A Closer Look on Today's Home and Building Networks

W. Kastner, P. Palensky, T. Rausch, Ch. Roesener

Abstract— **This article discusses popular control networks in the area of home and building automation (LonWorks, EIB, BACnet). The comparison includes technical aspects (platforms, security, network management, etc.) and general conditions for development (tools, starter kits, costs, licence policies, etc.). Finally, we identify possible drawbacks and "white spots" on the way to totally integrated and networked buildings.**

Index Terms— **Computer networks, Field buses, Building management systems**

I. Introduction

Control networks are an important basis for modern control and automation systems. Originally being a military development, their first civil application was in industrial automation and aeronautics. Meanwhile, they can be found in a large variety of automation applications like for instance in home and building automation (BACS: building automation and control systems). These networks interconnect heating, ventilation and air conditioning (HVAC), sun blinds, alarm systems, doors and windows, lighting scenes and also domestic appliances (the so-called "white ware" and "brown ware"). The purpose of this "massive networking" is to increase the efficiency (e.g. energy performance) and the comfort of buildings. The market of home and building automation system is shared between a number of proprietary systems and the three standardized main players, LonWorks, EIB and BACnet. Closed solutions like LCN [1] or proprietary BACS of large manufacturers are typically not "open" i.e. internationally standardized and published. Open standards can be implemented by anyone which leads to broad variety of products, healthy competition and a higher product quality.

During the last years, three open building networks asserted their positions in the market: the well established LonWorks and EIB networks and the relatively new BACnet, all three standardized and published. "Which one to take" or "which one is the best one" are questions that can only be answered when all circumstances are known. The systems are very similar and differences can best be evaluated when the desired installation or the respective project is known in all details.

This paper, however, tries to discuss the application areas, interoperability and other technological aspects. Even if the basic principles of these three networks are very similar, there are significant differences when it comes to tools, physical layers or certification. By identifying the strengths and weaknesses of these networks, it is possible to define the requirements for the next generations of networks which is done at the end of the paper.

II. General Requirements

Building networks face the following requirements:

- large number of nodes
- robust physical channels
- sometimes relatively wide physical network - structures
- flexible network management
- low costs

The three subjects of our investigations pursued similar strategies. They consist of small embedded network controllers that use a shared carrier sense multiple access (CSMA) communication media in an event-triggered manner and that use routers to connect rooms with rooms and floors with floors.

The costs are still one point that can be optimized. Especially in private homes this technology still did not have a real "breakthrough" since it is approximately three times more expensive than a traditional electrical installation. Only when the number and the complexity of the functions (like lighting, temperature control, security, etc.) rise, building networks are more economical than traditional electrical wiring. This is the reason why the majority of BACS are installed in large office buildings that need flexibility while having many complex functions (e.g. for facility management systems).

III. LonWorks

LonWorks is a field area network, introduced by Echelon Corp. in the mid-nineties [2]. It is a general purpose and peer-to-peer network. The *LonTalk* stack [3] implements seven protocol layers, similar to the ISO/OSI seven-layer reference model. The term "general purpose" alludes to its large variety of applications in trains, buildings, production plants, etc. The majority of LonWorks nodes is used in building automation,

Manuscript received June 16, 2004.

W. Kastner is with the Department of Automation, Vienna University of Technology, Austria (e-mail: k@auto.tuwien.ac.at).

P. Palensky, is with the Institute of Computer Technology, Vienna University of Technology, Austria (e-mail: palensky@ict.tuwien.ac.at).

T. Rausch, is with the Institute of Computer Technology, Vienna University of Technology, Austria (e-mail: rausch@ict.tuwien.ac.at).

Ch. Roesener, is with the Institute of Computer Technology, Vienna University of Technology, Austria (e-mail: roesener@ict.tuwien.ac.at).

since modern office buildings are sometimes equipped with up to 70.000 nodes.

Since LonWorks is a peer-to-peer network, its network management is relatively sophisticated. There are virtually no simple “slaves” but rather peers with a distinctive need for network management.

The mightiness of the LonTalk protocol with its large variety of transport services (acknowledged, authenticated, request/response, etc.), addressing schemes (physical addresses, logical addresses, group addressing, broadcast, etc.) and network structures (routers, many different transport channels, etc.) almost necessarily lead to powerful middle-ware that demands quite some processing power on the management station: *LonWorks Network Services* (LNS), an object oriented database system, where many network management and integration tools are based on. It registers and manages all network resources like nodes, channel parameters or configuration properties. One of the most popular management tools is Echelon's *LonMaker Installation Tool*®. Its user interface is based on Microsoft's *Visio*® whose schematics help organizing the network structure in a graphical and visual way. A powerful competitor to the LNS-based tools is *ICELAN2000* from IEC, a professional network management tool.

LonWorks' interoperability guidelines are issued by LonMark International, an NPO (non-profit organization) that designs and maintains LonMark “objects”, functional profiles and standard data types [4]. These profiles are easy to implement and offer a high level of functionality. A special feature of LonMark compliant nodes is their ability of self-documentation: they can tell who they are, where they are, what they do, etc. This helps a lot during network management.

LonWorks technology is standardized in the USA under EIA 709.x [3] and in Europe under prEN 14908-x [5]. These standards cover the LonTalk protocol stack and the physical media. The functional profiles are not yet standardized.

Large LonWorks networks use high speed channels (LonTalk/IP or 1.25 Mbit/s twisted pair) as backbones that – via routers - interconnect the standard 78kbit/s twisted pair segments of the field devices. The network topology of the famous FTT10 channel is as flexible as can be, there is no need for nerving bus-, tree- or any other topology. It is robust, galvanically insulated, polarity-insensitive and – despite its costs - maybe one of the main reasons to choose LonWorks over other technologies.

Nodes can be built at relatively low costs, depending on their hardware features and their performance starting from approximately USD 10. References and success stories in various businesses can be found on [6]. Originally the only hardware for LonWorks nodes came from Echelon: the so-called *Neuron Chip*, produced by Toshiba and Cypress. Meanwhile other companies start to implement LonWorks technology in hard- and software which further stimulates competition and innovation (e.g. [7]).

IV. EIB

EIB (European Installation Bus) is an open, standardized OSI-based bus system constituting as a field-bus for building automation. Taking the peculiar specifics of home and building automation applications into account, it was designed for a high number of participating nodes facing low real-time requirements.

EIB is a decentralized, event-triggered system with distributed intelligence. The network is structured hierarchically: The smallest unit is a *line* accommodating up to 256 nodes. A maximum of 15 lines can be connected to a so-called *main line* via line couplers. This kind of structure is called an *area*. As a result, up to 4080 nodes (excluding couplers) can be combined together within a single area. Further structuring of the network can be done using backbone couplers to connect up to 15 areas to a backbone line, forming a *domain*. Each line and each area respectively contains a separate voltage supply in order to maintain the proper functionality of the remaining system in case of a line's failure. Line couplers and backbone couplers are further supporting the reduction of traffic within the particular portions of the network by blocking messages that are not allowed to pass the specific coupler.

Data is transferred over twisted pair at a rate of 9600 bit/s, over power line at a rate of 1200 to 2400 bit/s. The implementation of EIB on other physical media (coaxial cable, infrared, radio frequency, fiber optics) is in progress. The interoperability of products manufactured by different vendors is warranted by the EIB-trademark, which was until recently under control of the EIB Association (EIBA) [8]. EIBA is responsible for certifying system and application implementations for compliance with the specification. An EIB network is configured using proprietary software, which is called EIB Tool Software (ETS) maintained by EIBA, too. This software provides the capabilities to assign addresses and to download programs and parameters to the nodes as well as to the couplers in the network.

Within an EIB system, every bus device is addressable in two ways: A device's *physical address* is its unique identifier for naming throughout installation and configuration. It corresponds to the device's location in the logical topology of the network. The physical address is assigned during installation. Once programmed, the physical address is primarily used for downloading application programs to the bus device, for setting/updating parameters in the device and also for downloading *group addresses* to the bus device. Bus devices that fulfil a common task are assembled to a group, communicating by exchanging group telegrams. In contrast to physical addresses, the address of a group does not reflect the subdivision of the EIB in areas and lines, but the members of a certain group may be located anywhere on the bus. The advantage of group addressing is that a group telegram can be received and processed by all members of a group simultaneously. Hence, group addressing simplifies the communication between bus devices and reduces the network traffic, significantly.

The communication model used within the EIB is based on the ISO/OSI 7-layer model with layers 5 and 6 left empty. Each device on the bus has to be able to understand the messages of the EIB protocol. Hence, a special component must be integrated inside the device which is responsible for managing the communication on the bus. This component is called *Bus Coupling Unit* (BCU). BCUs are available as an EIB standard product (in various versions e.g. DIN-rail mounted, flush-mounted) and are composed of a transceiver and a communication controller. The latter is a microprocessor providing the EIB system software (i.e. the EIB protocol stack) and has space for an internal application program. More complex application programs have to be run on a separate microprocessor. In this case, the application processor can access all EIB-related functionality provided by the BCU using the *Physical External Interface* (PEI) which normally acts as standardized interface to simple application modules (switches, temperature sensors, etc.). Alternatively, the processor can implement the EIB protocol stack itself, using a standard transceiver IC for connection to the EIB medium or the TPUART-IC that interacts with the microprocessor on Layer 2. For applications with even higher demands on processing power or on the human-machine interface, PC-based solutions come into play. Connection to the EIB is usually accomplished using serial communication with a BCU. Additionally, *Universal Serial Bus* (USB) interfaces are available for "legacy-free" PCs. For Microsoft Windows based systems, EIBA offers a certified software component called *Falcon* which provides a high-level API for accessing functionality throughout the network stack. For the Linux operating system, which provides an interesting perspective toward cost-effective embedded platforms, both commercial and open-source kernel level drivers for BCU access as well as TP-UART based serial interfaces are available [9].

In 2002, EIB merged with *BatiBus* [10] and *EHS* (European Home System) [11] to form the new KNX standard. Although EIB is now correctly known by the name of *KNX TP1/PL110 S-Mode*, "EIB" will definitely stay as a label for a specific subset of KNX functionality for quite some time. The Konnex Association [12] has taken over EIBA's tasks for providing an independent board for manufactures and cares for the specification [13] which is laid down in the European Standards EN 50090 [14].

V. BACnet

In the late 1980s several manufacturers and operators of building automation facilities started to work on a new protocol standard called BACnet. Under the patronage of the American Society of Heating Refrigerating and Air-Conditioning Engineers (ASHRAE) big efforts were undertaken to take all aspects of building automation (HVAC, control, fire detection, alarms, etc.) into account. Interoperability between devices of different vendors was one of the main objectives. Usually the decision for a specific vendor restricts future enhancements due to non-interoperable devices. By providing a solid standardized basement, the manufacturers of building automation equipment should be encouraged to build truly interoperable devices.

In spring 1995, ASHRAE published the result of this effort: the first version of the BACnet Standard [15], preceded by three drafts and hundreds of comments worldwide. Over the last years, BACnet has been improved continuously and become an international ISO standard [16].

Like in other modern control networks, BACnet specifies various kinds of interfaces to physical processes. This includes inputs for measuring parameters and outputs for setting values (both digital and analogue), as well as control loops, schedules and many more. Every piece of information in BACnet is encapsulated within a BACnet *object*. These data structures are distributed over the network and may, besides environmental parameters, represent results of calculations, trend analysis or other non-physical values. The information which is stored in such objects is available to all other nodes in the network by message exchange mechanisms called *services*. These services follow an event-based approach and are separated into 5 different classes, like alarm and event services or object access services.

The main focus of BACnet lies on the "higher layers", the interoperability and functions. But still, the standard also defines several transmission media types. These types range between cheap low bandwidth technologies like Master Slave/Token Passing (MS/TP), a simple BACnet specific transport protocol based on EIA-485, and high performance physical layers like "Ethernet" (ISO 8802-3). For Internet connectivity, the BACnet/IP protocol has been added to the first version of the standard in 1999.

The BACnet standard defines a unified way of publishing the functionality of BACnet devices. It provides a template which is called *Protocol Implementation Conformance Statement* (PICS). With this document the manufacturers are able to describe the behaviour of a device in detail. Another way to achieve a high level of interoperability are so-called *Plugfests*. At these informal meetings technicians of different manufacturers convene and mutually test their products for interoperability.

Currently there are three *BACnet Interest Groups* (B.I.G.s) in North America, Europe and Australian/Asia which locally convey the application of the standard. The *BACnet Testing Laboratories* (BTL) provide certification services and list devices which are interoperable in respect of the BACnet standard. In Europe these certificates are provided by the WSPCert in Stuttgart by order of the B.I.G.-EU.

Within a building there are various ways to use the BACnet protocol. In Europe, BACnet is famous as "management backbone" while the field devices – connected via some gateway - are still based on KNX or LonWorks. American installations use MS/TP devices for seamless BACnet connectivity. On this account, also the network nodes which are used in those regions are different: BACnet devices in

Europe are sometimes more complex than those used in North America.

The philosophy of BACnet was to archive interoperability between devices of different manufacturers. The standard allows the composition of multi-vendor installations to satisfy all requirements in building automation.

VI. Comparison by usage

As already mentioned all three subjects of our investigations – LonWorks, EIB and BACnet – are highly specialized and mature technologies for home and building automation applications. Very often non-technical reasons lead favoring one over the other. The availability of local support and maintenance companies or the service around the products (warranties, installation support, etc.) are important economical factors.

The technological differences are, however, not easy to evaluate. Usually, only a given application, a given project or installation, can be the basis for a reliable decision. The differences of these networks are sometimes incomparable, so the price and the performance of a benchmark installation often is the only measurable attribute.

This section lists objective aspects of the given technologies in order to get a first tool to evaluate them. This methodology should help to rate building networks in an as-neutral-as possible way:

Devices are implementations of the respective standards. The number of devices implemented with a standard (and the variety of vendors) can give a hint about the market situation, the usability and the maturity of a technology.

Protocols define the different services within communication. The features of these protocols (connectionless communication, network topology, etc.) are an indication of the flexibility of the technology. Complex protocols might be flexible but might also complicate reaching protocol conformance when new communication members are implemented.

Media describe the hardware for transmission, like twisted pair cables or wireless media (radio frequency, infra-red). It gives information about data rates and future development in communication (size of data packages).

The *maturity* of technology looks into the history of the standards and related (former) standards to discuss the level of development. This might give an outlook about new development and changes within the standard.

Reliability of transport copes with the ability of the technology to offer methods (both hardware and software) for robust data transport. How is data secured?

The *network scalability* describes how the topology deals with growing structures and how does this affect the network management.

Interoperability within the technology, but also between devices of different standards (gateways, network transitions), is another important factor for the success of a BACS.

Security is a very important topic and ignored far too often. As control networks often provide functionalities for supporting life safety (fire alarm) and security applications (burglar alarm), the system itself has to be on a high level of security (in contrast to the secure data transmission in the point *Reliability of transport* this security means things like authentication or cryptographic protection against unauthorized reading and tampering of data).

TABLE I
Protocols

	LonWorks	*EIB*	*BACnet*
Profiles	X	X	X
Layer 7	X	X	X
Layer 6	X		
Layer 5	X		
Layer 4	X	X	
Layer 3	X	X	X
Layer 2	X	X	X
Layer 1	X	X	X

The devices used in buildings can be classified into white ware appliances (refrigerators, washing machines or dishwashers, etc.), small electronic devices (e.g. a blender or a vacuum cleaner), brown ware (like VCRs, stereo systems or TV-sets), office equipment (devices with special office application, e.g. personal computers, printer, but also telephone or fax), network infrastructure (router) and interoperability devices (gateways between networks of different technologies).

Domestic appliances are typically not yet part of a home and building automation application. First exceptions are Siemens' HES (Home Electronic System) with its Home Assistant [17] or the first prototypes for combining Bang & Olufson's HiFi Systems with EIB.

BACnet with its native IP support under BACnet/IP has a strategic advantage. It will seamlessly integrate into the very likely IP-dominated future of entertainment equipment. EIB and LonWorks are already offering a large variety of IP Gateways for this purpose. The same holds for Office Automation equipment (personal computers and the like).

All three networks describe their protocol stacks in the ISO/OSI 7-layer reference model style. Only LonWorks implements all these seven layers which results in a mighty and complex LonTalk protocol.

EIB orients its network structure by design on the structures of buildings: rooms, floors, etc. It is the tree topology which is therefore the basis for EIB wiring [18]. LonWorks and BACnet offer more flexibility in this aspect as well as in its scalability [2].

All three networks offer a variety of physical media. BACnet inheres a special role since it is very tolerant

TABLE II
MEDIA

Channel	*EIB*	*LonWorks*	*BACnet*
TP (a)	X	X	X
TP power	X	X	X (c)
Power Line	X	X	X (c)
Radio	X	X	X (c)
Fiber Optics		X	X (c)
Infra Red	X	X	X (c)
Ethernet		X (b)	X
IP	X (b)	X (b)	X
ARCnet			X
Telephone line			X

(a) Twisted Pair
(b) tunnelling, only
(c) no native support, present if LonTalk is used as physical layer

TABLE III
STANDARDIZATION EFFORTS

	EIB	*LonWorks*	*BACnet*
1986		Echelon founded	
1987	INSTABUS development community founded		ASHRAE SPC135P founded
1988		LonWorks announced	
1990	EIBA founded		
1991		Tools and Chips available	Public draft of standard
1992	First products available DIN V VDE 0829		
1994		LonMark founded	
1995			ANSI/ASHRAE Standard 135-1995
1998	prEN 13154-2	EIA-709.1 prEN 13154-2	ENV1805-1
1999	Konnex Association founded		ENV13321-1
2003	EN 50090		ISO 16484-5:2003
2004		Ballot for prEN 14908	

Details:
ENV1805-1 „Data Communication for HVAC Application Management Net – Part 1: Building Automation and Control Networking (BACnet) for management layers
ENV13321-1 „Data Communication for HVAC application automation net – Part 1: BACnet, Profibus, WorldFIP“ for automation layer
EIA-709.1 „Control Network Specification“, US Standard
prEN 13154-2, European Standard for LonTalk, EIB, etc.
DIN V VDE 0829 “HBES (Home and Building Electronic Systems”
EN 50090 “Home and Building Electronic Systems (HBES)”
ISO 16484-5: „Building automation and control systems - Part 5: Data communication protocol“
prEN 14908: European Standard for LonWorks

regarding its lower layers. Even IP or LonWorks are allowed for the transport channel.

EIB and LonWorks on the other hand are tightly coupled to their media and it was only on the last years that they emancipated from them. Currently they use Ethernet/IP only for tunneling purposes, but it seems to be natural that eventually EIB or LonWorks communication objects will be transported natively over IP.

Surely, if IP is transported via some certain channel (ISDN, Ethernet, wireless LAN, etc.) the 'X' for IP is subsequently valid for this channel type as well.

The foundation for all three networks that are investigated here was laid in the late eighties. LonWorks and EIB originally were industrial products that later found their way into various standards. BACnet on the other hand was intended as standard from the beginning that was followed by products later.

EIB and BACnet do certification on the device itself, while LonWorks just does a formal test of the application layer interface. In Europe, it is expected that all network technologies in buildings must follow a common testing and certification procedure in future [19] which will probably unify the certification procedure.

An extremely important factor for building automations is interoperability. Multi vendor systems and “second sources” only all manufacturers follow certain rules.

EIB and LonWorks follow similar principles in the first step: strong data types like *EIB Interworking Standard* (EIS) or *Standard Network Variable Types* (SNVTs) help to make data more transparent and comprehensive. *LonWorks' Functional Objects* and *EIB's Object Interworking Standard* add one further step to organize data and functionalities in a standardized way. BACnet uses object oriented interoperability as well. However, its data types are not that strictly handled as LonWorks’ SNVTs.

Security seems to be an unwanted child in home and building automation [20]. The three classical aspects of

TABLE IV
SECURITY FEATURES

Service	*EIB*	*LonWorks*	*BACnet*
Encryption	n/a	n/a	DES
Integrity	n/a	challenge-resp. mechanism	DES
Authentication	plaintext password based access control	challenge-resp. mechanism	challenge-resp. mechanism using DES

network security encryption, integrity and authentication are only implemented in BACnet.

EIB and LonWorks only offer weak security mechanisms. Especially the initial network management ("commissioning") exposes security weaknesses. BACnet implements the popular *Data Encryption Standard* (DES) [25] which uses a symmetric 56-bit key. Due to the limited key size of DES and resulting successful attempts to crack the encryption, DES does not provide a very high level of protection any more.

Network management for building networks is, due to their possibly large number of nodes, a difficult issue. LonWorks offers, as already mentioned, the large group of LNS-based tools and some non-LNS based ones. One point of criticism that is valid for both families is their closed architecture – open standards (in this case maybe an SQL-based database) and interfaces would boost innovation and lead to more and more optimized tools.

The question of an open standard database for all tools does not really apply to EIB, since there is only one tool, namely ETS. The disadvantage of missing competition and a de-facto monopole on management software is compensated by the high functionality of ETS and the strict certification procedure: every certified EIB product can be administered by ETS.

In BACnet there is currently no standardized management tool available. Every manufacturer is free to use any tool which fits his needs and used transport media best.

The reliability of the transport very much depends on the lower layers in the protocol stack. LonWorks for instance uses 16 bit CRC (cyclic redundancy check) checksum while EIB uses a number of parity bits that allow for detecting single bit errors. Both technologies have acknowledged or request/response services and repeat packets that are not successfully transmitted (i.e. Acknowledged). Depending on the installed transport media, BACnet uses different mechanisms for achieving secure data transmissions. While MS/TP for instance uses only a simple CRC checksum, BACnet/IP over Ethernet is able to utilize all error detection capabilities of TCP/IP over this physical media.

All three network technologies have some sort of router and segment concept. Combined with the CSMA arbitration it is relatively easy to add nodes or network segments. The only limiting factors are the channel bandwidth, the maximum number of nodes (mainly electrical reasons), and the address space (software boundary).

Merely EIB sometimes reaches its upper bound in terms of bandwidth, since it operates on 9,6 kbit/s, which on the other hand can be easily avoided when EIB segments are interconnected via Ethernet. EIB theoretically has a maximum number of 57.600 nodes [21] while in BACnet the unique 22 bit wide object identifier marks the limit of the address range. A BACnet network has therefore a maximum of 2^{22}, i.e. 4194304, nodes. LonWorks' maximum number of nodes is, based on the "Neuron ID", 2,8E14 but when subnet/node addressing is applied, this number lowers to 32385 [2] within one "domain" (2^{48} domains possible). Typically nodes that belong to one trade like "light" or "heating" are put into one common domain. Electrical limitations of the physical channel (e.g. RS485, used by all three of them, allows only a maximum of 32 nodes per segment) can be overcome with routers and repeaters.

Concluding it can be said that all three networks are very well suited for home and building automation. They offer a similar level of maturity from the physical characteristics up to the tools. Recently, combinations like BACnet & EIB or BACnet and LonWorks became popular, probably due to the lack of suitable BACnet field devices. Improvements are possible and necessary for all three of them. The main goals are addressed in following chapter.

VII. FUTURE ASPECTS

The networks presented in this document are the worthy "winners of the fieldbus wars" in the 1990s. But still there is room for improvement as well as wanted aspects that might not be feasible with these networks.

One major obstacle on the way to the mass market is still the price. In order to be competitive to traditional electrical installations the hardware prices must be reduced dramatically. The protocol stacks, however, are still too large to fit into a 1$ node. One way out of this would be to use hierarchical where the outermost capillaries (segments) consist of extremely simple technologies. [22] also describes scalable protocols, *protocol data units* (PDUs) and hardware.

Another key to success will be the seamless integration with other networks in buildings like

- multimedia networks,
- telecommunication networks, and
- office networks.

The reason for merging these networks with building automation networks is not only "saving wires", but more common applications ("from IO to CEO") and management. Since all these networks appear to be based on IP technology sooner or later, the goal of convergence leads to convergence of IP-based networks and building automation networks. This does not only mean that the same physical channels or more or less "invisible" gateways are used. Of much more relevance are the higher layers and interoperability. Common data types and semantics should be the main focus of the convergence efforts. There are already first attempts, based on XML (www.obix.org), to unify data structures and to make building network information more suited to the Internet.

A further point for improvement is network management. Currently the three networks desire sophisticated network management (with tools, databases, etc.). Only KNX shows first promising plug-and-participate mechanisms that greatly simplify installation. What is needed is a consistent coexistence of traditional network management, plug-and-participate (automatic assignment of network addresses) and plug-and-work (automatic configuration of the applications, as far as possible).

One topic that will keep us busy during the next years are wireless automation networks. Features like energy-aware protocols or ad-hoc networking make wireless networks very attractive for building automation [23]. The three examined network technologies are not designed for nodes that "appear" and "disappear" sometimes, which is possible in wireless networks. Imagine nodes that are mounted in the car but should participate in a building application (think of fire alarm): the nodes in the car come and go as the car does. The protocols and the respective network management of future building networks must therefore be capable of for instance ad-hoc networking and location based services.

Most security aspects like encryption and authentication are currently out of the scope of standardized building automation protocols. The augmented use of networking functionality in various areas requires strong security principles to avoid misuse. A malicious change of the controlled temperature in a regular room may be regarded as disturbing; within a sensitive area like a server room it may be devastating. Lessons learned from electronic commerce should be applied to building automation networks. As in electronic commerce, key distribution and key management are the real challenges, especially when the network is expected to be flexible [24].

One problem in demanding these new features is that they might violate an existing protocol standard (conformance) or higher layer agreements (interoperability). It is now the task to find out if the new features are important and valuable enough to risk incompatibility with existing installations or if it is possible to keep backward compatibility.

References

[1] LCN Gebäudetechnik http://www.lcn.de

[2] Loy, D., Dietrich, D. and. Schweinzer, H.-J (Eds.), Open Control Networks, LonWorks/EIA 709 Technology, Kluwer Academic Publishers, 2001

[3] Consumer Electronics Manufacturers Association "The ANSI/EIA 709.1 Control Network Protocol Specification", 1999

[4] LonMark Application Layer Interoperability Guidelines V3.3, LonMark Interoperability Association, USA, 2002

[5] prEN 14908-1 Open Data Communication in Building Automation, Controls and Building Management - Building Network Protocol - Part 1:Protocol Stack, European Committee for Standardisation (CEN)

[6] Echelon Corporation http://www.echelon.com/

[7] Loytec electronics GmbH http://www.loytec.com/

[8] EIB Association online. http://www.eiba.org/

[9] EIB for Linux http://www.auto.tuwien.ac.at/eib4linux

[10] BatiBUS for "on-line" buildings. http://ww.batibus.com/

[11] EHS Association online. http://www.ehsa.com/

[12] Konnex Association online. http://www.konnex.org/

[13] Konnex Association. KNX Specifications, Version 1.1, 2004

[14] EN 50090: Home and building electronic systems (HBES).

[15] ASHRAE 135-1995] ANSI/ASHRAE Standard 135-1995 - BACnet - A Data Communication Protocol for Building Automation and Control Networks. American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc., 1995.

[16] Building automation and control systems – Part 5: Data communication protocol. ISO 16484-5:2003, International Standards Organisation, 2003.

[17] de-SPECIAL Bussysteme für die Gebäudeinstallation, ISBN 3-8101-0124-9, Hüthig & Pflaum Verlag, 1999

[18] T. Sauter, D. Dietrich, W. Kastner (Eds.), EIB Installation Bus System, Publicis, 2000.

[19] European Building Automation and Controls Association http://www.eubac.org/

[20] P. Palensky, "Smart Card Security for Field Area Networks", Proceedings of the IEEE-Siberian Conference on Communications and Control SIBCON-2003, Tomsk, 1.-2.10.2003

[21] "Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications", IEEE Standard 802.3, IEEE Inc., New York, USA, 2002

[22] P. Palensky, Requirements for Next Generation Building Networks, Proceedings of the International Conference on Cybernetics and Information Technologies, Systems and Applications (ISAS/CITSA), 2004

[23] S. Mahlknecht, P. Palensky; Wireless Demand Side Management in Home and Building Automation; Proceedings of DUE - Domestic Use of Energy Conference, Cape Town, South Africa, (2003), ISBN 095424683

[24] Khalili, A.; Katz, J.; Arbaugh, W.A.; Toward secure key distribution in truly ad-hoc networks Proceedings of the 2003 IEEE Symposium on Applications and the Internet, 2003 , 27-31 Jan. 2003

[25] FIPS PUB 46–1 National Bureau of Standards. FIPS PUB 46–1: Data Encryption Standard. 1988.

Wolfgang Kastner is associated professor at Vienna University of Technology. Among others, his research interests include: field area networks and their connection to higher networks, as well as component and service oriented frameworks.

Peter Palensky holds a Dr. degree from the Vienna University of Technology, Austria and is a scientific employee of the Institute of Computer Technology (Vienna Univ. of. Techn.). His research areas are distributed applications, computer networks and energy management. He teaches Microcomputer Architecture and Distributed Systems and leads a number of industrial and academic projects about security, data acquisition and communication technology.

Thomas Rausch received the M.S. degree in computer science from the Vienna University of Technology in 2003. He is currently part of the scientific staff at the Institute of Computer Technology (Vienna Univ. of. Techn.). His research fields include control networks, routing algorithms and distributed systems.

Charlotte Roesener has graduated from the Vienna University of Technology, Austria and is a scientific employee of the Institute of Computer Technology (Vienna Univ. of Technology). Her research areas are automation, bionic, psychoanalytical modelling and data processing.