Bachelor thesis
Powerline in Building Automation

Jürgen Maier
MatrNr.: 0825749
Stud.Kennzahl: 033 535
mail: e0825749@student.tuwien.ac.at

September 24, 2011

Erklärung zur Verfassung der Arbeit

Jürgen Maier
Eschenweg 1, 2223 Martinsdorf

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit - einschließlich Tabellen, Karten und Abbildungen -, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

(Ort, Datum) (Unterschrift Verfasser)

Contents

1 Abstract

This thesis, "Powerline in Building Automation", discusses the communication of electronic devices over existing powerline systems in a building.

The thesis is split into three parts. In the first part powerline communication (PLC) is introduced in general. Afterwards advantages, disadvantages and security issues are discussed.

The second part describes different protocols used with PLC. First an overview of each protocol is given, followed by a closer look on how the powerline communication is realised. The protocols chosen for this thesis are:

- LonTalk
- KNX powernet
- X10
- IPC
- UPB
- CEBus
- digitalSTROM

In the third part all protocols are compared to one another and a short market analysis is added.

I want to thank Ao.Univ.Prof.Dr. Wolfgang Kastner for his support and guidance while writing this thesis and Sandra Burin for her patience.

2 Powerline in Building Automation

2.1 Home and Building Automation

Home and Building Automation systems work generally similar. Sensors and actuators are connected to control several functions of an indoor environment. There are many different technologies available for the underlying control network, which differ both on the logical and the physical layer.

Building Automation (BA) - According to [13], BA systems are designed to control and manage building service equipment. The systems help to improve comfort while trying to use the available resources in an efficient way. The overall costs can be reduced not only by less maintenance but also by decreased energy consumption.

In a BA system several parts are controlled. The traditional domains are Heating, Ventilation and Air Conditioning (HVAC) as well as Lighting/Shading. Via automation systems energy consumption can be monitored at a central station, reduced and even automatically prevented. New technologies gain more and more intelligence by cooperating with an increasing number of sensors to estimate the future needs. For example, an HVAC system counts the number of people entering and leaving a room and adjusts the air cooling.

Nowadays new technologies like safety and security are integrated into BA systems. Safety systems are responsible for controlling the building itself and protecting it against malfunctions which could harm people. An example here is a fire alarm system. Such subsystems are connected so they can be observed and controlled at a central station. Also, security is a rising subject in BA. This includes, for example access control and intrusion alarm.

Home Automation (HA) - According to [13], comfort and prestige are the key drivers for HA systems. With respect to energy efficiency and economic benefits popular applications for HA are the control of domotics, multimedia devices ('brown goods') and housekeeping appliances ('white goods').

In difference to BA, HA systems are operated by an engineer only in rare cases. Most users have never worked with such a system before. Therefore, there are other prerequisites for HA than for BA. HA systems have to be easy to configure and use, and they also should support most devices that can be found in homes. Easy installation of additional devices (plug'n'play) is also desireable.

From the perspective of the system level, Building Automation and Home Automation are similar to one another. They both read sensors, control actuators and report the status to a central position. However, in Building Automation it is the goal to make a building cheap, safe and secure with respect to the people that work in it. So everything is done to reduce energy while providing a comfortable environment. In Home Automation the system is mainly used to make life easier. So for example it would be possible to turn the lights on in the bathroom, to activate the coffee machine and the TV at once with a single switch beside your bed. The responsible system is designed for simple handling and configuration so that everyone can integrate such a system into his house. Another difference according to [13] is the amount of devices involved. While in HA systems only a limited number of units have to be controlled the amount in

BA systems is much higher. However the complexity of HA systems should not be underestimated because of the special requirements and the heterogenity of the participating devices.

2.2 Powerline Communication

2.2.1 Description

The term Powerline Communication (PLC) describes a system which communicates over the same line which distributes the power signal. Overall the powerline is a very noisy medium.[1] That is the reason why communication protocols from other media like TP cannot be used on a powerline network. Therefore, it was necessary to develop new mechanisms that are resistant to the problems occurring on powerlines to make a communication possible. As we will show in Section 3 the different protocols meet these requirements in various ways. An effective solution is to manipulate a sinus signal in a specific modulation scheme and superimpose the resulting signal onto the power signal. The receiver then splits both signals and regenerates the data sent.

In the following, a short overview on different modulation schemes is shown. More details can be found in [5], [30] and [27].

Amplitude Shift Keying (ASK) - Through this method data are encoded by an alternating amplitude of a signal. A special form of ASK is Binary ASK (BASK). It is often used in implementations and encodes the data by either setting the amplitude to the original value or to zero. Therefore the signal is present in its original form or not at all. That is why this modulation scheme is also called ON/OFF keying.

Frequency Shift Keying (FSK) - Here the symbols are encoded through an alternating frequency of the signal sent. If the gap between the frequencies representing '0' and '1' is narrow then it is called Narrow FSK (NFSK). If this gap is big compared to the transmission speed it is called Spread FSK (SFSK).

Phase Shift Keying (PSK) - As the name implies the data are encoded through the phase of the signal. A popular form is Binary PSK (BPSK) which encodes 2 different states.

Spread Spectrum - The idea of the Spread Spectrum modulation is the distribution of the signal over a wide frequency band. This makes the signal more resistant against noise and (un)intentional jamming. We further distinguish between Direct Spread Spectrum (DSS), Frequency Hopping Spread Spectrum (FHSS) and Chirp Spread Spectrum (CSS).

All protocols have in common that they reduce the communication speed for a better and more reliable communication. The throughput of the different protocols reaches from several bits to some kBits. Compared to Information Technology this amount is rather low but for simple control tasks, as they appear in BA, this is more than needed.

[1] For further details see Section 2.2.3.

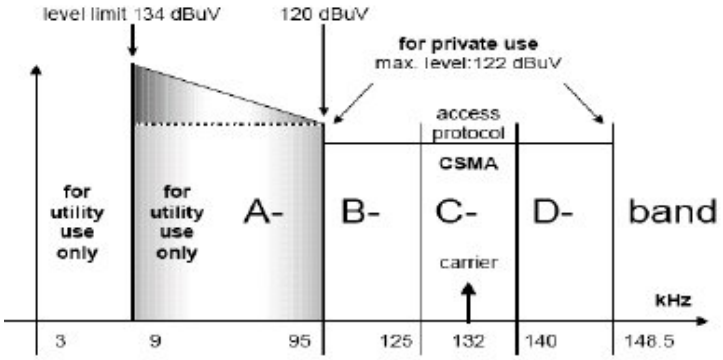

Figure 1: CENELEC EN 50065 standard [6]

Only signals with specific frequency components are allowed to be used for communication beside the 50 Hz power signal on the powerline. In 1991, the European CENELEC Standard EN 50065 was introduced, which regulates the use of the frequency range from 3 to 148.5 kHz in Europe (Figure 1). This standard differs significantly from the one used in the United States or Japan. Thus, it is not possible to use their devices in Europe. In this standard not only the allowed frequencies but also the maximal signal level for the signal frequencies are specified. Compared to the European standard the US system allows a much wider range of frequencies to use. More information to EN 50065 can be found at [6].

EN 50065 divides the frequency range into 4 bands:

A - This band reaches from 3 to 95 kHz and is reserved for the power suppliers. The maximal signal level is defined by 134 dBμV (= 5V) at 9 kHz up to 120 dBμV (= 1V) at 95 kHz.

B,C,D - These bands are intended for private use. The B band reaches from 95 to 125 kHz, the C band from 125 to 140 kHz, and the D band from 140 to 148,5 kHz. The maximal signal level in these bands is 122 dBμV (= 1.25V). In the C band there is furthermore a carrier sense multiple access (CSMA) protocol defined. With the other bands no such definition has been made.

2.2.2 Motivation for PLC

When designing a communication system in a building, the decision for the appropriate communication medium is one of the first that has to be made. If a cable based technology is chosen the next step would be to plan where and how cables are installed. For new buildings these decisions can be integrated into an early planning stage, so only a small amount of extra costs would emerge. In existing buildings, however, this might become a very challenging task. The

walls have to be pried open to insert the cables which is very expensive and in some buildings even impossible. According to [17] this is the main advantage of PLC. With powerline communication systems no new or additional cables have to be integrated into the house.

The advantage of powerline against radio, which also does not require extra cabling, is, that the signal level can fluctuate much when radio technologies are used. Many new buildings are built with armored concrete which weakens or even blocks radio signals. To compensate this phenomenon more radio stations have to be installed and eventually even have to be connected with a cable. If such an action is necessary, radio based systems lose their main advantage compared to cable based systems. Due to the fact that communication on the powerline does not face such weakening or blocking effects, it should be possible to communicate across a whole construction in sufficient quality in an average building. How good the communication parameters are depends on the installed wires and the complete power network but also on the installed devices. The communication parameters like e.g. maximum cable length should be calculated as early as possible to prevent later communication problems.

[23] points out that PLC, different from other technologies, does not interfere with other devices in the building like it could happen with radio communication, if the protocols mentioned in this thesis are used. However disturbances might occur when high frequency signals (MHz range and higher) are transmitted. Also reflection issues, which might occur with infrared communication methods, can be neglected with powerline systems. Another advantage of powerline systems is, that they can be installed easily where they are needed. The only prerequisite is a power socket, which is normally available in each room.

The main area of application for PLC can be specified as control networks in buildings where

- the integration of a cable tree is too expensive or not possible
- radio communication systems are not practical
- the available cabling is capable of the desired functionality
- the communication system shall be cheap and easy

2.2.3 Problems with PLC

In this section the problems that might emerge when power line communication systems are used are described shortly. For a more detailed discussion of the physical problems see [7] and [28].

As mentioned in section 2.2.1 the transmission speed of powerline systems was chosen at a low point to ensure a communication free from errors. For that reason the protocols described here can be mainly used in control networks. For multimedia networks, e.g. to stream video data, there is simply not enough bandwith available. For such installations other protocols have to be chosen.

A power line communication system can not be installed everywhere. Some devices can affect or even disturb the communication. So it is essential to check before the installation, as well as while operation from time to time, if the installed devices or devices that shall be installed decrease the communication quality. Depending on the used communication protocols units affect a specific

system more or less. The abilities of the installed powerline cabling for powerline communication also have to be investigated.

The power line was designed to only carry power signals. Therefore it has an overall very bad noise characteristic. The problem is, that depending on which devices are connected, the noise is always different. It even differs when varying devices are activated and is also affected by the noise produced from neighbouring buildings. So it is impossible to avoid it completely. Noise can even destroy a communication if for example it appears at the same frequency of the communication protocol. Therefore noise on a power line has to be investigated very thoroughly. Specific details can be found in [8], [31] and [18].

[34] and [29] distinguish between three kinds of noise:

Noise - This type of noise is randomly divided over the whole spectrum. On a power line system there is a high noise density up to about 20 kHz. Beyond that frequency the density decreases with increasing frequency. At about 150 kHz there is only about 1/1000 of the value at 20 kHz left. It is not possible to filter that noise type because of the random spreading.

Small band noise - This type produces noise only on a small section of the frequency spectrum which can be seen as spikes. It can be cut out with a band stop filter.

Impulse noise - This is a very short (typically from 10 to 100 μs long) voltage spike on the line. We have to distinguish between two different forms of impulse noise, periodic and aperiodic noise. Periodic noise is e.g. produced by light dimmers and occurs always at the same time e.g. once a halfcycle by light dimmers. The aperiodic noise is produced by switching a device on or off. Nothing is known in advance about this kind of noise, neither the time, the duration nor the signal level. That is the reason why it is the hardest to handle.

To determine the future noise before the installation, each installed device can be categorised as one of four different classes depending on how much noise it produces. Each class has a characteristic number that defines how much noise the devices in this class produce. A higher number means more, a lower number less noise. The classes can be seen in Table 1. To determine the communication quality of the future system the characteristic numbers of each device have to be summed up. With the result the quality of the powerline communication can be determined. This has to be done independently for each protocol.

2.2.4 Security

[14] differs between *Medium access* and *Device access* as the possibilities to get access to a communication channel. For the purpose of this work the *Medium access* is discussed further because the *Device access* is protocol and manufacturer dependent.

In *Medium access*, the attackers get physical access to the communication channel. This is possible at each single power socket because of the topology of powerline systems (open medium). In most cases nothing more has to be done

K=1	lamps
	jalousie motors
K=10	fridge
	stove
	energy saving lamp
	HiFi- and video devices
K=50	PC
	PC screen
	copy machine
	microwaves
K=1000	USV
	power inverter

Table 1: characteristic noise numbers [20]

to access the data sent on the bus. Then it is possible to copy the complete communication from the power line, as an example.

The most protocols do not take attackers into consideration. They let the application or more precise the transceiver modules encrypt and decrypt the data with a secure encryption algorithm. An exception is digitalSTROM which claims to be tap-proof. That is the reason why the protocol specification is only available for registered members of the digitalSTROM alliance (security by obscurity).

According to [15] LonTalk has some simple security functions built in. For that purpose a random number is sent by the sender after each message. The receiver calculates a hash-code over that number and sends back the produced hash code. The sender compares the code received from the receiver and its own calculation. This method can however just be used to determine if the receiver is real. The communication itself is not encrypted and can be read in clear text from the power line. CEBus also implements a similar method (see Section 3.6.1).

One underlying problem which all power line communication protocols suffer from is that power lines do not start and end at building borders. If no counter measures are taken, a power line communication could be read in the next building and vice versa. This does not only affect the communication quality but is also a security problem. It would be possible for attackers to read the communication of a building from the outside. Therefore special devices are mounted to prevent communication from crossing the borders. Depending on the protocol this is a simple or challenging task. For protocols that use frequency modulation a simple low pass or band pass filter can completely remove the communication signals. It gets more complicated with protocols that change the signal itself like UPB. Here the developers themselves claim that the communication is still readable after a power transformer, which normally destroys every powerline communication.

Further information to security can be found in [16].

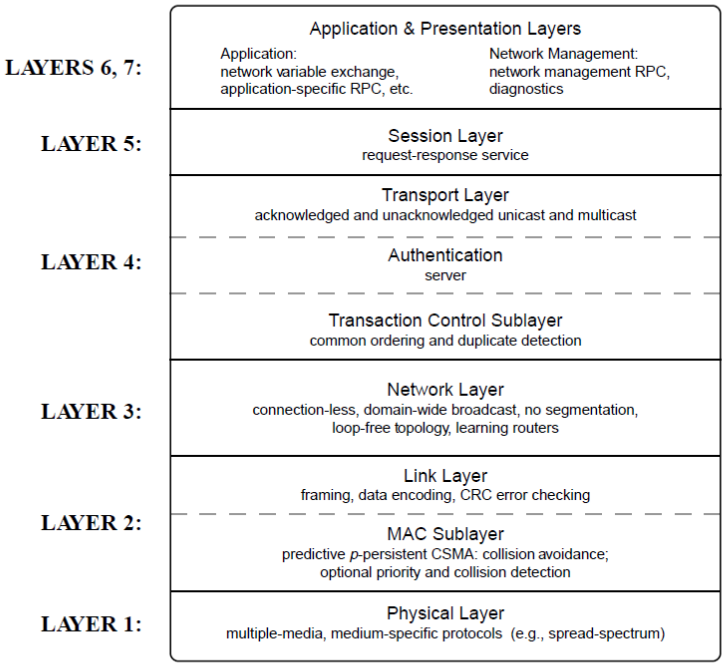

Figure 2: ISO/OSI layers in LonTalk [9]

3 Current Communication Protocols

In this section different protocols are described. It is shown how they work and how they realise a communication on the powerline. As mentioned above, the focus lies on the powerline.

3.1 LonTalk

The LonTalk protocol was developed by the Echelon Corporation and it was designed for control networks. Therefore it was optimised for short messages, low bandwith, low maintenance and multiple communications media. The supported media types include twisted-pair, power line, radio, IR (infrared), fiber optic and coaxial, among others.

LonTalk was designed as a medium independent protocol. So the system works with every transmitter, as long as it fulfills the communication requirements of the so called 'Neuron Chip'. This special chip is described in a following section.

3.1.1 Protocol

The LonTalk protocol uses all 7 layers of the ISO/OSI reference model, which are described underneath (see also Figure 2).

Physical Layer - It is the medium dependent part of the protocol. This layer looks and works in a different way for each type because many different media types are supported. So-called 'channel types' were defined to assure that transceivers from different manufacturers work properly together. To be interoperable to one channel type is a prerequisite to get certified. In one channel type many different characteristics of a communication channel are defined, including the medium type itself (TP, PL, ...), bit rate, the frequency used to communicate and the modulation scheme. The different types on the powerline are described in Section 3.1.2. A detailed overview on all standard channel types can be found in [22].

Data Link Layer - This layer is divided into two parts: the Link Layer and the MAC Sublayer. The latter is responsible for controlling the bus access. It uses a p-persistent CSMA protocol, which is described later in detail. The first supports for a number of reasons a simple connection-less service.

Network Layer - The Network Layer provides a loop free topology even on physical loops. An intelligent routing algorithm is used to minimise overhead and to avoid additional routing traffic.

Transport Layer - The Transport and the Session Layer are the heart of the protocol hierarchy. The Transport Layer can be divided further into the Transport Layer, the Transaction Control Sublayer and Authentication. The Transaction Control Sublayer is used for transaction ordering and duplicate detection. The Transport Layer is connection-less and it is used for the reliable delivery of a message to single and multicast addresses. As an optional feature the Authentication confirms the sender's identity.

Session Layer - It implements a simple Request-Response-Service to provide access to a remote server.

Presentation and Application Layer - Here, besides the usual services for sending and receiving messages, the concept of network variables is implemented. It is possible to share data among nodes with this method.

Addressing

Following [10] each LonTalk address is a layer 3 and 4 address, no addressing is done at layer 2. There are three basic address types with three parameters shown below:

- (Domain, Subnet, Node)
- (Domain, Subnet, Neuron_ID)
- (Domain, Group, Member)

Domain - The domain identifier uniquely identifies a domain in a special context. If a worldwide uniqueness shall be achieved this address can be expanded to 48 bits. If a smaller context (e.g. a building) is used, a smaller size can be chosen.

Generally, communication is only possible within one domain. If interdomain communication is required it has to be realised with an application level gateway.

A domain can also be seen as a management area, meaning that group and subnet addressing are handled by domains and only have meaning in the context of this domain.

Subnet - The subnet field is 8 bit long so 256 different subnets in one domain can be uniquely identified. The subnet 0 signifies that the subnet is undefined or unknown. Subnets are logic channels and need not correspond to physical channels. Two subnets can be defined on the same physical channel or one subnet can be spread over different channels connected via store and forward repeaters or bridges.

Node - The node field identifies a node in a subnet. This field is 7 bits wide. 127 nodes can be addressed per subnet (node address zero is not allowed). The logical node number identifies the node as a member of the subnet. A single node can be member of up to two subnets, which then must be located in different domains. In each of these subnets the physical node gets a logical node address.

Group - Groups are used to identify a set of nodes in a domain. They are intended to collect nodes, with the same or similar functions.

Member - This number uniquely identifies one node in a group.

Neuron_ID - The Neuron_ID is rather a name than an address. Like the MAC address a device gets its Neuron_ID during the production process. This ID is unique in the world and cannot be changed afterwards. The Neuron_ID can only be used as destination address and only in combination with the domain and subnet identifier.

Neuron Chip

The Neuron Chip is the heart of a LonTalk node and implements the LonTalk protocol. It communicates directly with the I/O circuitry (sensors/actuators) and the transceiver. It takes the data from the I/O and the transceivers and computes on this data what shall be done next e.g. set actuator, send value, etc.

This special chip is typically carried out as a microcontroller which can have several CPUs and an integrated memory. Many different types are manufactured e.g. by Toshiba or Motorola. A detailed description for each chip can be found in the corresponding data book. The information for this thesis was taken from [33].

The communication between Neuron Chip and transceiver can be realised in three different modes: differential, single-ended and special purpose. In all modes the transceiver only has the purpose to transmit the data it got from

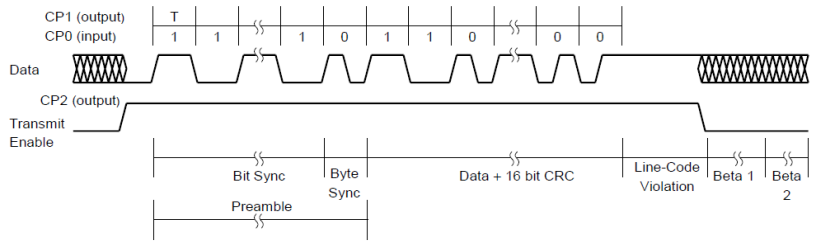

Figure 3: Neuron Chip communication in Single-Ended Mode [33]

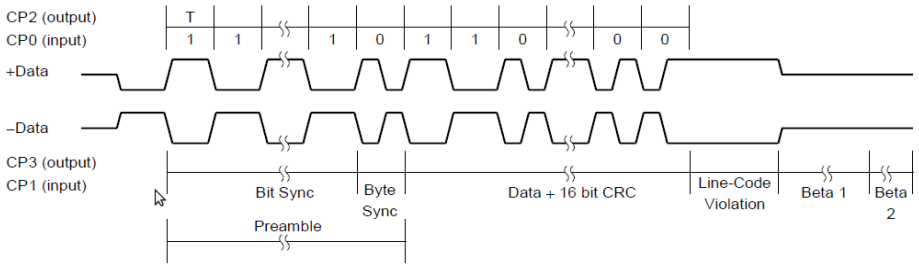

Figure 4: Neuron Chip communication in Differential Mode [33]

the Neuron Chip on the bus and to communicate the received data from the bus back to the Chip. If the transceiver is capable of detecting collisions on the medium it can report this via a special pin to the Neuron Chip.

Single-Ended Mode - This mode is used mostly with external active transceivers. In this mode the communication port encodes and decodes the data using the Differential Manchester code. This code scheme defines a transition at the beginning of each bit. An '0' is represented by a transition in the middle of a bit and an '1' by its absence. This method assures that there are no long DC components on the bus.

At the beginning of the transmission (Figure 3) the Neuron Chip sends a series of '1' on the bus if the medium is free. This series, which is called Bit Sync, is used by the other nodes to synchronise. The exact number of bits sent in the preamble can be configured by the user. At the end of the Preamble one '0', the Byte Sync, is sent to signalise that the data begin. After all data have been sent the Neuron Chip terminates the communication by a line-code violation of the Manchester Code. It therefore holds the line 2 $\frac{1}{2}$ bit times high or low depending on the state of the data output.

Differential Mode - The Differential Mode is equal to the Single-Ended Mode regarding many parts (Figure 4). The main difference is that data are

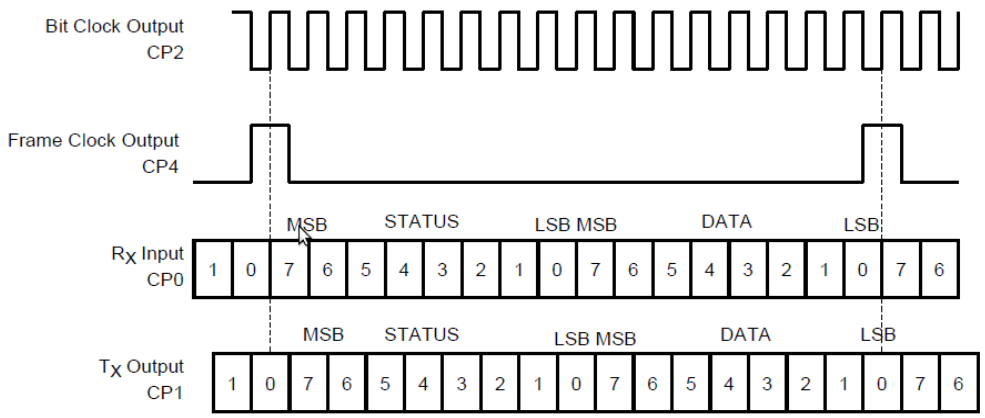

Figure 5: Neuron Chip communication in Special Purpose Mode [33]

sent in differential mode. Two different lines are used for data transmission, one holding the data and the other one holding the inverse data. This communication mode is more resistant against transient errors. The data are extracted by calculating the difference between the two lines.

Special Purpose Mode - Within this mode (Figure 5) the data are provided in an unencoded format and without a preamble by the Neuron Chip. Then an intelligent Transceiver adds its own formatting. When receiving data the intelligent Transceiver removes all formatting from the sender and transfers the received information unencoded back to the Neuron Chip. In this case the Transceiver has to be more complex and has to have advanced functionality like buffers or handshake methods to ensure proper communication between Chip and transceiver.

A particular protocol is used for this mode. It works with packets of 16 bits, 8 bits of status and 8 bits of data and data rates up to 1.25 Mbps.

The Transceiver can support a collision detection mechanism optionally. If the Neuron Chip realises a collision it acts differently depending on which communication mode is used. In Direct Mode the transmission is completed first and then it is checked if a collision was detected. Optionally it can be configured in a way, so that the transmission is aborted if a collision happens during the preamble. In Special Purpose Mode the transmission is aborted immediately. In both modes the transmission is retried as soon as the bus is free again. If no such mechanism is available the only way to detect a collision is to request an acknowledgement.

3.1.2 Powerline

Power line channel types

As mentioned in the description of the Physical Layer (Section 3.1.1) many different channel types were defined for many different media. [22] mentions following channel types for power lines:

PL-10(L-E) - This type uses the frequency band 100kHz - 450kHz and Spread Spectrum as modulation scheme. It supports a bit rate of 10kbps and line-to-earth coupling. Because of its wide frequency range this type cannot be used in Europe.

PL-20(L-N), PL-20(L-E) - These channel types use narrow-band signaling over the 125kHz-140kHz[2] frequency band and support a bit rate of 5kbps. The transceivers are compliant to the ANSI/EIA/CEA-709.2-A and the European CENELEC EN 50065-1 standard. The used frequency band is reserved for private use so this type can be installed with BA. The difference between the two types is that the L-N type uses line-to-neutral signaling while the L-E type uses line-to-earth signaling. As modulation scheme Binary Phase Shift Keying (BPSK) is used, which encodes the data through phase shifts of the signal sent.

PL-20A(L-N) - The transceivers of this type are also compliant to the CENELEC EN 50065-1 standard. They use line-to-neutral narrow-band signaling over a 70kHz - 95kHz frequency band and support 3600 bps. BPSK is used as modulation scheme, as with the PL-20(L-N) and PL-20(L-E) type. The frequency band used is defined as not private and therefore BA systems cannot be built with this channel type.

PL-30(L-N) - Here the Spread Spectrum modulation is used on the frequency band 9kHz - 95kHz. The data are transmitted with line-to-neutral coupling and a maximum bit rate of 2kbps can be reached. This type is CENELEC EN 50065-1 conform, but it cannot be used for private systems because of the specification in the standard.

Bus access

Now we take a closer look at the access protocol mentioned in the Physical Layer. In the LonTalk protocol predictive p-persistent CSMA is used to regulate the bus access. A more detailed description including a pseudo-code of the algorithm can be found at [11].

We have to introduce some variables to understand the correct function of this method (Figure 6):

Beta1 - A fixed duration senders wait after a conversation finished.

Beta2 - The duration of a single randomised slot.

[2] C band in the CENELEC EN 50065-1 standard (Section 2.2.1)

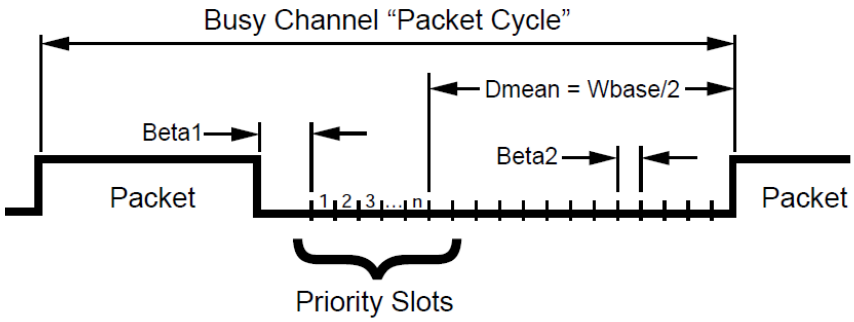

Figure 6: LonTalk bus access [33]

w_{base} - The base number of how many slots of duration Beta2 the random algorithm works on.

BL - A dynamic parameter that represents the channel backlog. The more data are sent over the communication medium the higher this variable gets. BL is always ≥ 1.

T - A random number between 0 and BL*w_{base} that defines how many slots of the length Beta2 a node waits before it begins to send.

If a node wants to send, it monitors the channel. If no transmission is sensed for the duration Beta1 the device states the bus as idle. Then it starts the random timeout of T time slots of length Beta2 (T between 0 and BL*w_{base}). If the bus is still idle when the timeout expires the node starts its transmission. If it senses another transmission before its own timeout expires, it waits until the end of the transmission and starts the protocol again.

Optionally 0 to 127 priority slots can be used. They follow the Beta1 timeout immediately. Priority slots should be defined uniquely to a node so that no collisions occur. These slots are for example used to send acknowledgement answers. In [11], advices are given how the priority fields shall be handled. For example a node shall not send two priority message in sequence. Instead it shall try to send the second message over the normal protocol.

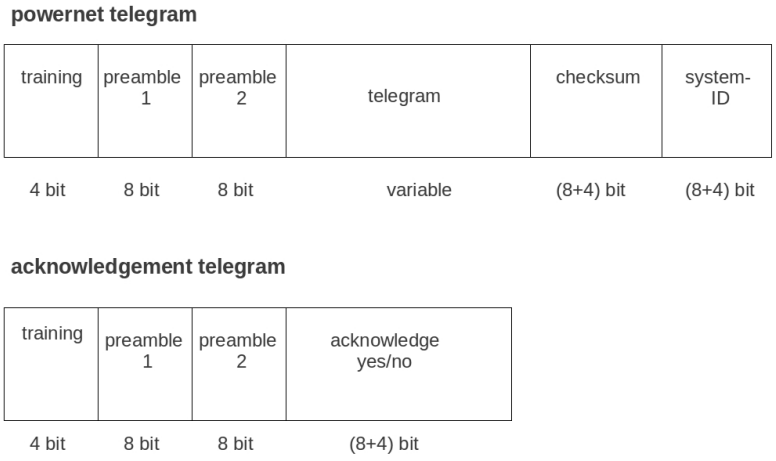

Figure 7: powernet telegram, original: [35]

3.2 KNX Powernet

The powernet protocol is part of the KNX technology which supports many different physical media like twisted pair or radio.

3.2.1 Protocol

In KNX, the OSI layers 1,2,3,4 and 7 are realised. The powernet protocol differs only in the physical layer and the data link layer from the KNX/TP protocol.

A powernet system can be partitioned into 8 areas, each one can then be separated into 16 lines and on each line 256 devices can be addressed. This makes a whole of 32768 devices. Devices can be addressed by group addresses or by their physical address, which has to be unique in the whole system. Please note that devices in one group do not have to be installed in the same area. All in all it is possible to define 15 main groups and 2048 sub groups.

The powernet telegram (Figure 7) is very similar to that of the KNX/TP protocol. The same LPDU is used, which contains much information like source and destination-ID and of course the data. The powernet protocol only adds four start bits and two preamble bytes. A checksum byte and system ID are added at the back. After the message has been sent the receiver sends an acknowledgement message back. This message consists of four training bits and two preamble bytes at the start plus 12 bits that represent acknowledgement yes or no. If the receiver does not fulfill that the sender will automatically resend the message. It is also assured that the sender has the possibility to send the next message right after the acknowledgement of the receiver. So it is taken care that no other device can interrupt its communication. But in that way it is also possible that a malicious device monopolizes the bus.

Powernet uses a time divided protocol to control access to the medium. If a device wants to send on the bus it has to wait till the current message is over (including waiting for acknowledgement and resend). When it recognises that

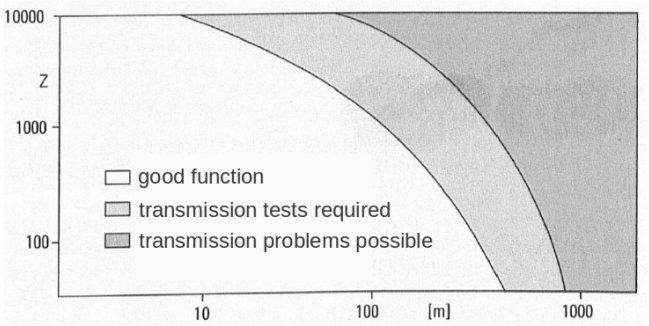

Figure 8: transmission quality depending on cable length and noise ratio, original: [21]

the bus is free it rolls the dice and waits that amount of time before it starts its sending try. If two devices roll the same value, a collision is unavoidable. That is the reason why it is so important that after a reset the pseudo-random parts in each device are set to a different state.

To determine the maximum cable length the characteristic number of all electronic devices connected to the power line have to be summed up (see Section 2.2.3). The calculated number can be looked up in Figure 8 to see if transmission tests have to be done with the desired cable length. This has to be carried out before installation to determine if additional devices have to be installed.

3.2.2 Powerline

The transmission method used with powernet is Frequency Shift Keying. In FSK the symbols '0' and '1' are represented through two different frequencies. To get more accurate results the difference between these two frequencies shall be a multiple of the bandwith. On a channel with no or little noise a frequency gap corresponding to the bandwith is sufficient. As described above the power line is a noisy communication medium. Thus, a much bigger gap should be chosen. This is then called Spread Frequency Shift Keying (SFSK).

As described in [32], powernet uses the SFSK method to transmit data over the powerline. Therefore, the lowest of the three frequency bands for private automation defined in the CENELEC standard from 95 to 125 kHz is used. An '0' is represented by a signal frequency of 105.6 kHz, an '1' by a frequency of 115.2 kHz. Each signal representing one bit has a length of 833,3 μs which results in a baud rate of 1200 bit/s. In a 50 Hz system this means 24 bits per cycle or 12 bits per half cycle.

Powernet was designed for 50 Hz systems and only works in range of $\pm 0.5\%$. Normally Energy suppliers fulfill this requirements but problems can occur when generator current is used for transmission.

Following [35], when sending, the transmitter does not create an analog signal from the beginning but reads predefined values from a ring buffer. These values then are converted by a digital-analog converter to a step signal and after that the signal is smoothed by a low pass filter. Finally, the data signal

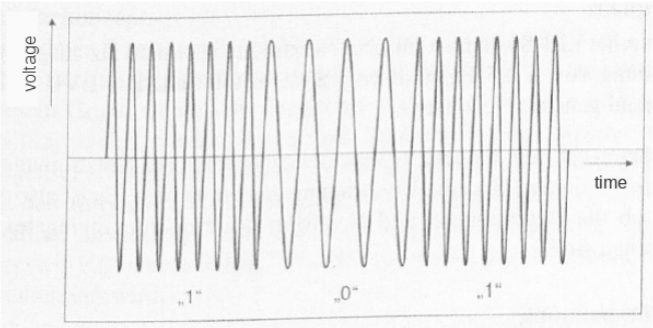

Figure 9: example for a phase continuous signal [35]

is superimposed on the power line signal with a maximum voltage of 1.26 V_{eff}. If the output has to switch from one frequency to another, meaning from '0' to '1' or vice versa, this happens in a phase continuous way. Thus, no jumps occur within the signal sent. Such a phase continuous signal can be seen in Figure 9.

To ensure that signals are received correctly on a noisy medium a special receive method is used in powernet, called matched filter optimum receiver: The received signals are compared to stored reference signals and from that comparison a so called 'correlative coefficient' is calculated. This coefficient is 0 when the signals do not match at all, and represents the highest value if the signals match completely. In between each value is possible. After a complete bit the system decides through a higher-lower-compare if the received signal was a '0' or '1'. With this method it is possible to decode signals even with a lot noise on the line. More information on this method can be found in [35].

Because the power line does not end at the building border the powernet signals have to be filtered on their way to the public power net. This can be done with a band stop filter, which suppresses signals in the frequency band from 95 to 125 kHz. At the mid frequency (110 kHz) signal attenuation has to be greater than 30 dB, at the edges (95 and 125 kHz) 25 dB are enough. This band stops can be used in 2 different ways:

- The band stop can be used to prevent powernet signals from going out in the public net and to prevent noise in the frequency band to come in.
- It also can be used for segmentation. Power line is per definition an open medium which means that every device is connected and that would mean that only one device can send at a time. With bandstops, communication islands can be realised.

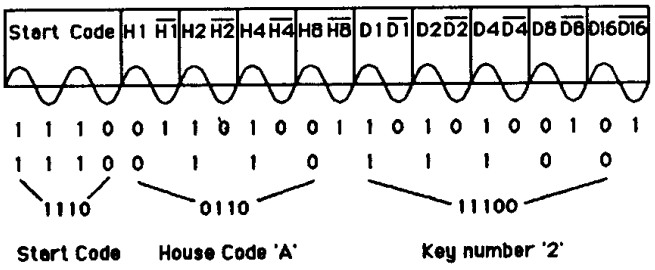

Figure 10: X10 frame when key number 2 is pressed [38]

3.3 X10

The X10 protocol format was first introduced in 1978 and is one of the oldest protocols available. As mentioned in [38] the X10 code format is patent registered by the manufacturers. Only owners of special Power Line Interfaces are allowed to develop X10 receiver and transmitters.

3.3.1 Protocol

Messages in the X10 protocol are sent in an eleven bit frame (an example is shown in Figure 10). This frame consists of:

Startcode (2 bits) - The startcode is the only signal that violates the rule to send the inverted signal on the negative half cycle (see Section 3.3.2). It always has the form 1-1-1-0 meaning that in the first three half cycles bursts are sent. This code is used to indicate the start of a new transmission.

House Code (4 bits) - It is used for addressing devices and covers the range from A to P. For example, each floor in a building receives a different House Code.

Function Code (5 bits) - In the function code field actions and addresses can be transmitted. An '0' in the last bit means that the 4 bits correspond to an address. An '1' means that an action command was transmitted.
The standard X10 protocol can be extended by two special function codes, Extended Code (01111) and Extended Data(11001). After the Extended Data code an arbitrary number of data bytes can be sent. There is no gap allowed between these bytes, because that can lead to an erroneous reception. It is possible to send the number of following data bytes in the first byte. This mode can be used e.g. to transmit analog values.

The 'Extended Code' function code determines that the next 8 bits, that have to follow without a gap, are interpreted as a code. With this method it is possible to extend the X10 system to 256 codes.

To send a command to a device two different messages have to be sent. The first message contains the address of the destination device. When a device reads its address it knows, that the following message has to be read and executed. In

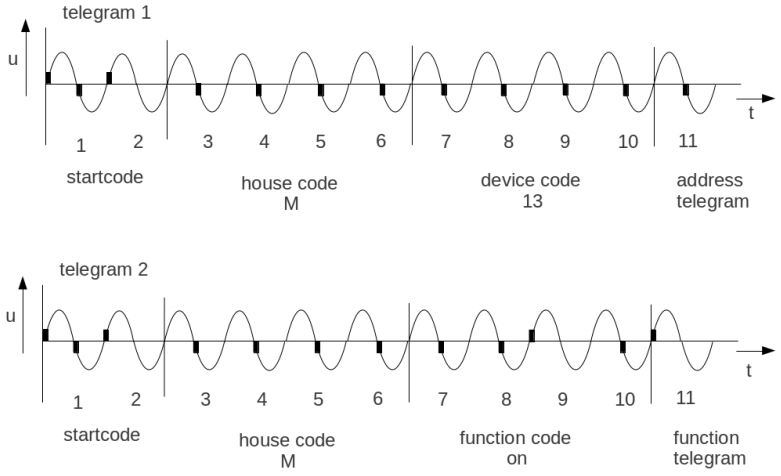

Figure 11: X10 telegram, original: [37]

the second message the action is transmitted. 16 different commands, like ON or OFF can be defined. Figure 11 provides an example for these two messages.

For safety reasons each message has to be sent twice. So two address messages and two action messages have to be sent to a device per command which results in 4 messages à 11 bits. Because of the fact that between the address messages and action messages there has to be a gap of three cycles (three bits) the complete message length accumulates to 47 bits. With a baud rate of 60 bits (in a 60 Hz system) the transmission of a single command over the powerline takes about 0.8 seconds.

Single devices are addressed by their house and address code. In that way 256 different devices can be addressed. If two or more have the same address they are seen as a group. By sending a command to that address each device executes the desired action.

3.3.2 Powerline

The communication in the X10 protocol is realised with frequency modulation. Therefore a 120 kHz, 1 ms long signal with a maximum load of 5 mV_{SS} is superimposed on the power signal. This burst is sent right after the zero crossing point from negative to positive of the power signal because of the low noise there.[3] The communication bursts are broadcasted over the whole installation in the building. Thus, in every power socket X10 communication is available.

A 120 kHz burst represents an '1' while the absence of a burst means '0'. With respect to three phased systems the burst is sent three times, to meet the zero crossing point of each phase. Figure 12 shows the X10 signals on the power line with the timings in a 60 Hz system. On the left picture the timing

[3] As described later, at the other zero crossing point (from positive to negative) the inverted bit is sent.

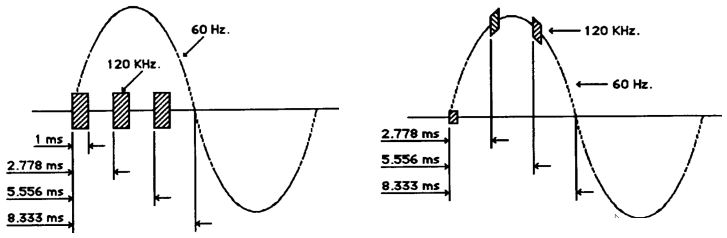

Figure 12: X10 signal [38]

of the signals can be seen. This is not how the signal actually looks like on the line because the bursts are superimposed on the power signal. The resulting waveform can be seen on the right picture in Figure 12.

To prevent the X10 bursts to spread outside of the building a simple low-pass filter, which blocks the 120 kHz signals, is enough. This device can be mounted in the fuse box to make sure no piece of communication can be read outside of the building.

The fact that the signals sent can be read back is used to realise a collision detection bus access protocol. If a transmitter reads a different value than it has sent, it stops sending. Different implementations for the collision detection protocol are possible. For example, the transmitters can wait for a random amount of time after they sensed the line as free before they start sending. This is implemented to avoid collisions because every process starts sending at a different point of time. Of course if two transmitters wait the same random time a collision is inevitable.

An extension to that bus access protocol can be realised if every transmitter gets a unique time interval with a fixed length. If a transmitter wishes to send, first it has to wait for that time interval to pass and then starts its random timeout. The shorter this fixed time interval is, the higher the priority of the transmitter is. However, even though all the extensions, collisions occur from time to time.

The X10 receiver only reads from the power line for a short time after it detected a zero crossing point to reduce errors. It should be the goal of the transmitter to send the burst as closely as possible to the zero crossing point. For error detection the bit is sent in the first half cycle (positive half cycle) and the inverted signal in the second half cycle (negative half cycle). That means that if an ‘0’ has to be sent no bursts would be in the first half cycle (representing ‘0’) and in the second half cycle there would be three bursts (representing the inverted ‘0’). Another error reduction arrangement is to accept only signals that have a sending load higher than a specific value. So they can be differed from noise in the specific frequency range.

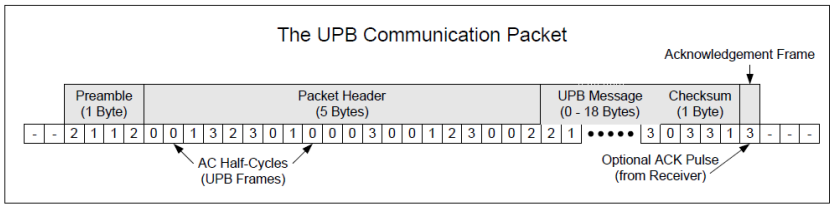

Figure 13: UPB frame format [26]

3.4 Universal Powerline Bus - UPB

UPB was developed by the Powerline Control Systems (PCS) company as improvement of X10. According to [25], UPB claims to be 100 to 1000 times more reliable than X10 and 10 to 100 times more reliable than CEBus or LonTalk at the same price. In this context reliability means that a transmitter/receiver pair works right after installation. The UPB protocol claims a reliability value of over 99.9%.

3.4.1 Protocol

For addressing in UPB IDs are used. Each device gets a unique 8-bit ID between 1 and 250. The IDs 0 and 251 to 255 are reserved for special purposes. To address more devices an additional 8-bit Network ID is used to group the power line in virtual networks. As mentioned in Section 4.2.4, the Network ID has to be unique at one power transformer. Otherwise massive problems can be the result.

The UPB frame contains the following fields (Figure 13):

Preamble - The preamble is used for the receiver to synchronise with the transmitter and to adjust gain and timing to receive the following message as good as possible. It also learns of position and relative size of the pulses. The preamble is one byte with pulses at position 2-1-1-2 (see Section 3.4.2).

Packet Header - In the five byte Packet Header (HDR) the Control Word (two bytes), Network ID (one byte), Destination ID (one byte) and Source ID (one byte) are stored. In the Control Word several control information like packet size and how the packet shall be received is stored. The Network ID defines which UPB network shall receive this message; up to 256 virtual networks. One device can only be part of one virtual network. In the Destination ID and Source ID field the ID of the receiver and the sender are sent. For the receiver the Source ID can be very useful if it has to reply to the transmitter.

UPB Message - The payload has a variable length of 0 to 18 byte. The first byte is reserved for the Message Data ID. This field is used to identify the message. Many messages only contain the Message Data ID.

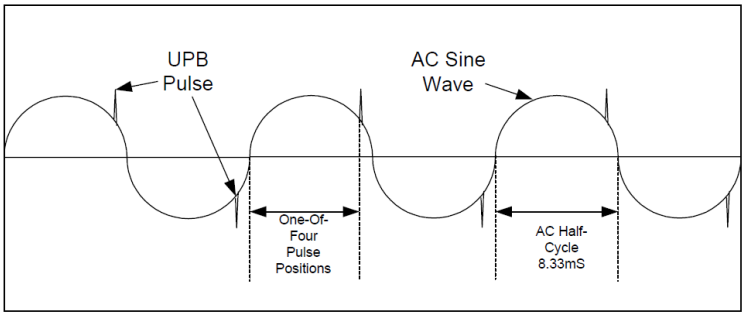

Figure 14: UPB pulse positions [26]

Checksum - The checksum is used to check the integrity of the received packet. It is computed by summing up all bytes of the packet header and the UPB message, then taking the 2's complement of that sum and truncate the result to 8 bits. The receiver just sums up all fields (including checksum) and receives 00 if the transaction worked.

Acknowledgement Frame - After the checksum the sender stops sending and the receiver has the opportunity to return an acknowledgment. The acknowledgement is a single UPB pulse at position 3 to signal the transmitter that the packet was accepted. There are two more methods of acknowledgements which can be controlled with the Packet Control Word inside the packet header.

3.4.2 Powerline

UPB uses for the data transmission single pulses. Therefore a capacitor is charged and then in a single moment released, which produces a strong peak on the line (Figure 14). This peak is said to be strong enough to be recognized even after a transformer [26]. The data itself is presented by the exact time the peak is sent. The protocol differs between 4 different positions representing 0, 1, 2 and 3. The time frame when these pulses can be sent is called the UPB frame and was placed at the end of the first halfcycle. This place was chosen because of the relatively low noise characteristics and some other attributes.

The complete UPB frame is 800 μs wide (Figure 15). Position 0, 1 and 2 are all 160 μs wide. The rest, 320 μs, is position 3. In order to receive the pulses properly they have to be accurate to ± 40 μs. Two UPB frames are one half cycle apart which is at 60 Hz 8,333 ms. Each of the 4 pulse positions can be decoded to 2 bits. With a frequency of 60 Hz, 2 UPB frames per cycle and 2 bits per UPB frames the baud rates results in 240 bits.

Further information about the UPB protocol can be found in [26].

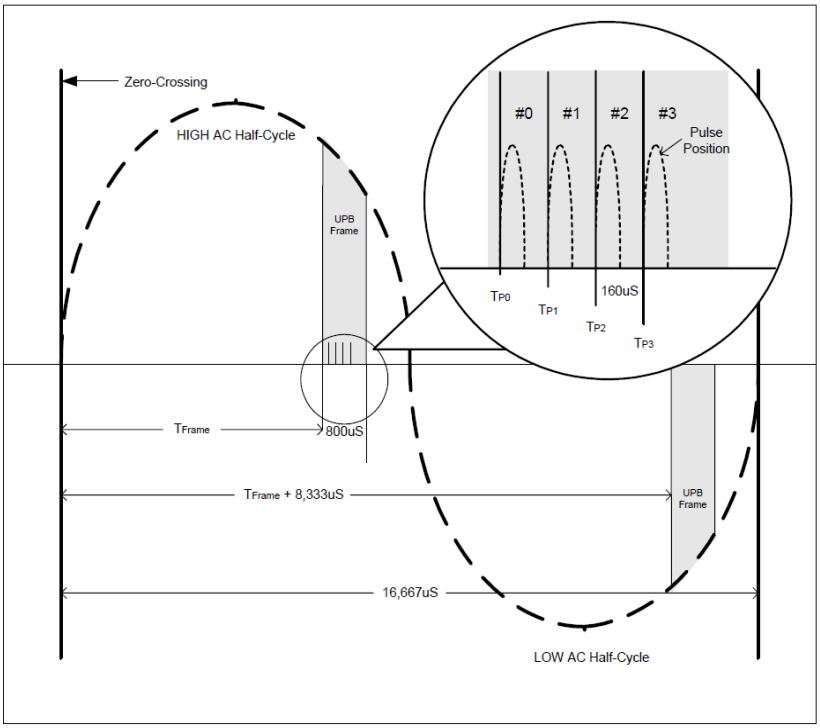

Figure 15: UPB pulse frame [26]

3.5 Industrial Powerline Communications - IPC

In 2004, after the finalisation of the UPB protocol[4], the company Powerline Control Systems (PCS) began to develop a new powerline protocol for industrial buildings. The goal was a high reliable communication system for low-speed electronic devices on the three-phased industrial power wires with very high noise and attenuation. Following [19], IPC is the most reliable communication protocol at the moment and is used with the GreenWorx Lighting Control System also from PCS.

3.5.1 Protocol

To reach the aim of increasing reliability the bandwith had to be decreased. Also some new ways to increase the signal strength and combat noise effects were developed by the engineers from PCS.

There was not much information released about how the protocol works. From the information available at [19] the communication is very similar to that of the X10 protocol.

3.5.2 Powerline

A strong low-frequency burst is superimposed on the AC signal. In difference to X10 this happens only once every cycle. This burst represents 1 bit which results in a baud rate of 60 bits per second in a 60 Hz system. The information whether the burst represents an '0' or an '1' lies in the position of the burst. If the receiver detects the burst before a certain point in the powerline cycle it interprets it as '0', if it was detected after that point as '1'.

The attenuation of the signal is claimed to be not high because of the low frequency. So the signal is able to travel extremely long distances (over 6000 metres typically). To prevent the signal from leaving the building it can be assumed that a simple low pass filter can filter the data signal. Depending on the exact frequency of the burst this is a more or less challenging task. There is also the possibility that the bursts strength can lead to troubles because a filter with a high absorption in the filter attenuation band is required for filtering.

[4]The UPB protocol was developed for HA systems and works with single strong pulses. For more information refer to Section 3.4, [26] and [25]

3.6 Consumer Electronic Bus - CEBus

The CEBus protocol is one of the oldest protocols available today. The standardisation process started in 1984 by EIA by the number IS60. After a long development phase CEBus became in 1995 a joint ANSI/EIA standard under the number EIA-600.

The CEBus standard was intentionally designed for HA systems. For that reason its main focus lies on an easy handling and expandability and not so much on robustness. Despite, it is used in BA too.

CEBus was defined for many different media like powerline (PL), coax cable (CX) and twisted pair (TP). For all the different media the packet format is the same. Bridges, that connect two different media, only have to convert the signals and do not have to remodel the message. Also the speed for all kinds of media is the same and is about 10.000 chirps (see below) per second.

In most cases a CEBus system is designed as a peer-to-peer network. That means that every node is equivalent to the other and every node can control any other node if it is capable of that task. Of course there exists the possibility of a centralised system, where one node is more special than another.

3.6.1 Protocol

The CEBus realises only four of the seven layers in the ISO/OSI reference model, in detail the Physical, Data Link, Network and Application Layer. Like in the reference model each layer adds some information to the original data.

Application Layer - This layer is responsible for the interface with the node application. It decides which information shall be sent and moves them to the NL.

Network Layer - This layer assures network-wide services. It adds an NPDU header, which reflects the desired NL services requested, and passes the frame to the DLL.

Data Link Layer - The DLL is used for reliable transmission and reception. It adds a control field, a TO address and a FROM address to the frame.

Physical Layer - It is responsible for the pure transmission over the powerline. It adds a preamble and a 16 bit CRC, the FCS, for the purpose of error correction to the frame and then transmits it over the power line.

Frame format

According to [12] the CEBus frame consists of the following parts (Figure 16):

Preamble - Each packet starts with the so called preamble, consisting of a pseudo random pattern of eight 0 or 1 symbols followed by a Preamble EOF. This field is mainly used for transmission collision detection.

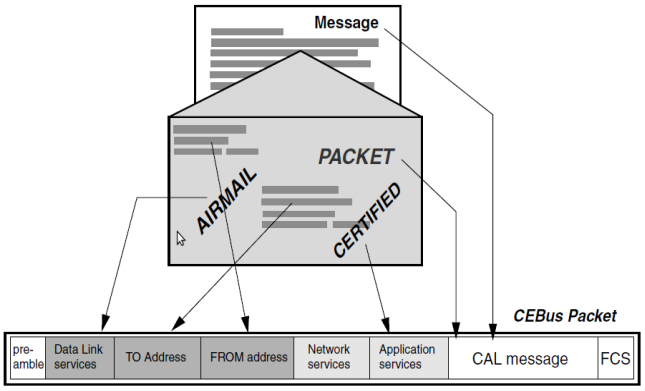

Figure 16: CEBus frame format [12]

Data Link services - Determines Data Link services like access priority and delivery priority which are handled by the Data Link layer.

TO address - In this field the address of the receiver is sent.

FROM address - Here the sender's address is transmitted.

Network services - This field determines packet routing through the network which the Network layer handles.

Application services - Through this field a reply can be requested from the receiver as well as the optional message authentication. This field is handled by the Application layer.

CAL message - This field stands for the payload which usually is about 4 to 10 bytes long. This is actually only one forth to one half of the whole packet length.

FCS - The Frame Checking Sequence at the end of the frame is used to check the message for bit errors.

Security

Because security is also an uprising subject in HA, CEBus supports two optional features, message authentication and encryption. With message authentication it is impossible for a malicious sender to generate a valid message. However the messages are sent in clear text over the line and can be read easily at any power socket. Exactly for that purpose the encryption was introduced.

As mentioned these features are optional and have to be implemented only by the devices which need a certain level of security.

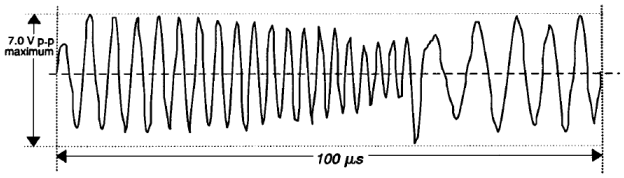

Figure 17: CEBus signal [12]

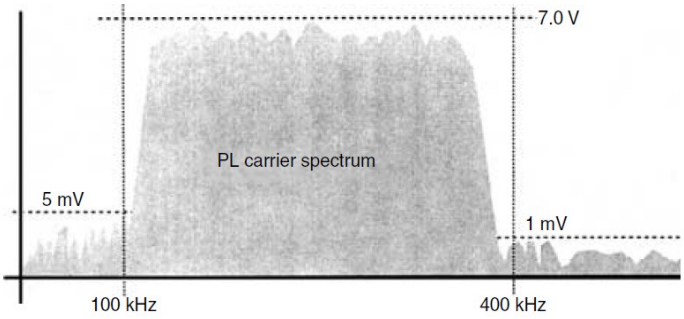

Figure 18: CEBus signal spectrum [12]

3.6.2 Powerline

The CEBus protocol uses Spread Spectrum Carrier (SSC) modulation for the powerline communication. The intention was to distribute the signal over a wider range of frequencies and to make it resistant against noise and jamming. For the US market the frequencies from 100kHz to 400kHz are used. These frequencies violate the CENELEC 50065 standard. Because of that CEBus system cannot be installed in Europe.

For data transmission so called 'chirps' are sent. A 'chirp' is a signal that sweeps through the frequencies. For the CEBus standard the signal starts at 200 kHz and runs through to 400 kHz. Then it jumps back to 100 kHz and sweeps to 200 kHz. The signal can be seen in Figure 17. This special form was chosen because of many reasons, e.g. to minimize AM radiation.

The chirps are produced by reading 360 standardised digital values and converting them through a DAC and a low pass filter to the wanted signal. Through the special form of the signal it is possible to spread it over the whole frequency range from 100 kHz to 400kHz with only little disturbance in the lower and higher frequency bands (Figure 18).

Two states are defined on the powerline, a SUPERIOR and an INFERIOR. As the names indicates the SUPERIOR state dominates the INFERIOR. The SUPERIOR state is always represented by a chirp sent. The INFERIOR state differs depending on when it appears. In the preamble it is defined as the absence of the signal, in the data signal as the inverted SUPERIOR state, meaning the chirp in phase shifted by 180 degrees. This has to be done to have the carrier on all the time and so keep the receiver 'locked' to each UST (see below) to still

symbol	description	duration	length in USTs
'1'	symbol 1 on the data line	100 μs	1
'0'	symbol 0 on the data line	200 μs	2
EOF	"end-of-field"	300 μs	3
EOP	"end-of-packet"	400 μs	4

Table 2: CEBus symbols and timing

be able to distinct between SUPERIOR and INFERIOR states.

As described above chirps are used for data transmission. A chirp is always 100 μs long, which is defined as the Unit Symbol Time (UST). An exception from that rule is the preamble (see below). To mark the end of a symbol and the start of the next symbol alternating states are used, meaning that the first symbol is sent in SUPERIOR state, the second in INFERIOR state, the third in SUPERIOR state again and so on. The different symbols itself are thereby encoded by the time, or more precise by the number of chirps, the system stays in one state. To decode the data the receiver only has to measure the time from on state change to the next and then look up the symbol in Table 2.

To give an example the preamble field is described a little closer. Due to the fact that the idle state of the line is the INFERIOR state the first symbol is always sent in the SUPERIOR state. The eight preamble bits are then sent in alternating states. At the end the Preamble EOF, that consists of eight SUPERIOR 1 symbols, is attached. For a better distinction between preamble and data symbols, each chirp in the preamble is 114 μs instead of 100 μs long.

Four different symbols were defined for the CEBus protocol. They can be seen in Table 2. Symbol '1' only takes half the time to send as the symbol '0'. Therefore, CEBus coder try to translate the data into codewords with as many '1' as possible. Because of that fact the baud rate depends on what data are sent.

The two additional symbols in Table 2 are EOF and EOP. The end-of-field (EOF) symbol is sent after each field in a frame. This is very important for optimisation methods like leading zero suppression. The end-of-packet (EOP) symbol is sent only at the end of a whole frame. It marks the end and is the signal for waiting senders to start their bus access protocol.

Bus access is obtained by a Carrier Sense Multiple Access / Collision Detection and Collision Resolution (CSMA/CDCR) protocol. Here the sender first listens to the line. If it is idle for a specific amount of time the sender starts to transmit. If it now determines a collision it steps back and waits till the line is free again. Collision detection is realized with SUPERIOR and INFERIOR states. The SUPERIOR state overrules the INFERIOR state. So a sender that puts an INFERIOR signal on the line and reads a SUPERIOR state back knows, that another node tries to send in parallel and backs off. Because the sequence in the preamble is pseudo random it is probable that a collision is detected within the first eight bits of a transmission.

To decrease collision probability different concepts have been introduced.

Priority - Three different priority levels were introduced to determine the time the sender has to wait before it can send its telegram after the last EOP.

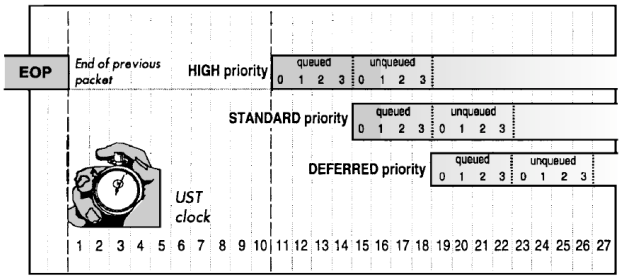

Figure 19: CEBus bus access [12]

With HIGH priority this duration is 10 UST, with STANDARD 14 and with DEFERRED 18.

Random start delay - Randomisation is done in many ways with the CEBus protocol. For example, a random number from 0 to 3 is added to the earliest UST when a sender is allowed to transmit. This reduces the chance that two senders with the same priority start an attempt at the same instant.

Priority and random start delay can be seen in Figure 19. Some more techniques with a more detailed description as well as further details on the CEBus protocol can be found in [12].

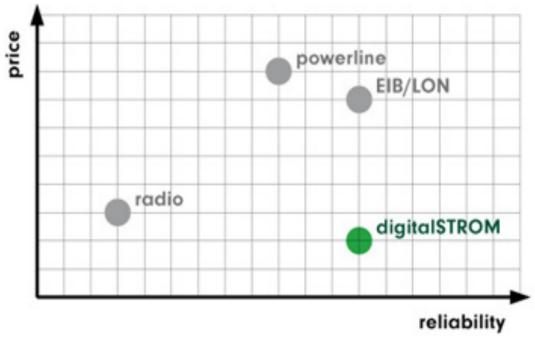

Figure 20: reliability of digitalSTROM [2]

3.7 digitalSTROM

digitalSTROM is a very young technology. First parts have been introduced at the end of April 2011. Depending on [3], the system shall be cheaper than radio, powerline and KNX/LON and as reliable as KNX/LON (Figure 20). Further details are available at [2] and [3].

3.7.1 Protocol

Here the basic parts of a digitalSTROM system are introduced. How they work together is described later in this section.

dSID - digitalSTROM identifier: Is a unique 96 bit number like the MAC address. With this number each device can be clearly identified. The dSID is stored on the digitalSTROM-chip.

dSM - digitalSTROM-Meter: Per electric circuit one dSM has to be installed. The dSM has to be mounted in a fuse box and receives and transmits messages to and from the digitalSTROM-chip (in detail the dSID) over the powerline cables. There can be at most 1008 different dSID per dSM. dSMs are able to communicate with each other and with a dSS with a specific dS485 protocol. In one system at most 62 dSM are allowed, which leads to an amount of 62496 dSIDs. dSM are also capable of measuring the power consumption of their electric circuit.

dSS - digitalSTROM-Server: The dSS is also mounted in the fuse box and is used to combine several dSM to one system. A dSS is optional allowing to fulfill complex operations over several different electric circuits. This is achieved with an open source software called digitalSTROM-Konfigurator. With that configurator it is possible to set e.g. different lighting schemes over the web interface of the dSS. Furthermore the dSS can be connected to the LAN and can then be accessed from the Internet. It is even possible that the dSS automatically sends power information to the power supplier for accounting.

dSF - digitalSTROM-Filter: The dSF alters the power signal, so that a digitalSTROM communication is possible over the powerline.

dS485: This protocol is used for the communication between dSM - dSM and dSM - dSS. It is based on the RS/TIA485.

digitalSTROM-Klemme: The digitalSTROM-Klemme is a lustre terminal with a built in dSID. It is used for devices which are not yet ready for digitalSTROM communication. Therefore it is installed right before the device on the power cable. The chip in the lustre terminal receives the commands from the dSM and then sets the current accordingly.

digitalSTROM-Tasterklemme: This device is mounted behind a switch and sends the status of the switch to the dSM.

System integration

The digitalSTROM protocol works with a master-slave workflow. Each electric circuit is one encapsulated master/slave region in which the dSM is the master and the dSIDs and digitalSTROM-Tasterklemme are the slaves. The communication here is realised over the powerline with the digitalSTROM-protocol. If the digitalSTROM-Tasterklemme registers a movement of the switch, it sends a telegram to the dSM. The dSM calculates what has to be done and sends the command, e.g. 'switch lights on' in broadcast style on the powerline. All dSIDs check if they have to take action and then do the action that was configured.

A small example shall illustrate that. It is possible to configure different light schemes. Let's assume you activate scheme 2 with two presses on the light switch. When you press the switch two times, the digitSTROM-Tasterklemme sends that to the dSM. The dSM knows that scheme 2 is desired when the switch is pressed twice and sends the command 'activate scheme 2'. Each dSID receives that message and looks up what it has to do at that specific scheme and controls its object accordingly. That is the reason why it is very easy to move objects between different electrical circuits.

digitalSTROM parts can be implemented with many different devices like light, video, .. and each of them are specialised for that special functionality. To make the distinction of parts from different areas of application more clearly a color scheme is used (Figure 21). The basic function are predefined e.g. for light devices on/off. This supports plug and play installation. If you connect a new device to the powerline it can be used immediately. Of course you have to do some configuration if you want that device to play a specific role in a specific scheme but e.g. to switch off all lights in the room just connecting is enough.

The dSM can be connected with each other and a dSS too. So it is possible that the dSS controls many different power circuits at the same time. Therefore the dSM communicates with the dSS via the dS485 protocol. The dSM receives the commands from the dSS. Then the flow of information to the dSID is the same as in the example above. For the dSM it makes no difference if it receives the commands from the digitSTROM-Tasterklemme or from the dSS.

Farbe	Gruppe	Beispiele
Gelb	Licht	Decken-, Wand- und Stehleuchten
Grau	Schatten	Jalousien, Rollladen, Sichtschutz
Blau	Klima	Heizung, Lüftung, Klima
Cyan	Audio	Radio, CD-Player
Magenta	Video	Fernseher, Projektor, DVD-Player
Rot	Sicherheit	Schutzfunktionen, Brand- und Einbruchsmelder
Grün	Zugang	Klingel, Türöffner
Weiss	Custom	Kochherd, Waschmaschine, Kühlschrank
Schwarz	Joker	Zur freien Verwendung

Figure 21: color scheme in digitalSTROM [1]

Security

According to [3] the digitalSTROM system is completely tap-proof. As a reason the fact that the data transmission is encapsulated to single energy circuits is mentioned. It is also pointed out, that the decision to patent the transmission method and keep it just for members of the digitalSTROM alliance is based on security reasons (security by obscurity).

3.7.2 Powerline

digitalSTROM uses a method different from that of other protocols. Not much information was released about how this protocol works because it is patent restricted and only members of the *digitalSTROM.org* have access to a closer description. In [4], [3] and [2] the procedure is described the following: The sender switches the current on and off several times when the alternating current is close to a zero point. There is no high frequency modulation like it is used with other protocol. For that reason it shall be possible to drive digitalSTROM beside some of the above mentioned protocols.

4 Solutions on the market

4.1 Comparison

After we looked at each protocol in detail we now want to compare the different protocols to one another. The following table shows a comparison of the most important characteristics.

protocol	**filtering**	**modulation scheme**	**access protocol**	**address range**	**speed (bit/sec)**
LonTalk	easy	many	p-persistant CSMA	many	up to 10k
KNX	easy	BFSK	time divided	32768	1200
X10	easy	short 120 kHz pulses	CSMA/CA	256	60
UPB	hard	strong spikes	n.A.	64000	240
IPC	easy	short pulses	n.A.	n.A.	60
CEBus	medium	SSC	CSMA/CDCR	many	10k chirps
digitalSTROM	easy	current on/off switching	n.A.	62496	n.A.

4.2 Market analysis

After this listing of different protocols in detail we now want to investigate what system and devices are currently available on the market for each protocol.

4.2.1 LonTalk

LonTalk was designed completely medium independent. This means that every medium is supported as long as the used transmitter and receiver fulfill the requirements defined by the Neuron Chip. That is the reason why transmission methods, which differ in speed, signal form and used frequency bands, can be used with the same protocol. Only transmitter and receiver have to be developed for each technology, which makes LonTalk extremely flexible and adjustable. This is one of the reasons why LonTalk can be and is used all around the world.

With LonTalk the main distributor is the Echelon Corporation. On their website a huge range of products is presented. Beginning from the Smart Transceivers 3120/50/70, Neuron Chips, Routers and FPGAs over utility products like for example software tools to complete building automation solutions. In the case of solutions there are many different alternatives available, like for example lighting control or building energy management, that are optimised for the required needs.

4.2.2 KNX powernet

The KNX powernet standard uses SFSK, a rather simple method, as modulation scheme. In order to receive the sent signal properly a special reception method was develop, called matched filter optimum receiver. This method ensures correct reception even with high noise.

Due to the fact that the communication is realised by only two different frequencies, a simple band stop is enough to filter the KNX signal from the powerline.

Powernet is mainly distributed by the Busch-Jaeger company. In their portfolio there are not only transceivers but also high integrated devices like room temperature regulators and clock timers. The single devices can be ordered in many different colors and forms to fit in every building. Complete systems can be ordered at certain electricians, which can be found on the Busch-Jaeger homepage.

4.2.3 X10

To handle transmission problems many methods have been introduced in the X10 standard such as replicated sending or inverted bit sending. This indicates that this method of transmission is not very stable. Each signal in the 120 kHz frequency band can disturb the communication. Unfortunately many devices generate high frequency signals from time to time. So even simple machines in a building can disturb the X10 communication. On noisy lines a communication can even become impossible and so another standard shall be chosen.

By transmitting only 1 bit per cycle the baud rate is limited to 60 bit (in a 60 Hz system). A single simple command has 47 bits. So it takes about one second before the desired action is really executed. This can be way too long for some tasks e.g. light switches. X10 is therefore not suited for situations, where timing is of importance. Nevertheless X10 was a precursor in the area of powerline communications and was chosen as the base for many powerline protocols that followed X10.

Despite the fact that the X10 protocol is rather old by now, there are still products available at the market. In many online stores like Amazon different devices like remote controls and lamp control modules can be bought. This products are mainly produced by the X-10 Powerhouse company.

4.2.4 UPB

According to [25], the UPB protocol can be used besides any other PLC system and does not disturb others or gets disturbed by them. This is possible due to the unique transmission method used with UPB.

This main advantage is also its main disadvantage. Based on the fact that the pulses sent cannot be filtered properly and they also are still present after a power transformer it has to be taken care, that each building at one power transformer has a different Network ID. If two buildings share one ID, intentionally or unintentionally, it is possible to control one building with the automation system of the other one. This is a very serious problem because it represents a huge security risk. It is not only about the fact that the data sent can be read easily. It would be even possible to control all parts of the building from the outside, allowing, for instance, intruders to disarm the security systems.

On the web different devices like button controller or lamp modules can be ordered. Even complete applications like, for instance, fan control or fish tank

control are available. A distributor for the American market would be for instance Web Mountain Technologies [36].

4.2.5 IPC

IPC was developed to serve in industrial plants with a lot of disturbance and noise on the powerline. For that reason the whole protocol was built as robust as possible to withstand even a high amount of noise.

The company PCS uses its protocol IPC in the GreenWorx™ System. This is a Lighting Control System that, corresponding to [24], is the "first fixture-level lighting system that uses building's existing power wiring for two-way communication". This means that every single device can be controlled individually instead of only whole power strings. Unfortunately there was no option available to order this system or just devices over the web page. Also from other companies this system was not sold.

4.2.6 CEBus

The CEBus standard uses a specific kind of transmission method, which distributes the signal over the whole frequency band. This method, which is mainly used by the military, makes the signal very resistant against jamming. Due to that fact filtering the CEBus signals is a challenging task because a wide frequency range has to be filtered.

On the market CEBus products are not so present as others. On the web only a few distributors can be found, but their sites are outdated or have no option to order the parts. However, the portfolio reaches from simple integrated circuits like transmitters to complete modules, which only have to be plugged into a power socket.

4.2.7 digitalSTROM

digitalSTROM is not only thought as a data communication system but also as power metering and power saving system. In accordance with [2] the digitalSTROM-chip shall reduce the power consumption of a device below 0.3 Watt. The system is also able to detect high power consumption of a device e.g. the fridge and then informs the user to check the device. Both the dSM and the digitalSTROM-chip can detect high current consumption. Of course the dSM only recognises a failure but cannot determine exactly which device it is. Only the digitalSTROM-chip can announce which device really acts malicious.

Another area of application is the intelligent usage of current. The power prices are by law published at the beginning of a day. So the system can use more current when it's cheap e.g. for cooling the fridge or the washing machine and reduce the power consumption when the power price is high. The energy suppliers also planned to use this system to control and smooth peak load situations. So it could be possible to activate washing machines only at night when the overall power consumption is low.

One downside of the protocol is, that parts with an inductive or capacitive resistance cannot be used because the current has to be changed immediately to

transmit correctly. This means that not all devices are capable to be installed in a digitalSTROM network.

There is also some extra space in the fuse box needed. For each electric circuit you have to install a dSM (90 x 17,5 x 70 mm) and a dSF (90 x 35 x 70 mm). The optional dSS (90 x 17,5 x 70 mm) also needs extra space if installed. In large systems this extra space can reach tremendous dimensions.

Depending on the information at [2] (July 2011) it is already possible to order the digitalSTROM system from some specific electricians in Germany and Switzerland. A detailed list can be found at [2]. For trained electricians it is possible to buy the parts at an electrical distributor. It is not described if individual parts are sold to private users too.

5 Conclusion

Building Automation as a whole is becoming more and more important these days. Increasing energy prices, make buildings, which reduce energy consumption automatically, necessary because they can save a lot of money. Also safety and security is an uprising subject, which can be handled very easily and elegantly with a BA system.

As we have seen the usage of the power line cables for communication brings some advantages and disadvantages. As shown above there are different protocols available which have overcome the problems on the cables and can provide a reliable communication. The protocols used in this area of application are built for robustness and so communicate with low speed, which completely satisfies the needs in BA. Of course the presented protocols are not the only ones available. There exist protocols, especially for the HA sector, exist, that ensure a bandwith of 200 MBit/s and more (e.g. HomePlug AV, HomePlug AV2, Gigle). This is needed for multimedia tasks like streaming video or sound over the network. So the list of protocols presented here is not even close to complete, but it gives a short overview of how data can be sent over the powerline and their advantages and disadvantages.

An issue with powerline systems which will grow more important in the future is security. Due to the fact that the powerline network does not end at a building border it is necessary to avoid the insertion of and accordingly the leaking out of information. Otherwise this would be a big security risk and might lead to incalculable consequences.

6 Glossary

BA: Building Automation
CA: Collision Avoidance
CD: Collision Detection
CSMA: Carrier Sense Multiple Access
DLL: Data Link Layer
HA: Home Automation
HVAC: Heating, Ventilation and Air Cooling
NL: Network Layer
PDU: Protocol Data Unit
PL: Physical Layer
PLC: Powerline Communication
SSC: Spread Spectrum Carrier
TP: Twisted Pair
UST: Unit Symbol Time

References

[1] aizo ag. *digitalSTROM Installationshandbuch*, 201.

[2] digitalSTROM Alliance, `www.digitalstrom.org`.

[3] aizo ag Schweiz, `www.aizo.com`.

[4] Patent wo 2006/034866 a1, 04 2006.

[5] Klaus Dostert. *powerline communications*. Prentice Hall PTR, 2001. pp. 92-107.

[6] Klaus Dostert. *powerline communications*. Prentice Hall PTR, 2001. pp 73-76.

[7] Klaus Dostert. *powerline communications*. Prentice Hall PTR, 2001. pp 5-31.

[8] Klaus Dostert. *powerline communications*. Prentice Hall PTR, 2001. pp 32-41.

[9] Echelon® Corporation. *LonTalk® Protocol Specification*, 3.0 edition, 1989-1994. pp. 12-16.

[10] Echelon® Corporation. *LonTalk® Protocol Specification*, 3.0 edition, 1989-1994. pp. 12-16.

[11] Echelon® Corporation. *LonTalk® Protocol Specification*, 3.0 edition, 1989-1994. pp. 20-28.

[12] Grayson Evans. *CEBus Demystified, The ANSI/EIA 600 User's Guide*. The McGraw-Hill Companies, Inc., 2001.

[13] Mag. Dipl.-Ing. Wolfgang Granzer. *Secure Communication in Home and Building Automation Systems*. PhD thesis, Technische Universität Wien, 2 2010. pp. 1-4.

[14] Mag. Dipl.-Ing. Wolfgang Granzer. *Secure Communication in Home and Building Automation Systems*. PhD thesis, Technische Universität Wien, 2 2010. p. 13.

[15] Mag. Dipl.-Ing. Wolfgang Granzer. *Secure Communication in Home and Building Automation Systems*. PhD thesis, Technische Universität Wien, 2 2010. pp. 43-46.

[16] Mag. Dipl.-Ing. Wolfgang Granzer. *Secure Communication in Home and Building Automation Systems*. PhD thesis, Technische Universität Wien, 2 2010.

[17] Werner Harke. *Smart (Home) Control*. C.F. Müller Verlag, 2007. p. 7.

[18] Werner Harke. *Smart (Home) Control*. C.F. Müller Verlag, 2007. p. 8.

[19] Powerline Control Systems, `http://pcslighting.com/greenworx/IPC_Technology.php`.

[20] Franz Kammerl, Heinz Lux, Bernd Schade, and Arno Valerius. *Gebäudesystemtechnik mit EIB*. Publicis MCD Verlag, 2001. pp. 27-28.

[21] Franz Kammerl, Heinz Lux, Bernd Schade, and Arno Valerius. *Gebäudesystemtechnik mit EIB*. Publicis MCD Verlag, 2001. p. 29.

[22] LONMARK International. *LONMARK® Layer 1-6 Interoperability Guidelines*, 3.4 edition, September 2005. pp. 9-34.

[23] Elena Mainardi and Marcello Bonfè. Powerline communication in home-building automation systems. Engineering Department, University of Ferrara, pp. 1-2.

[24] Powerline Control Systems, `http://pcslighting.com/greenworx/index.php`.

[25] Powerline Control Systems. *Universal Powerline Bus Communication Technology Overview*, 08 2002.

[26] Powerline Control Systems. *UPB Technology Description*, 1.4 edition, 04 2007.

[27] Christian Reichel. Home automation sytems based on powerline communication. Master's thesis, TU Wien, 2003. pp. 14-21.

[28] Christian Reichel. Home automation sytems based on powerline communication. Master's thesis, TU Wien, 2003. pp. 3-11.

[29] Christian Reichel. Home automation sytems based on powerline communication. Master's thesis, TU Wien, 2003. p 12.

[30] Rainer Rosch, Klaus Dostert, Klaus Lehmann, and Robert Zapp. *Gebäudesystemtechnik*. Verl. Moderne Industrie, 1998. pp. 28-31.

[31] Rainer Rosch, Klaus Dostert, Klaus Lehmann, and Robert Zapp. *Gebäudesystemtechnik*. Verl. Moderne Industrie, 1998. pp. 25-27.

[32] Thilo Sauter, Dietmar Dietrich, and Wolfgang Kastner. *EIB Installation Bus System*. PUBLICIS, 2001. pp. 166-167.

[33] TOSHIBA CORPORATION, Semiconductor Company. *Neuron® Chip, TMPN3150/3120*, 2006. pp. 97-107.

[34] Jens Uetrecht. *Das vernetzte Haus*. Franzis Verlag, 2000. pp. 318-320.

[35] Jens Uetrecht. *Das vernetzte Haus*. Franzis Verlag, 2000. pp. 325-331.

[36] Web Mountain Technologies, `http://www.webmtn.com/products/products.php?cat=UPB`.

[37] Hermann Wellers. *Gebäudesystemtechnik*. Cornelsen Girardet, 1995.

[38] X-10 PRO. *X-10 Communications Protocol and Power Line Interface PSC04 & PSC05*, 2.4 edition. pp. 1-4.