

[26] M. Wollschlaeger, "A framework for fieldbus management using XML descriptions", *Proceedings of 2000 IEEE International Workshop on Factory Communication Systems*.

[27] R. Birkhofer, "XML for Automation Devices - A Multi-Schema Approach", *Proceedings of XML Europe 2001*.

[28] P. Krishnamurthy, J. Kabara and T. Anusas-amornkul, "Security in wireless residential networks", *IEEE Transactions on Consumer Electronics 2002*, 48/1.

[29] P. Palensky, and T. Sauter, "Security considerations for FAN-Internet connections", *Proceedings of the 2000 IEEE International Workshop on Factory Communication Systems*, pp. 27 –35.