HI-SMART

HI-SMART: HIGHER EDUCATION PACKAGE FOR NEARLY ZERO ENERGY AND SMART BUILDING DESIGN

MODULE #5

CHAPTERS 1-5: SMART CONTROL AND AUTOMATION

Co-funded by the Erasmus+ Programme of the European Union

MŰEGYETEM 1782 · STU SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA · TECHNISCHE UNIVERSITÄT KAISERSLAUTERN · ENERGIAKLUB CLIMATE POLICY INSTITUTE APPLIED COMMUNICATIONS

SMART BUILDINGS

1.1 BUILDING AUTOMATION

In our modern industrial society, more and more procedures and processes are being automated. The degree of automation in residential and functional buildings is also constantly increasing worldwide because residents and operators want more and more comfort, safety and economy.

In this context, building automation has developed into an important sub-area of automation technology and offers customer-oriented solutions for all types of buildings.

A distinction is made between building automation for residential and functional buildings and "smart home" systems for private users.

Building automation (GA) refers to the automatic control and regulation of building functions, such as heating, air conditioning and ventilation as well as lighting and shading.

As an important component of technical facility management, building automation aims to save energy costs and operating expenses, to perform functional sequences automatically and according to predefined setting values (parameters) across all trades, and to simplify their operation and monitoring.

For this purpose, all sensors, actuators, control elements, consumers and other technical units in the building are networked with each other. Processes can be combined in scenarios and enable an intelligent and optimized interaction of the various components.

Building automation is often confused with smart home systems. Especially in recent years, the number of smart home systems for private users has grown rapidly.

This can be attributed on the one hand to the ever lower prices and to the well-known manufacturers such as Apple, Amazon, Bosch etc., who have seen strong growth opportunities in the market.

In more and more households, speech assistants are being used, with which not only music is played or information is retrieved from the Internet, but also "smart" components such as radiator thermostats or lights can be controlled.

Accordingly, these are technical systems and procedures for living spaces and houses, which are intended to improve the quality of life, safety and more efficient use of energy on the base of networked and remotely controllable devices.

In addition to the networking of building services (e.g. lighting, shading, heating), the networking of consumer electronics (e.g. smart TV, music system) and household equipment (e.g. refrigerator, washing machine) is also part of smart home.

The entry into the smart home world is usually made possible by simple, radio-based systems, which are relatively easy to install, even by non-experts.

But these systems often have two disadvantages:

- They are cloud-based. That means that the software that drives the devices runs on a vendor's server and you need to connect your devices to that server. But what happens if the server is no longer accessible? (Example: https://www.heise.de/newsticker/meldung/Smarter-Tueroeffner-Nello-Ab-18-Oktober-ohne-Funktion-4545084.html)
- The systems (not all of them) often have poor interoperability with systems from other manufacturers. Therefore system A cannot communicate with system B. This means you are bound to one manufacturer.

Despite these disadvantages, there is also an important advantage. The internet is full of help and a large community and maker scene has developed in the smart home area.

But what is the difference to building automation?

Building automation also connects building technology (e.g. lighting, shading, heating), but not consumer electronics and household equipment.

There are therefore intersections that affect the networking technology.

However, the connection and networking in BA takes place via standardized systems and interfaces. Thus, there is a good interoperability of different systems and manufacturers.

The BA is also easily expandable, either by sharing existing cabling or by radio systems.

As in the smart home area, there is a strong growth market in the BA area with well-known manufacturers such as Siemens, Sauter, Johnson Controls, Wago etc.

DEFINITIONS

When we deal with building automation, we cannot avoid the most important standards.

One of the most important standards at European level is the EN ISO 16484. It is split into 6 parts:

- Part 1: Project specification and implementation
- Part 2: Hardware
- Part 3: Functions
- Part 4: Applications (under preparation)
- Part 5: Data communication protocol
- Part 6: Data communication conformance testing

According to EN ISO 16484, the definition of building automation is as follows:

"description for products, software, and engineering services for automatic controls, monitoring and optimization, human intervention, and management to achieve energy — efficient, economical, and safe operation of building services equipment

Note 1 to entry: The trade designation and the industry branch are also referred to as building automation and/or building control." [EN ISO 16484-2; October 2004]

DIN EN ISO 16484 cannot cover all regional issues. In Germany this is taken over by the VDI guideline series 3814

This guideline applies to:

- Automation of buildings and real estate portfolios
- Trades (is partially) whose functionality is achieved by building automation
- Facility management, if BAC functions are used for operation
- Temporally over the entire phases in the life cycle of a building, especially for conception, planning, construction, operation and use
- Application by all natural and legal entities that concert by BAC

Although a guideline is not a standard, it is a recognized rule of technology and must generally be observed. In the event of damage, experts often base their assessment of liability on whether the guidelines have been observed.

In 2019, the Directive 3814 was completely revised and is structured as follows:

<u>Sheet 1: Basics</u>

Sheet 1 presents the basics for understanding building automation, explains terms and addresses the topics of the following sheets.

<u>Sheet 2: Planning</u>

Sheet 2.1 "Planning; Requirement planning, operator concept and specification sheet" enables a complete description of the construction task with regard to building automation.

Sheet 2.2 "Planning; planning contents, system integration and interfaces" provides assistance for the planning process.

Sheet 2.3 "Planning; Operating Concept and User Interfaces" the planning of the human-machine interface to building automation is described.

Sheet 3: Functions and macros

The new version of Sheet 3 offers a modular system of functions and function macros for the description and representation of automation tasks in rooms (room automation functions) and systems (system automation functions), supplemented by management functions. It also contains the description and representation forms of the functions for building automation. The sheet 3 is divided into:

Sheet 3.1 GA functions, automation functions

Sheet 3.2 Macro functions (draft expected in 2020, currently in VDI3813)

Sheet 4: Methods and tools for planning, execution and handover

Sheet 4.1 presents working tools and methods with which a complete and clear description of addressing systems and component lists for building automation in different planning phases is possible.

Sheet 4.2 presents working tools and methods with which a complete and unambiguous description of the requirements of the building owner for building automation in different planning phases is possible

The aim of the guideline VDI 3814 part 4.3 (draft expected in 2020) is to present working tools and methods with which a complete and unambiguous description of automation tasks for building automation in different planning phases is possible.

Sheet 5: Energy efficiency (draft expected in 2020)

Functions (e.g. energy management functions) will be introduced, with which energy efficiency through building automation can also be functionally represented in relation to EN 15232 and IEC 60364-8-1.

Sheet 6: Qualification of persons (draft expected in 2020)

Describes competence profiles for different roles of persons (e.g. BA specialist planner, project manager, programmer, FM service provider). The working tools of the guideline series VDI 3814 part 4 are to be conveyed to the required extent.

OBJECTIVES AND DISCIPLINES OF THE BA

Different goals can be pursued and combined with the BA.

Examples:

- Reduction of energy consumption through intelligent control.
- Controlling heating, ventilation or air conditioning systems according to demand and time.
- Switch or dim lighting according to demand, time of day or season and movement, even from several individual channels simultaneously in the form of light scenes.
- Control shading devices depending on sunlight and wind in time and according to demand.
- Recording of consumption data from heat meters, water meters, gas meters and electricity meters.
- Gain in convenience through intelligent control: for example, a predefined lighting situation can be created at the touch of a button without having to switch or dim several lamps individually - or alternatively, defined actions can be triggered by logical links of switching states.
- Load control on the basis of consumption data acquisition by sequentially switching on lights.
- Central recording and display of all control processes in the building.
- Security through alarms when critical situations occur.

TRADES IN BUILDING AUTOMATION

The technical building equipment includes a large number of systems that are required for the operation of the building. Among the most important operational technical systems are those for the supply of heat, cold, fresh air, water and electrical energy.

In addition, there are also facilities for waste disposal, e.g. lifting units for waste water. Depending on which tradesmen install these plants, the plants are assigned to a certain trade.

The trade is referred to as craftsman's work or construction work. Classical trades are e.g. bricklaying, plumbing or electrical work.

Since today's functional processes are to be carried out automatically in terms of economic efficiency, regulation and control modules are necessary.

For some of the trades, the supplier provides the modules required for building automation. He is then responsible for the measurement and control technology of these trades.

These are primarily heating, cooling and ventilation systems, which are often referred to as HVAC systems.

In any case, it is particularly important during the execution of the project that the interface between the operational systems of the individual trades is precisely described in terms of both data technology and logistics.

Building automation combines all trades in terms of information technology and thus enables central monitoring.

THE BAC SYSTEM

The technical implementation of the building automation is done with Building automation and control systems (BACS).

The BAC functions of the BAC system are produced via software that is either adapted to a process (configured, parameterized) or individually produced (programmed) for a process. This software can be implemented in different hardware.

The necessary exchange of information of the components of a BAC system (information flow) is done via the BAC system network.

There will usually be interfaces to a BAC system, through which a dialogue between the BAC system and the human being (operating and monitoring) takes place.

There may also be interfaces between a BAC system and other systems, through which a dialog between the systems takes place in an interoperable manner.

The system aitomation and room automation must be coordinated with management and control equipment (MCE) to ensure complete functionality of the building automation.

For example, systems must provide exactly the amount of energy that is needed in the rooms. This requires the necessary interoperability between systems, rooms and MCE.

"BACSs, which are able to control and monitor building service systems and devices via building management systems are some of the most important FM tools.

"BACSs are particularly important for building management in the “operation and use” life cycle phase, in particular for the sustainable (automated) operation of buildings in the context of TBM." (VDI, 2019)

Structural classification in:

- System automation and controls (SAC)
- Room automation and controls (RAC)
- Management BACS (M-BACS)

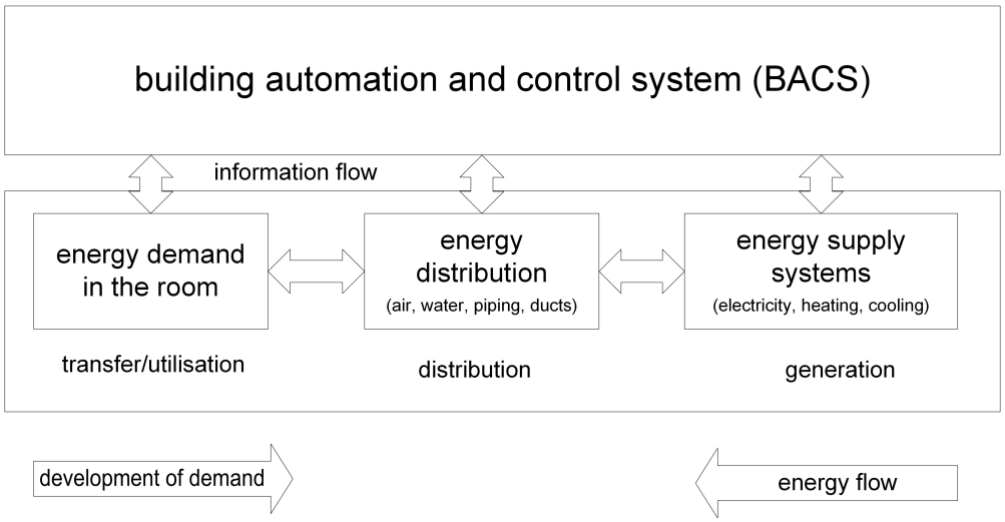

Figure 1: Structure of the BAC system

System automation and controls (SAC) is the automation of systems including local operating and display components in buildings.

Systems are, for example, central ventilation, air conditioning, refrigeration or heat generation systems or security systems such as those installed in technical centers in buildings.

Room automation and control (RAC) refers to the automation of rooms in buildings, including local operating and display components.

BA management is the part of the BACS that performs the tasks required to process information for management.

Examples are functions to support higher-level energy management, maintenance management, cleaning management, fault management, room booking and room

administration management.

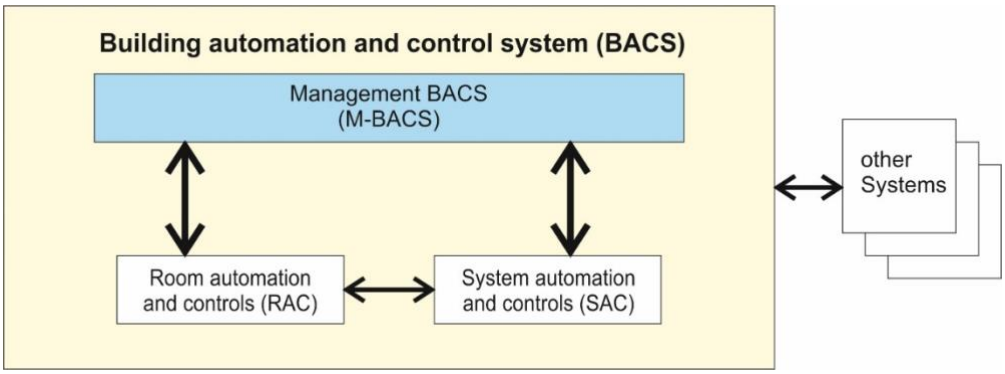

Figure 2: simple structure of the BACS (VDI, 2019)

The Figure 2 shows the simple structure of the BA system

The arrows represent the interfaces and communication channels.

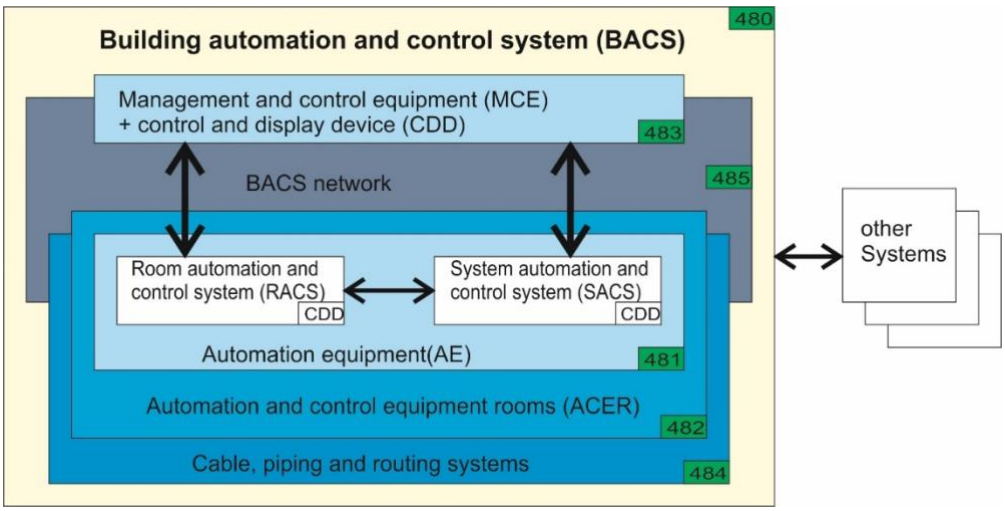

Figure 3: Cost structure of the BACS according to DIN 267 (VDI, 2019)

The Figure 3 shows the facilities and cost structure of the BACS according to DIN 267.

With the DIN 276 of 1993, building automation was introduced as an official trade in the construction industry. This was followed by special standards and the VOB/C [DIN 18386] as "General Technical Contract Conditions" and the standard performance book 070 for BA.

The increasing importance of room automation within building automation, especially for non-residential buildings, has been met by DIN 276 - "Costs in the building industry" since 2006 by reorganizing the cost groups.

In addition to the original meaning for cost estimation and accounting, the picture also shows the communicative relationships of the subsystems with each other.

While the communication between room automation and system automation is mainly for the demand-driven control of the energy generators, the interfaces of both automation systems to the management system are mainly for visualization, operation or trend recording.

DIN 276 provides specifications for cost determination in building construction and is divided into the following cost groups:

- 100 Land plot
- 200 Preparation and development
- 300 Building - Building construction
- 400 Building - technical installations
- 500 outdoor facilities
- 600 furnishings and works of art
- 700 Ancillary building costs

Building automation is classified in cost group 480.

Sustainable buildings can only be built if they are designed, planned and constructed using suitable methods.

An essential basis for the efficient use of BAC is a segmentation (modularization) of the building, which makes it possible to reduce investment costs for buildings, since in particular industrial manufacturing processes can be used for the technical building equipment systems (TBES) and the software of BAC can be duplicated cost-effectively.

This also creates the prerequisites for high flexibility and thus for simple conversions/conversions, which can be carried out cost-effectively, quickly and with little disruption by restructuring the segments. In this way, they lead to operational optimization and to a reduction of utilization costs.

Segmentation is achieved by structuring the building into identical or similar segments and equipping these with the same TBES. This can be easily implemented if, for example, an orientation is made to the axis grid of the supporting structure and this is coordinated with the requirements of the TBES and the BACS in the course of an integration planning.

Starting with the initial planning up to the ongoing operational management, buildings should therefore be divided into individual functional building parts. On the one hand, these are actually spatially separated building parts (e.g. single room, corridor, floor, technical center), on the other hand, however, they are function- or structure-forming building parts (e.g. area or zone in an open-plan office, supply area of a ventilation system).

However, the terms for building parts (e.g. zone, area) are not clearly defined, which means that they are used in practice in different contexts and with different interpretations. A functional description of RA is of crucial importance, because a "room" interacts with other parts of a building, is contained in other parts of a building or is combined to form a larger building part.

The picture in the slide illustrates this consideration in the form of a shell model. Rooms can consist of elementary building parts, the segments, but can also be combined to larger building parts or contained in larger building parts.

In this way, several segments can be combined to rooms and several rooms to areas, several areas in turn to one building, several buildings to the property, several properties to the property portfolio.

The shell model is used to functionally differentiate a room from the segment, area, building, property and property portfolio.

This functional consideration is to be illustrated using the example of a floor plan for the floor of an office administration building. The VDI model building from VDI 6009 part 1 is used here.

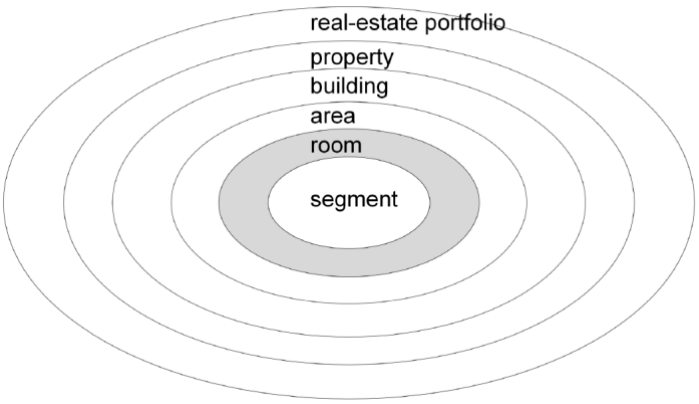

Figure 4: segmentation of the building into segments with similar building services (VDI, 2019)

Figure 5 to Figure 7 show a possible functional division and breakdown into segments, rooms and areas.

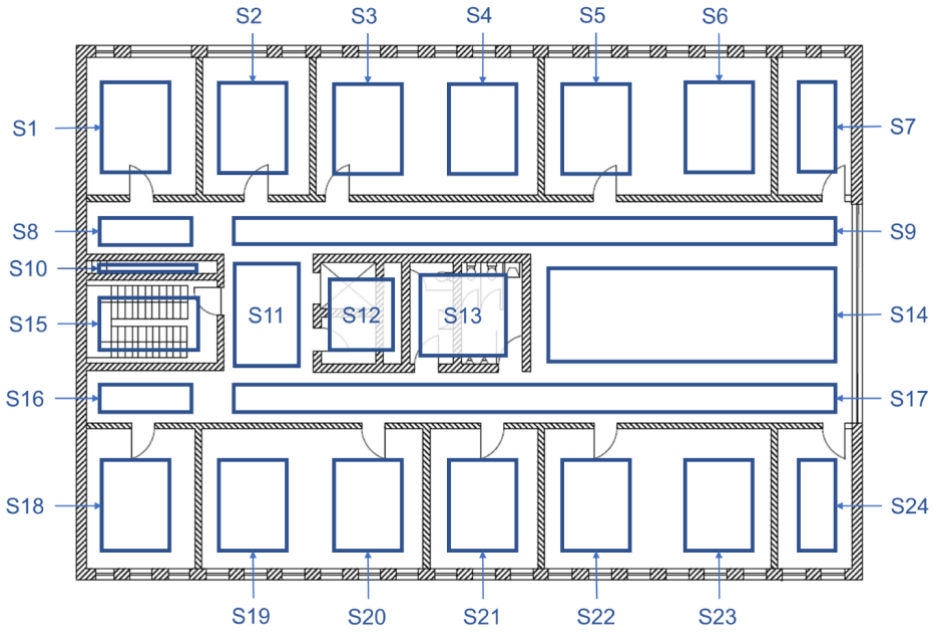

Figure 5: Example for the allocation of segments (S) in the specimen building (VDI, 2019)

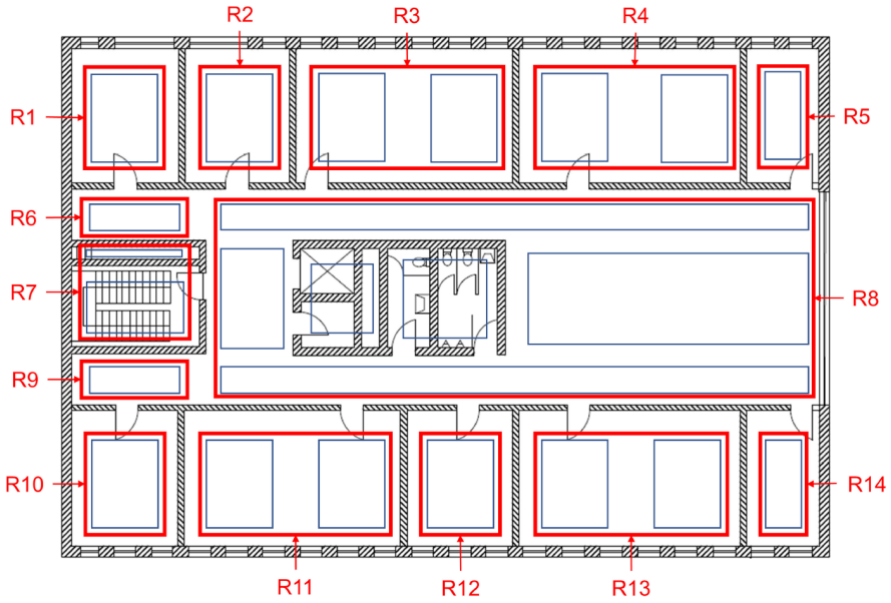

Figure 6: Example for the allocation of rooms (R) and segments in the specimen building (VDI, 2019)

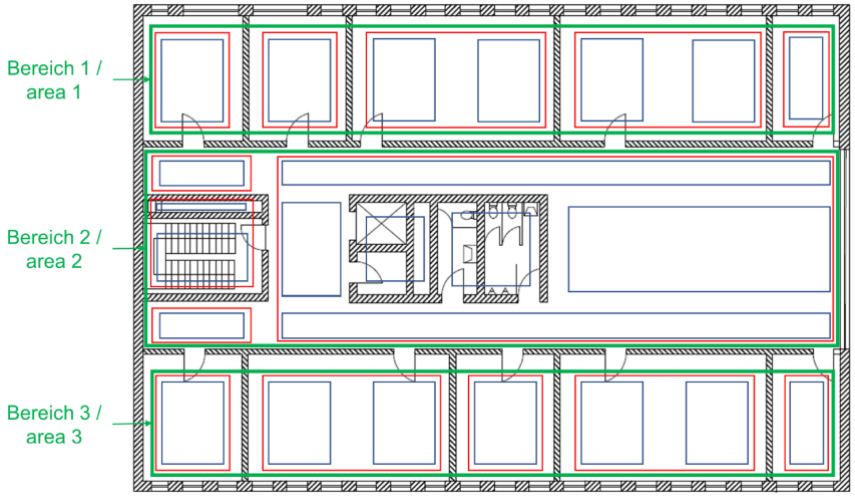

Figure 7: Example for the allocation of rooms (R), segments, and areas (A) in the specimen buildin (VDI, 2019)

ENERGY EFFICIENCY AND LIFE CYCLE COSTS

In the context of sustainability assessment of buildings, the energy-efficient operation of buildings and their systems is becoming increasingly important.

There is no doubt that building automation can make a significant contribution. This ultimately leads to efficient use of energy and resources in long-term building operation (life cycle) while at the same time meeting the highest possible demands on building use (utility values such as "productivity", "comfort", "cosiness", "flexibility", "security").

With EN 15232 and DIN V 18599-11 standards are available that define the requirements for BAC and TBES in the context of the overall energy efficiency of buildings.

EN 15232 Part 1: Influence of building automation and building management Method for calculating the contribution of building automation to the energy efficiency of buildings Efficiency classes according to EN 15232:

- Class A: highly energy-efficient BAC system and TBM functions
- Class B: extended BAC systems and some special TBM functions
- Class C: Standard BAC system
- Class D: BAC system that is not energy efficient. Buildings with such systems must be retrofitted. New buildings must not be constructed with such systems

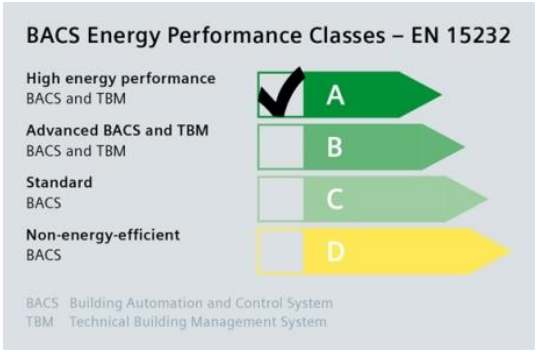

Figure 8: BACS Energy Performance Classes

This division into four classes facilitates a systematic planning process in that the BA efficiency classes, which may already have been defined in the "Conceptual Design" life cycle phase during requirements planning, can be made more concrete in the subsequent planning and construction phases through the appropriate selection of standardized BAC functions defined according to VDI 3814. It is important to note that the principle of cost-effectiveness is taken into account.

DIN V 18599-11 Energy efficiency of buildings

Part 11: Building automation

DIN V 18599 provides the basis for the calculation of energy requirements

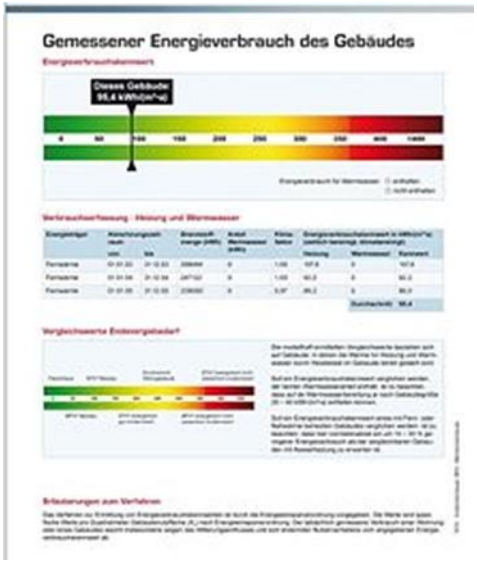

Figure 9: Calculation of the net, final and primary energy demand for heating, cooling, ventilation, domestic hot water and lighting

The DIN V 18599 series of standards deals with the calculation of the useful, final and primary energy demand for heating, cooling, ventilation, domestic hot water and lighting (energy balance) of buildings.

It was developed in a joint working committee of the DIN standardization committees for civil engineering (NABau), heating and ventilation technology (NHRS) and lighting technology (FNL). It provides a method for assessing the energy performance of buildings, as required by Article 3 of Directive 2002/91/EC of the European Parliament and of the Council on the energy performance of buildings (EPBD), which will be introduced in all member states of the European Union (EU) from 2006.

The complex technical regulations required for this purpose were published in July 2005 as DIN V 18599 under the title "Energy performance of buildings - Calculation of useful, final and primary energy demand for heating, cooling, ventilation, domestic hot water and lighting". A first revision was published in February 2007. The current version was published in October 2016. It was developed in a joint working committee of the DIN standardization committees Civil Engineering (NABau), Heating and Ventilation Technology (NHRS) and Lighting Technology (FNL). It provides a method for assessing the energy performance of buildings, as required by Article 3 of Directive 2002/91/EC of the European Parliament and of the Council on the energy performance of buildings (EPBD) from 2006 in all member states of the European Union (EU).

DIN V 18599 consists of 12 parts:

- Part 1: General balancing procedures, terms, zoning and evaluation of energy sources
- Part 2: Net energy demand for heating and cooling of building zones
- Part 3: Net energy demand for energetic air treatment
- Part 4: Net and final energy demand for lighting
- Part 5: Final energy demand of heating systems
- Part 6: Final energy demand of ventilation systems, air heating systems and cooling systems for residential buildings
- Part 7: Final energy demand of air conditioning and refrigeration systems for nonresidential buildings
- Part 8: Useful and final energy demand of water heating systems
- Part 9: Final and primary energy demand of power generating plants
- Part 10: Boundary conditions of use, climate data
- Part 11: Building automation
- Part 12: Table procedure residential construction

LIFE CYCLE COSTS AND OPTIMIZATION POTENTIAL

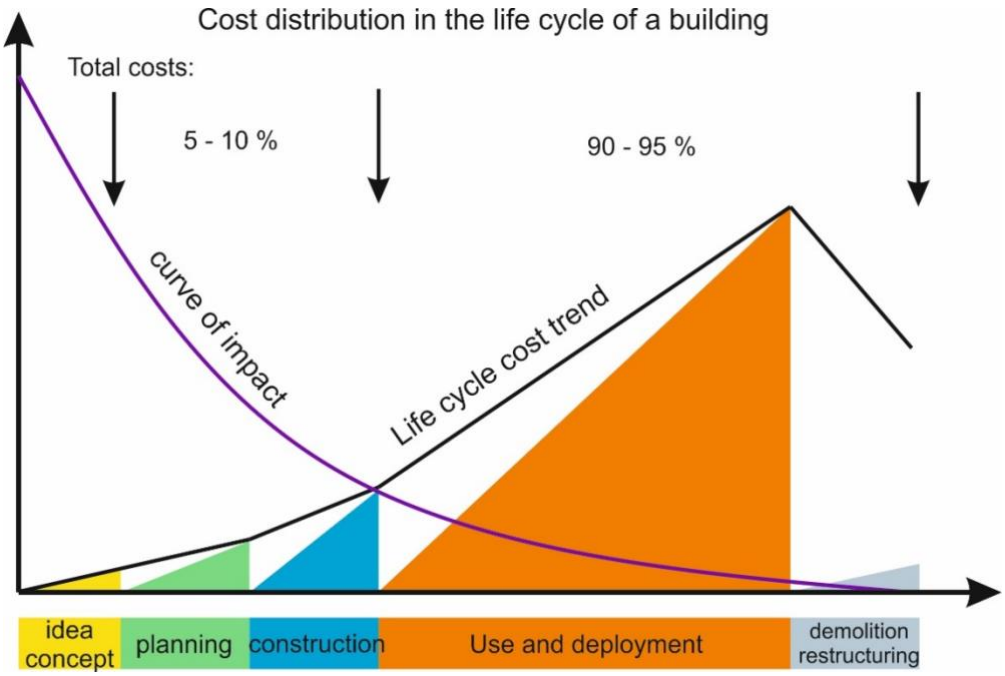

Figure 10: Life cycle costs and optimization potential

Life cycle costing is used for the economic analysis, evaluation and planning of investments. Investment expenditure, profitability and value stability are considered.

The life cycle costs of a building are all costs incurred over its entire life cycle. Included are the costs of all life cycle phases: Idea/concepts, planning, construction, usage, provision and disposal costs.

Depending on the building category and the period under consideration, the costs of use cause a multiple of the manufacturing costs (approx. 5-10 % manufacturing and 90-95 % use).

The aim is not only to minimize manufacturing costs, but also to reduce and optimize costs over the entire life cycle.

The curve of the life cycle costs can be influenced most strongly in the first phases (idea/concept, planning and construction), as shown in the influence curve in the picture. This also includes the use of building automation.

CERTIFICATIONS

There are a large number of audits and certifications for building automation. In most cases it is not the BACS itself that is certified, but the entire building.

However, a good BACS has a positive effect on the certification.

EN ISO 50001:

The EN ISO 50001 is a worldwide valid standard of the International Organization for Standardization (ISO), which is supposed to support organizations and companies in establishing a systematic energy management; it can also be used to prove an energy management system in accordance with the standard by means of certification (see lecture Energy Management in BSc. FM).

The introduction of an energy management system is basically voluntary; there is no legal obligation for certification. However, a certification according to EN ISO 50001 (or a registered environmental management system according to EMAS Regulation) is a prerequisite in Germany for the partial exemption from the EEG levy for eligible, particularly energy-intensive companies and, in the future, also for the relief of companies in the manufacturing industry from the electricity and energy tax.

The use of building automation with appropriate monitoring can support companies in certification to a large extent.

The BACS itself is not certified by DIN EN ISO 50001.

EU.BAC

Figure 11: eu.bac label

eu.bac - European Building Automation and Controls Association is the European Building Automation and Controls Association and represents the European manufacturers for Home and Building Automation and Energy Service Companies.

Since early 2013, eu.bac has been offering the eu.bac System Audit for energy-efficient and sustainable operation of building automation systems

Not everywhere where energy efficiency is written on the label is energy efficiency. This also applies to building automation systems. While individual components and products have been certified with regard to their energy efficiency for some time now, certification for entire systems was previously lacking. The European Building Automation and Controls Association eu.bac has jumped into this gap. eu.bac certification is based on scientific data and is part of the European standard EN 15232, making it one of the most important certifications for BACS.

The structured and standardized process makes it transparent how efficient the installed building automation in interaction with the technical building equipment really is. At the same time, the customer learns which control technology components and where energy can be saved most effectively. Similar to the energy label on household appliances, the letters E to AA and the color palette from red to dark green show the real estate owner or building operator at a glance how efficient the operation of his system is.

DGNB

German Sustainable Building Council - DGNB e.V. is Europe's largest network for sustainable building and has around 1,200 member organizations.

The DGNB has established and expanded a certification system for sustainable buildings and has awarded a Sustainable Building Certification in the quality levels platinum, gold, silver and bronze.

In order to make sustainable construction practically applicable, measurable and thus comparable, the DGNB has developed its own certification system. The system was first introduced to the market in 2009 and has been continuously developed since then, and is now not only considered the most advanced in the world, but is also internationally recognized as the "Global Benchmark for Sustainability".

The certification system is available in different versions for buildings, quarters and interiors. As a planning and optimization tool, it helps all those involved in construction to implement a holistic quality of sustainability.

In terms of content, the DGNB system is based on three key paradigms that set it apart from other certification systems available on the market:

- Life cycle assessment
- Integrity
- Performance orientation

The certification process consistently considers the entire life cycle of a project and instead of individual measures, the overall performance of a project is evaluated.

The NBB (Sustainable Building Assessment System) certification, which is based on the DGNB (German Sustainable Building Council), gives positive consideration to GA in the area of technical quality in operation and maintenance quality. (German Federal Ministry of the Interior, 2015)

LEED

To classify sustainable buildings, the US LEED (= Leadership in Energy and Environmental Design) system was developed in 1998 based on the British BREEAM certification system.

Buildings are assessed at b by awarding points for individual criteria. The sum of the points achieved determines how the building is rated in the certification process. LEED refers to all phases of the life cycle. The United States Green Building Council (USGBC), headquartered in Washington, and the Canada Green Building Council (CaGBC), headquartered in Ottawa, are responsible for the introduction and continuous development of the system.

- Evaluation categories:
- Sustainable sites
- Water efficiency
- Energy & atmosphere
- Materials & resources
- Indoor environmental quality
- Innovation & design process

The LEED certification awards points if a BACS is available for monitoring. For more information on LEED, visit https://www.usgbc.org/credits/existing-buildings/v2009/eac31

1.2 OPEN-LOOP AND CLOSED-LOOP CONTROL

The task of building automation is to make a technical process run as fully automatically as possible.

A technical process is a procedure by which materials, energy or information is transformed, transported or stored. In a technical process, the physical quantities are recorded and influenced by technical equipment.

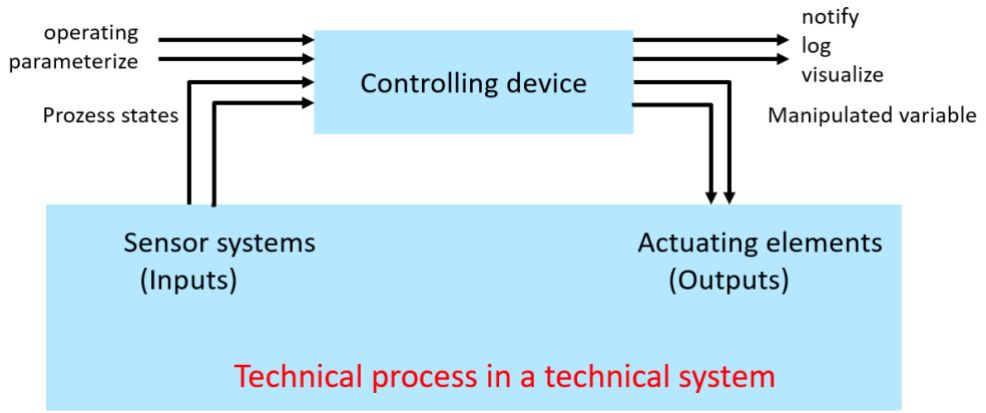

Figure 12: Technical process in a technical system

In order to automate a technical process, it is necessary both to obtain information about the process and to be able to actively interfere in the process. This process information is recorded in the form of measured values with sensors. The active intervention is done by actuators (sensors and actuators will be explained later). Therefore, the process can be influenced by the controlling device, depending on the process state recorded by the measured values. The figure shows the sphere of action.

The illustration also shows that the operator has access to the controlling system and can, for example, set parameters. In addition, the operator receives information about the technical process in the form of messages and logs, which can be displayed graphically on monitors, for example. This access and display option is also called "Operating & Monitoring".

OPEN-LOOP CONTROL

"Process whereby one or more variable quantities as input variables influence other variable quantities as output variables in accordance with the proper laws of the system.

Note 1 to entry: Characteristic for open-loop control is the open action path or in a closed action path the fact that the output variables being influenced by the input variables are

not continuously or sequentially influencing themselves and not by the same input variables." [IEC 60050-351:2006]

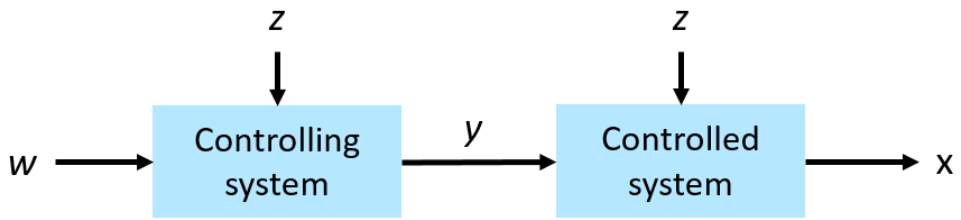

Figure 13: Structure of an open loop control

The shown basic principle represents a open loop control according to IEC 60050-351 (Commission, 2021).

On the basis of a given command variable „c", the control system generates a manipulated variable „y" in accordance with the previously entered control instructions ("the laws peculiar to the system"). This acts on the control path in such a way that the controlled variable „x" influences the process according to the requirements.

With this action sequence, the control system cannot influence the disturbance variable(s) „z". However, if it is possible to record the disturbance variables and make them available to the control system for evaluation, a control system can also react to these disturbances. Non-detected disturbances can still change the process, since, in contrast to a closed loop control, the reaching of the controlled variable is not permanently observed.

The entire sequence of actions is also called control chain and primarily reflects the behavior of a control system. An example for this can be the control of the temperature in a room. The target value would be a desired temperature curve, which is communicated to the control device. This, in turn, causes the heating valves to move into a position that results in a certain temperature at the end of the control path. The controller creates a direct relationship between the desired temperature and the valve position. This does not take into account, for example, parallel heating by persons present or the effect of prevailing outside temperatures.

Examples:

- Central heating boiler controlled only by a timer, so that heat is applied for a constant time, regardless of the temperature of the building
- Blind control with external brightness sensor

CLOSED-LOOP CONTROL

"Process whereby one variable quantity, namely the controlled variable is continuously or sequentially measured, compared with another variable quantity, namely the reference variable, and influenced in such a manner as to adjust to the reference variable

Note 1 to entry: Characteristic for closed-loop control is the closed action in which the controlled variable continuously or sequentially influences itself in the action path of the closed loop." [IEC 60050-351:2006]

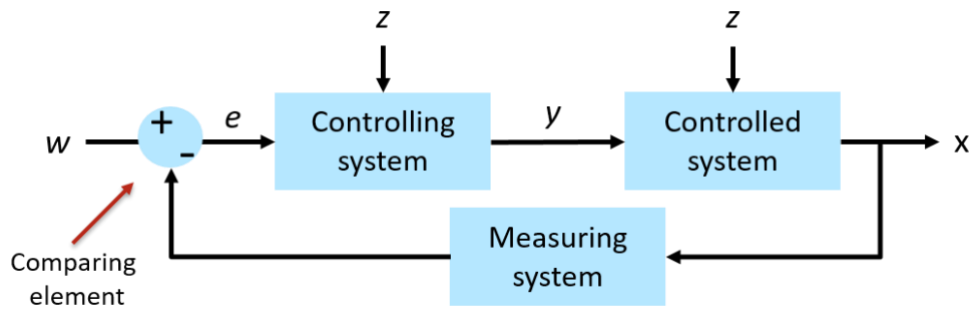

Figure 14: Structure of a closed loop control

The basic principle shown is a closed-loop control according to IEC 60050-351 (Commission, 2021).

A closed-loop control behaves completely different from a open loop control. Here, the controlled variable "x" is measured continuously and returned to the controlling system (consists of Controller and actuator) as a feedback variable "r". A corresponding manipulated variable "y" is then formed in the controlling system for correction. A closed-loop control system is characterized by a closed operating sequence, which is illustrated by the term control loop.

The controlling system is the functional unit which executes the control function(s). This means that it is to ensure that the controlled variable takes on the desired value or course. From the difference between the reference variable "w" and the feedback variable "r", the control device (with the aid of the reference element) forms the manipulated variable "y".

According to DIN IEC 60050-351, a controlled system is a functional unit which is influenced according to the control task. Such a controlled system can be an annealing furnace which is kept at a constant temperature by a closed-loop control. The burner and the control valve are also included. The closed- loop control system is completed by the temperature sensor as measuring element, the controller and the actuator. The set temperature is the target value. In the example it is equal to the reference variable.

Malfunctions are caused by changing ambient temperatures, e.g. opening the door for unloading and charging or cold annealing material.

The actuator is part of the closed-loop controlled system. It is located at the input of the controlled system and influences the mass flow or the energy flow. Typical final actuator elements for mass flows are:

- Salves
- Slider
- Flaps

The measuring system (also measuring element) is used to record the controlled variable. It converts the controlled variable into the feedback variable which is processed in the controlling device. In the simplest case, the measuring element is a sensor.

If the detection of external influences is absolutely necessary, a closed-loop control (no open-loop control) should be selected for the automation of the process.

Examples:

- Central heating boiler including a thermostat to compare the building temperature with the temperature set on the thermostat. This generates a controller output to maintain the building at the desired temperature by switching the boiler on and off
- Constant light control with internal brightness sensor

EXAMPLE OF A CLOSED-LOOP CONTROL

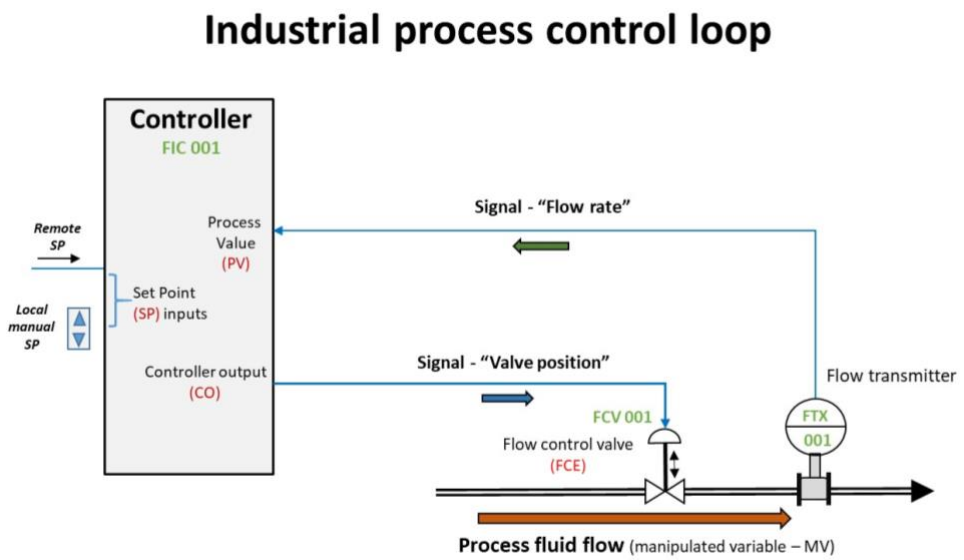

Figure 15: Example of a closed-loop control (Dougsim, 2011)

The basic building block of industrial process control systems is the "closed-loop control", which contains the elements for measuring and controlling a process value to a desired setpoint.

The controller can be a discrete piece of hardware or a function within a large computer-based SCADA or PLC system, shown here as a controller (SCADA or PLC will be described later). Setpoints can be set manually on location or from another source.

An example of a flow controller with a flow transmitter and a control valve is shown. The green text are "tags" that describe the function and identify the equipment. Since each control loop has a unique number, the tags are unique within an installation to avoid confusion. In this case:

- FIC = Flow indicating controller
- FCV = Flow Control Valve
- FTX = flow transmitter
- SP = process set point
- PV = process value
- CO = controller output
- MV = manipulated variable

PID CONTROLLER

In general, the controllers are distinguished according to their continuous and discontinuous behavior. Among the best known continuous controllers are the "standard controllers" with P, I and D behavior.

We will not discuss discontinuous controllers.

The influence of the manipulated variable on the controlled variable, and consequently the properties of a controller, are specified as transfer function G(s). It is the most common mathematical description of the behavior of linear control loop elements and therefore the description of controllers.

A controller can consist of one, several or a combination of P, I and D elements.

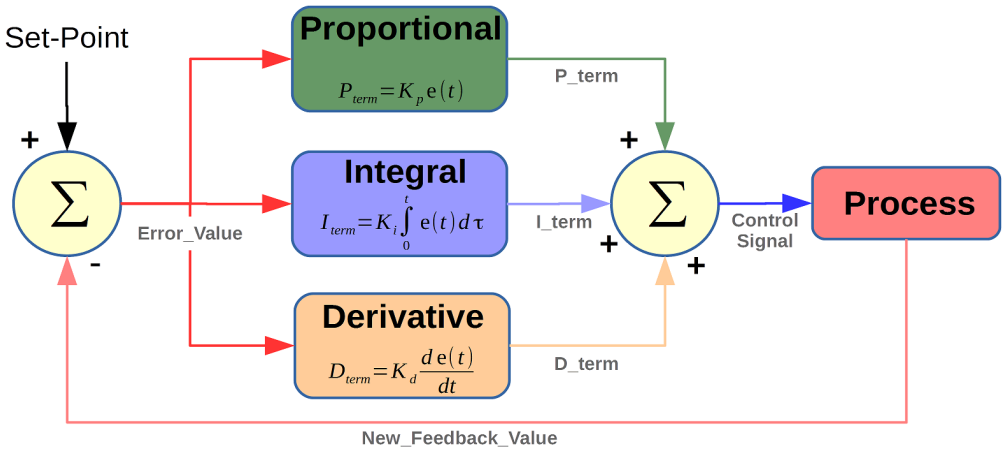

Figure 16: Design of a PID-Controller

P- element:

The P-element is a transfer element, which has a proportional transfer behavior.

Mathematically, this relationship in the time domain can be represented as follows:

$$y_{(t)} = K_p \cdot e_{(t)}$$

K_p is called proportionality factor. It indicates how much the control difference is amplified. The larger the proportionality factor, the smaller the control difference.

I- element:

Also called integral element, I-element or integral element and is a transmission element with an integral transmission behaviour.

Mathematically, this relationship in the time domain can be represented as follows:

$$y_{(t)} = K_i \int e_{(t)}\, dt$$

K_i is called integration constant. Since there is no steady state at the output, pure I-systems do not show any self-regulating properties. The only limitation results from the technical limitation, e.g. the overflow of the tank.

D- element:

The D-element is a transmission element which has a differential transmission behavior.

Mathematically, this relationship in the time domain can be represented as follows:

$$y_{(t)} = K_d \frac{de_{(t)}}{dt}$$

Differentiating, so-called D-behaviour simulates the 1st derivative of the input signal with respect to time. The output signal thus provides the rate of change of the input variable and serves to make a control fast. However, it must be taken into account that there is no pure D-behaviour in physics, since all systems have a mass (mechanical) or a capacity (electrical). An ideal jump function at the input (infinite gradient) thus provides an infinitely large impulse at the output, which is also technically impossible to reproduce.

A PI-controller is an addition of a P- and an I-element.

A PID controller is an addition of a P, I and D element.

OPERATING MODES

In addition to the automatic operation through open-loop and closed-loop control systems, there are also other operating modes. Depending on the requirements, different operating levels within the building automation system are provided for these, as shown in the following table.

Table 1: Operating modes

Operating modes in addition to automatic operation	
Manual operation	Meets the minimum requirements in terms of operation and signalling on site, but can only be used if the substation is intact
Local override operation	Allows direct intervention in the technical plant, even if the sub-station is not available. The emergency operation serves exclusively to maintain the emergency operation of important plants or plant components.
Local priority operating	Allows a direct dialog with the technical plant using the substation, if it is functional.

With regard to the European Machinery Directive, the use of the term "emergency operation" or "emergency operating level" is no longer appropriate in the field of building automation. The term "emergency" has a different meaning and may only be used in case of danger to life and health. For the best possible differentiation, the term "local override operation" or "local override operation level" is now used.

Local override operation allows direct intervention in the building control system. With this level, important parts of the system can be controlled manually to maintain important functions when the substation is unavailable, failed or disturbed. The operating elements of this level act directly and without regard to the automation device.

The local override operation can be realized conventionally with switches and push-buttons, but it must be ensured that all elements of the LVB are supplied by an independent power supply. To avoid manipulation, access to the operating elements of the LVB must be secured accordingly, for example by integration in the control cabinet.

When using a manual/local or local priority operating level, all safety-relevant functions must be solved externally. The local operation must not be used for safety shutdown. The operations of the local override operation are carried out directly, without securing or interlocking, in accordance with ISO 16 484-2, section 3.110, so that the full responsibility for all interventions remains to the operator

1.3 AUTOMATION PYRAMID

Building automation systems are hierarchically structured on three levels: The field, automation and management level. Together they form the automation pyramid.

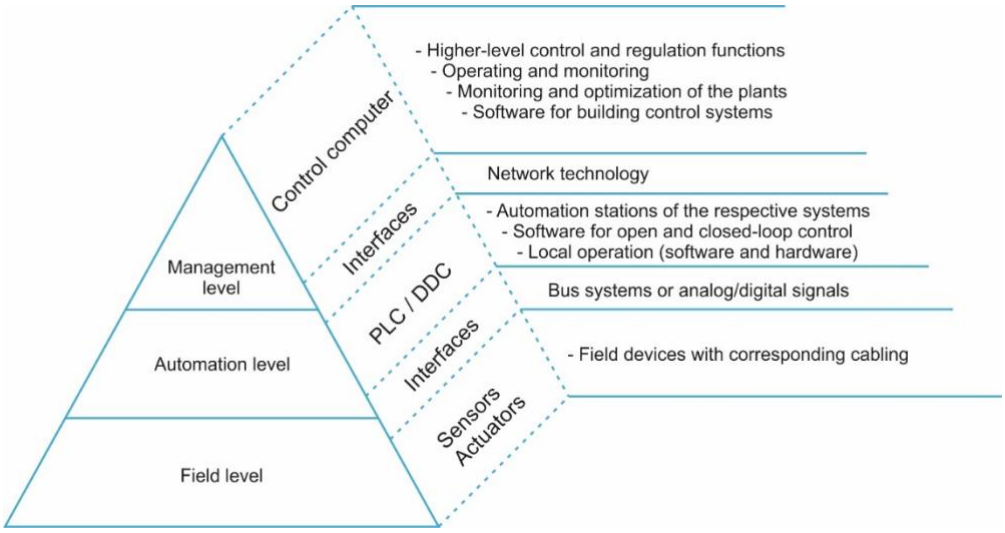

Figure 17: Automation pyramid

Field level:

On the lowest level, the field level, the various technical systems of the building are operated with the help of the field devices (sensors and actuators). Sensors record information (e.g. motion detectors, buttons, brightness, temperature) and send these as data telegrams via a suitable interface to the actuators or the higher levels. The actuators or higher levels receive the data telegrams and convert them into switching signals, e.g. for the lighting, heating, air conditioning and ventilation system. Information is both processed in the field level and provided for the higher levels.

Automation level:

The automation level takes over the task of the building's technical systems on the basis of the data supplied by the field level and the specifications from the management level in order to control and regulate. The automation equipment takes over the monitoring (limit values, switching states, meter readings), control and regulation of the technical systems. Automation stations process the resulting data and communicate them to the field or management level. They are small, powerful devices that can be configured with standardized software tools.

Management level:

At the management level, higher-level operation and monitoring of the processes and alarms in case of malfunctions are carried out. Information from building automation is collected here and evaluated e.g. at the monitor workstation or printed out on the protocol printer. The management level has the task of realizing control and optimization algorithms that span the entire plant and are superordinate to the plant. In addition to the standard PC, a redundant (multiple existing) data storage including possibilities for data backup and, if necessary, an uninterruptible power supply (UPS) is used as equipment feature. Management systems can be realized as central control room or as distributed systems with several operator stations based on a client-server architecture.

FIELD LEVEL

The field level consists of the sensors and actuators of a technical system. The measured values of the sensors were converted into electrical signals and sent to the higher level through suitable communication paths. The higher levels can also control the actuators, which can perform different functions.

Communication between the levels takes place either via analog/digital signals (see 3.1.2) or via bus systems (see 4).

ACTUATORS AND SENSORS

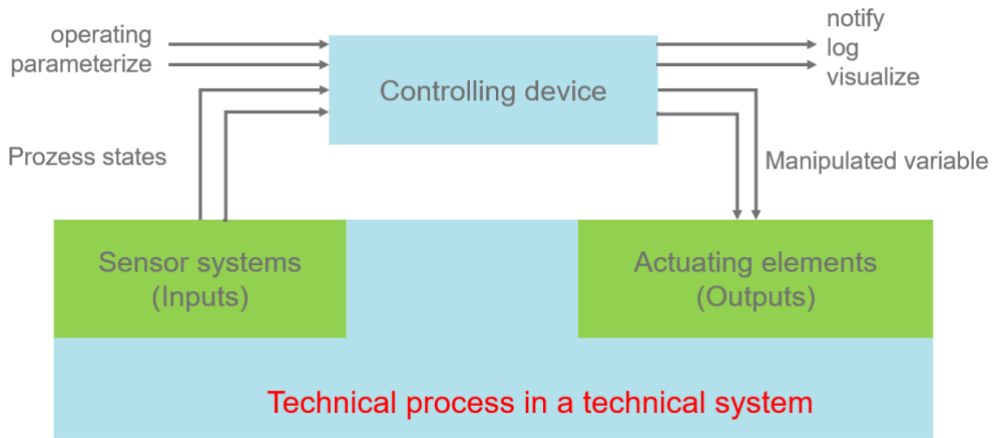

Figure 18Field level in a technical process (green shaded)

Sensors (inputs) and actuators (outputs) in a technical system are usually independent components which are connected to a technical plant and communicate with the control or regulation equipment of the building automation.

The sensors and actuators are located on the field level of the automation pyramid. Typical functions of the field level are switching, positioning, signalling, measuring and counting.

Sensors

A sensor (from the Latin sentire, meaning "to feel" or "to sense"), also called a detector, (measurand or measuring) transducer or (measuring) probe, is a technical component that is able to detect certain physical or chemical properties (physical e.g. heat quantity, temperature, humidity, pressure, sound field sizes, brightness, acceleration or chemical e.g. pH value, ionic strength, electrochemical potential) and/or the material composition of its environment qualitatively or quantitatively as a measured quantity. These quantities are detected by means of physical or chemical effects and converted into an electrical signal that can be further processed.

A distinction is made between binary, digital and analog sensors.

Sensors generate the input signals for the automation process.

Actuators

Actuators are usually described as drive units that convert an electrical signal (commands issued by the control computer) into mechanical movements or changes in physical parameters such as pressure or temperature and therefore actively influence the controlled process.

In measurement and control engineering, actuators are signal converters which form the final control elements in a control loop. During an open-loop or closed-loop control process, they convert the signals into effects that influence the controlled variable. An example is the opening and closing of a valve or a ventilation flap or the control of a blind motor.

A distinction is made between binary, digital and analog actuators.

Analogue, binary and digital signals

Definition: If a signal is both value and time continuous, it is called an analog signal. Such signals represent a continuous process continuously. Examples are speech, music, image and measurement signals.

Definition: A digital signal, on the other hand, is always discrete in value and time (and the message it contains consists of the symbols of a defined set of symbols). It can be, for example, a sampled and quantized (as well as coded in any form) speech, music or image signal.

An analog signal is a physical quantity that can take on continuous values in the course of size (amplitude) as well as in time.

A digital signal (digitus: finger, lat.) is a physical quantity, which can take only certain discrete values. The values correspond to the number of agreed states. If two states are agreed, then these are binary (digital) signals.

A signal is called value-continuous, if the significant signal-parameter - for example the momentary value - can take all values of a continuum (for example of an interval). If in contrast to this the signal parameter can take only countable many different values, then the signal is value-discrete.

Opposite to this the signalparameter of a time-discrete signal is defined only at discrete moments.

Binary signals

A binary signal consists of two (mostly logical) states. They are worth - and time discrete. There can be only one defined state at a time. "There is no such thing as a little pregnant".

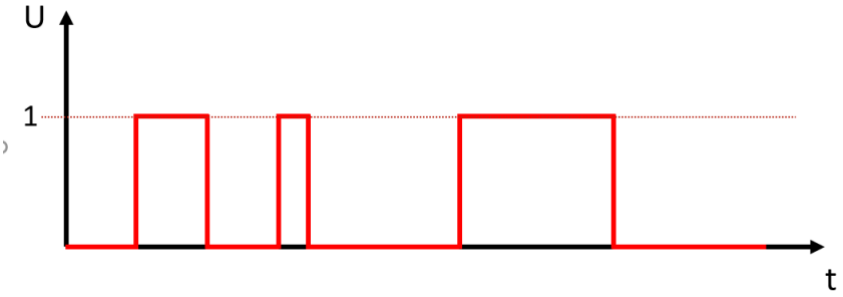

Figure 19: Binary signals

In the example the signal curve of a voltage U over time is given. The value range in this example was defined as 0 and 1.

The binary values are usually interpreted by an automation system as "on/off" or "open/closed.

Binary input signals

Binary input signals are supplied by sensors that can accordingly "only" map two states. Usually, these are output via pushbuttons, switches or signal contacts.

The signal voltage at the sensors is usually 24 V DC, although a wider signal range is specified in the open and closed-loop control equipment.

For example, an "on" signal at a 24 V DC input to a control system is detected from 15 V upwards. This serves to avoid errors caused by longer cable lengths, where the voltage can drop due to the line resistance of the cable.

Binary output signals

Binary output signals are provided for actuators that can control "only" two states accordingly.

Usually these are switching signals for motors, lighting etc.

The signal voltage for the actuators is usually 24 V DC. Larger voltages (loads) can be controlled via relays or contactors.

Digital Signals

Digital signals are similar to binary signals (and are therefore often erroneously combined). They are also value-discrete, but have a larger value range.

This value range is theoretically infinite, but from a technical point of view it is always limited depending on the application.

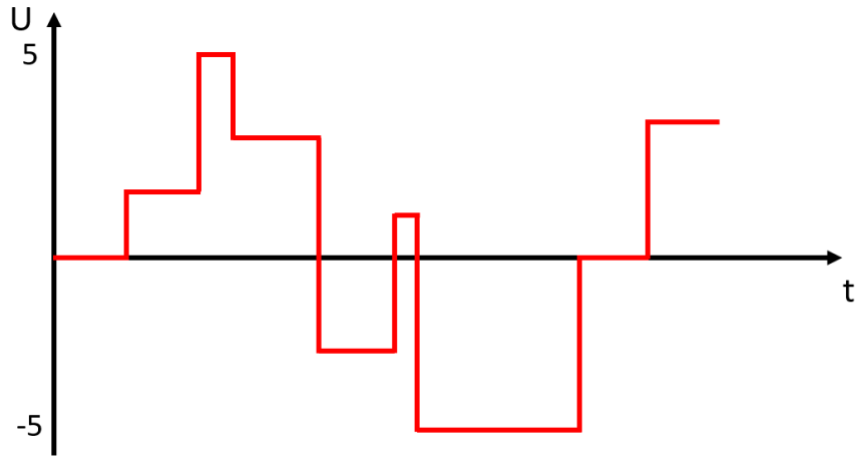

Figure 20: Digital Signals

In the example, the signal curve of a voltage U over time is shown. The range of values in this example is however larger than in the previous example. It includes all integers from -5 to 5.

Digital input and output signals are usually transmitted by bus systems (see chapter XXX).

Analog Signals

Unlike binary or digital signals, an analog signal is both value- and time-continuous and has an infinite number of values.

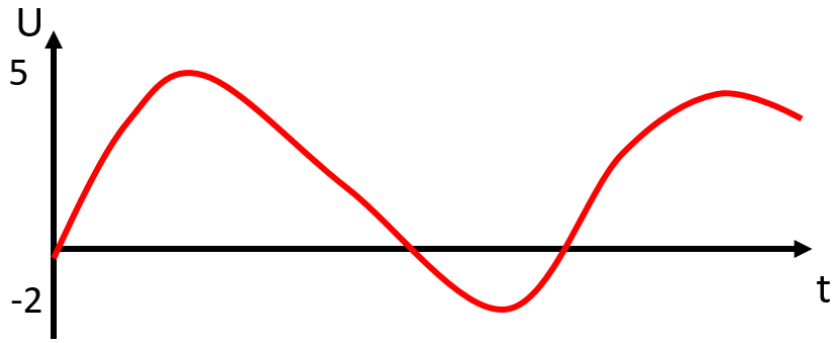

Figure 21: Analog Signals

In this example, the signal curve of a voltage over time is given. The value range in this example includes all real numbers from -2 to 5.

If an analog information shall be transmitted analog, then this is relatively simple. No special interface is necessary. Indeed there are certain interfaces and processing elements, but their function is relatively simple. In principle it is like connecting a loudspeaker to an (analog) audio amplifier. The signal is led from the amplifier to the loudspeaker via a cable and the loudspeaker outputs the signal as sound.

However, analog values cannot be processed directly by computers, just like control or regulation devices. They must be converted into digital signals by analog/digital converters (A/D converters) and transmitted. The sampling rate (sampletime) of the signal must be kept as low as possible. High sampling rate = high accuracy.

Even if the analog signal arrives at the control or regulating equipment as a digital value, one still speaks of analog signals and signal processing.

Analog input signals

Analog input signals in automation engineering are usually defined in their value ranges.

If the signal is transmitted via a voltage, the value range is 0-10 V.

If the line is monitored, i.e. it is checked whether the line is interrupted, the effective value range is 2-10 V. The value range 0-2 V is used for monitoring.

The same applies to signals that are transmitted via the current. Here the value range is 0-20 mA or 4-20 mA.

Nearly all sensors that measure physical quantities are analog sensors (e.g. pressure, humidity, temperature, electrical resistance etc.)

Example: Functional principle of pressure sensor:

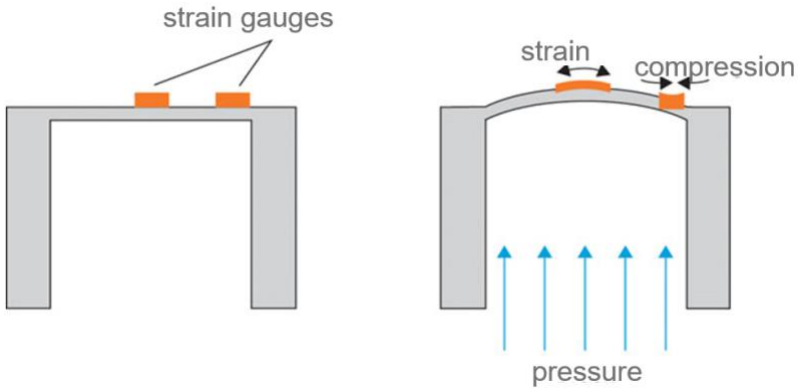

Figure 22: Functional principle of pressure sensor

The pressure sensor consists of a stable base body with a thin memran. Stretch marks are attached to the membrane. When the membrane is stretched or compressed, the sensitive resistance structures of the stretch marks are changed. The mechanical quantity (pressure) is converted into a proportional electrical quantity (resistance).

Analog output signals

Like the analog input signals, the analog output signals have fixed value ranges that correspond to those of the input signals.

Analog output signals can be used to control e.g. actuators, frequency converters (speed-dependent control of a motor), ball valves or volume flow controllers

AUTOMATION LEVEL

The automation level is the connection between the field and management level. They communicate upwards and downwards in the structure of the automation pyramid and must have corresponding interfaces.

Two main control systems are used at the automation level, the programmable logic controller (PLC) and the direct digital control for building automation (DDC-BA).In building automation, they perform automation tasks for building services equipment and systems. The corresponding programs are stored on them, how the automation should take place. They can also be operated on site, if equipped with operator panels (HMI interface = human-machine interface).

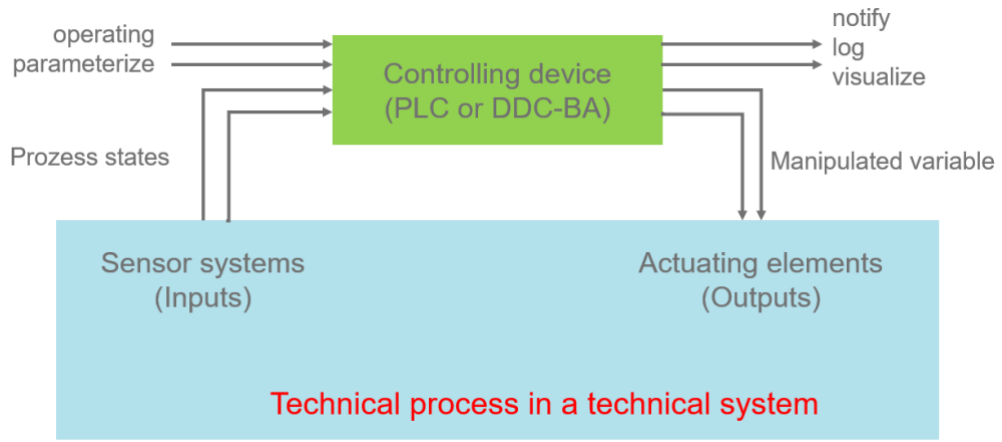

Figure 23: Automation level in a technical process (green shaded)

In the already known flow chart, the PLC or the DDC-BA represent the controlling devices that automate the technical process.

You can see that the sensors and actuators of the technical system (field level), as well as the equipment for operation, parameterization, notification, visualization and logging (automation level) are connected to the controlling device. The PLC or the DDC-BA is a central element in the BACS.

Building automation is of course not only "one" technical process, but is almost always composed of several different technical processes (e.g. HVAC, shading, lighting, etc.). Accordingly, several PLCs or DDCs are also used. One speaks of a decentralized system.

A few years ago, this was different, as everything was usually connected to a central controlling device system. This is called a centralized system.

PROGRAMMABLE LOGIC CONTROLLER

A programmable logic controller (PLC) is a component for open-loop or closed-loop control systems. It is defined according to DIN EN 61131 as follows:

"Programmable logic controller (PLC); digital electronic system, designed for use in an industrial environment It uses a programmable memory for internal storage of user-oriented instructions to perform special functions such as logic, sequence, time, counting and arithmetic, and to control different types of machines or processes through digital or analog inputs and outputs. The PLC and also its associated peripherals are designed to be easily integrated into an industrial system and used for all intended functions". (VDE, 2003)

The PLC has its roots in industrial automation. In recent years, it has also been increasingly used in building automation and in some places replaces the DDC-BA systems that have dominated until now, which in turn have their roots in room automation.

A PLC is programmed with a software according to DIN EN 61131-3. The program is stored on the internal, overwritable memory of the PLC.

A distinction is made between two systems::

1. (Standard) SPS = Specially developed hardware (is usually used)
   This hardware is based on a microcontroller, which is adapted to the requirements in the field of control engineering.
   It has a modular design and is usually mounted directly on standardized mounting rails, so-called DIN rails, in a control cabinet.
2. Industrial PC (IPC) (usually only for special or old systems)
   An industrial PC is similar in structure to a personal computer. However, it is adapted in form and function to the environmental conditions in an industrial plant (e.g. dust, heat etc.). In addition, IPCs are differentiated between a soft and a hard PLC. With a soft PLC, the complete functionality is executed as user software on the respective operating system. With a hard PLC the functionality is guaranteed by plug-in cards. These are not relevant in the area of the more modern BAC.

Hardware

A PLC or PLC system consists of at least three components.

These are:

1. Power supply unit:
   Most PLCs work with 24 V DC. The power supply unit converts the 230 V mains voltage accordingly. It supplies both the CPU and the connected modules.
2. CPU:
   The CPU (Central Processing Unit) is the heart of the PLC. It houses the microcontroller, memory and programming interface. In the past, an RS-232 interface (also called COM port) was usually used as programming interface. Today, almost only Ethernet interfaces are used. The CPU executes the control program, which was previously programmed by the users and contains the actual logic.
3. Modules:
   The modules (also extension modules) are the interfaces between the CPU and the connected systems. Via the input and output modules, the CPU receives information from sensors (inputs) and can control actuators (outputs). Communication modules are used to connect bus systems (e.g. next lecture unit). In addition, there is a large number of special modules such as counters, controllers, etc.

Functionality

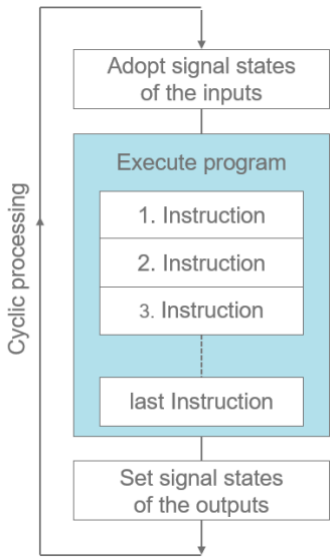

Figure 24: IPO-principle of a PLC

A PLC runs its program cyclically according to the "IPO" principle.

IPO = Import – Prozess – Output

One cycle consists of reading the signal states at the inputs, processing the control program and setting the signal states at the outputs. After the cycle is completed, the loop starts again from the beginning.

The time required for an IPO cycle is also called cycle time.

Programming

The programming languages with which a PLC can be programmed are standardized according to EN 61131-3, although most manufacturers offer their own software packages.

There are several different languages, from graphical to purely text-based.

DIRECTDIGITALCONTROL-BUILDINGAUTOMATION (DDC-BA)

DDC-BA's are similar in structure to a PLC and have their roots, as already mentioned, in room automation. They are normally used by the individual trades for controlling systems and, like PLCs, communicate with the management and field level via interfaces.

The hardware of a DDC-BA is largely similar to that of a PLC. The DDC-BA has a CPU and a memory. But, according to their task, DDC_BA are internally hard-wired and usually cannot be extended with additional modules.

The number of inputs, outputs and communication interfaces are fixed. Because of its expansion possibilities a PLC is more flexible (but also more complex) than a DDC-BA.

A DDC-BA has no standardized programming language according to IEC/EN and is usually programmed with manufacturer-specific programs. It is also possible that a DDC-BA is supplied by a manufacturer and can only be parameterized.

MANAGEMENT LEVEL

The highest and therefore superior level of the automation pyramid is the management level. The main tasks of the management level are:

- Monitoring and optimizing the operation of a plant
- Visualization of historical and statistical data
- Higher-level operation and parameterization of the system or equipment

The users can perform the tasks through one or more supervisory computers as a central control room or as distributed systems with several operator stations.

The management level forms, through an interconnection of all BA systems with (manufacturer-independent) interfaces to the automation level, an interoperable overall system.

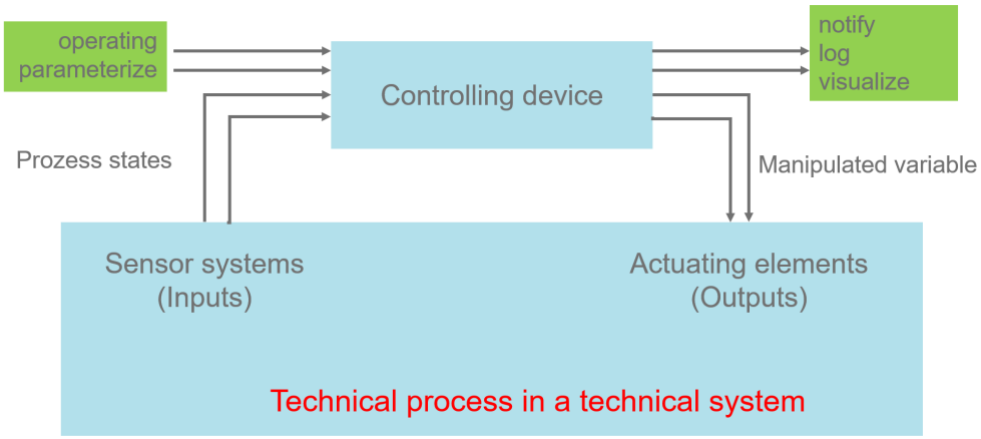

Figure 25: Management level in a technical process (green shaded)

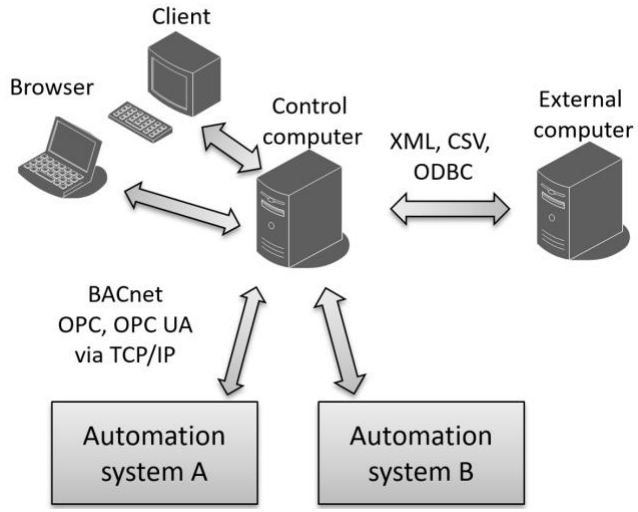

Figure 26: Schematic representation of a management level

In the Figure 26 you can see an example of a management level.

A control system is connected to two automation systems (A and B). The interface can be BACnet or OPC, among others (see 6.2 Network protocols in Building Automation).

The users access the control system via clients or browser-enabled devices in order to operate and monitor the plants and systems.

An external system can be connected via a data interface (XML, CSV, ODBC). This can be a database for storing the accumulated information, but also any other system that is allowed/able to communicate with the GA.

Current trends show that new web technologies such as HTML5 are shifting functions such as operating and monitoring more and more to the automation level. This is in line with standards, as these functions are not bound to the respective levels according to EN ISO 16484.

On the other hand, new functions (e.g. for energy management according to EN ISO 50001) were added at the management level.

1.4 BUSSYSTEMS

Before we really start with the bus systems, let's have a look at the difference to the conventional (analog and digital) signals. With the conventional signals, sensors/actuators are directly connected to the respective controller. This results in a so-called star wiring (Figure Figure 27).

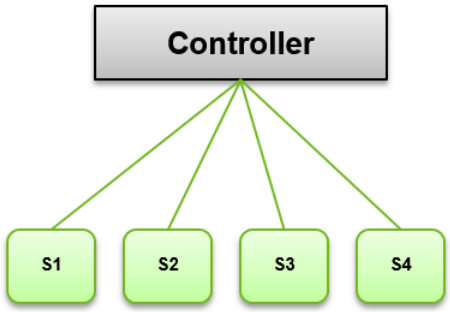

Figure 27: star wiring controller

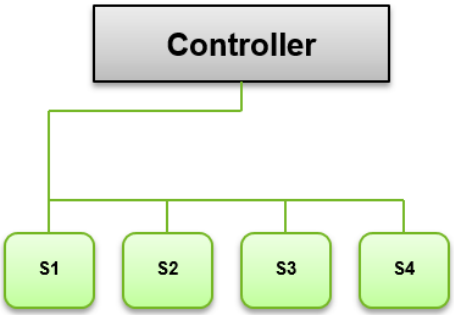

Figure 28: Bus system controller

Star wiring has the disadvantage that one cable is required per connection. On the one hand, this is expensive to install, on the other hand, cables are considered a fire load.

Bus systems are not wired as a star, but as shown in Figure Figure 28. The devices connected to the bus (Binary Unit System) are also called participants. The participants are connected to the bus. Each participant has a unique addressing. This means that fewer cables are required, which reduces costs and reduces the space required in the control cabinet.

Imagine as an example the bus connection of the public transport from the main station to the university. The street is the bus line (cable), and each stop is a participant. The bus (omnibus) carries the information (also data packages), that is the passengers from A to B. The bus knows the stop (address) and lets the corresponding passengers (information) get off and on at the right place.

Far more information can be transported via the bus than with conventional analog/digital signals, e.g. also diagnostic data. Due to the large amount of data, however, special diagnostic tools (as hardware or software) are required for commissioning or troubleshooting.

Bus systems describe the hardware signal transmission and thus represent the standardization of electrical levels and telegrams. There are manufacturer-specific and independent bus systems.

The counterpart to the bus systems are the protocols, which define the software technical definition of the data transmission. They standardize the grammar, language and semantics of data telegrams. Protocols are discussed in chapter 4.1.8.

Topologies

In addition to the classic bus, there are other topologies for connecting a technical system. The connections can be realized via cable or radio technology.

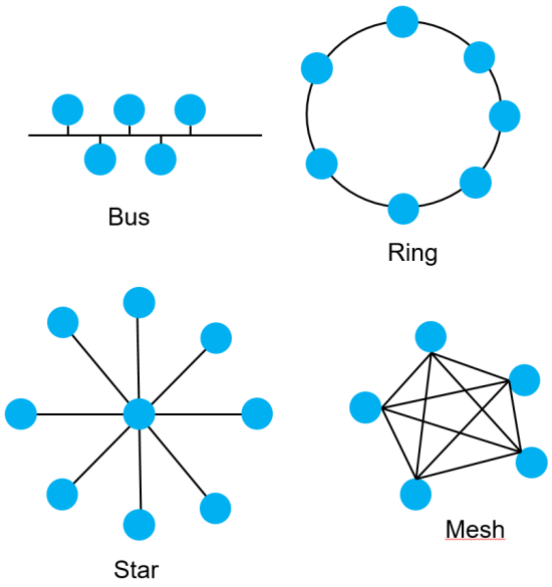

Figure 29: Bus Topologies

The topologies used in the BA are shown in Figure 27. The points represent the participants and/or controllers. The classic bus or tree cabling is used most often. The star cabling is mostly used in network technology.

Meshed and fully meshed systems are found almost exclusively in radio technology or when a system has to be secured as good as possible against failure (redundancy).

The ring topology had its origin in early network technology and is no longer used today.

Basic bus types

The best known basic bus types are the RS232 and RS485 bus.

RS232:

The RS232 (Recommended Standard 232) bus is the classic serial*1 2-wire bus. It was developed in the early 1960s by the EIA (Electronic Industries Association) and was frequently used in computers until the 2010s (COM ports).

A classic application was the point-to-point connection by means of telephone lines via modems. In addition, almost all PLCs used to be programmed via the serial interface.

The maximum line length for RS232 depends strongly on the data rate used. The faster the data must be transported, the smaller the maximum line length, e.g. at 19.200 baud*2 the maximum length is ~15 meters.

Nowadays RS232 can be found almost only in old systems. It was replaced by USB and Ethernet.

*1 "The serial interface is a colloquial term for an interface for data transfer between two devices, where single bits are transferred one after the other in time (serial data transfer). The term is used to distinguish it from a parallel interface, where several bits are transmitted simultaneously on several circuits. [Wikipedia - Serial interface]

*2 A baud is the unit for the symbol rate (walking speed) in communications engineering. It is indicated with symbol per second. A symbol in turn is defined by the measurable signal change in a physical transmission medium and can be, for example, system-dependent 1 bit or 1 byte.

Figure 30:RS232 (Homm, 2021)

RS485:

RS485 is an asynchronous serial interface*1 for connecting several participants. It originally comes from industry, but quickly found its way into building services engineering.

RS485 is very robust and can control many participants (e.g. 32). The cable length can be up to 1200 m and can be extended additionally with amplifiers. The data transmission can usually be selected faster than RS232 (max. 12Mbps).

In building services engineering RS485 is usually found in the protocols Modbus and BACnet (see Lecture Unit 4 and 6).

*1 "Asynchronous data transmission is a transmission method in communications engineering in which characters are transmitted asynchronously, i.e. at any time. Thus, in contrast to synchronous data transmission, the transmission is not aligned to a clock signal.". Wikipedia - Asynchronous data transmission]

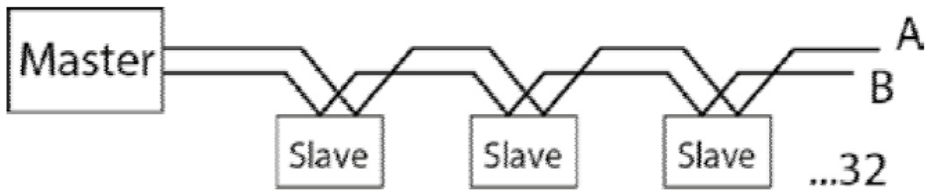

Figure 31: RS485 Master-Slave

FIELDBUS SYSTEMS

Fieldbus is the generic term for various physically distinct bus systems for automation, production engineering, building automation and automotive technology. These are wired or wireless bus systems with which field devices, i.e. sensors and actuators, such as drives, switches, motors, actuators and lamps are connected to the control devices and control computers and through which the fast data exchange between the components takes place.

Definition according to EN 61158:

Fieldbus:

- Communication system based on digital, serial data transmission
- Use in automation systems and process control systems

Fieldbus system:

- System with at least one fieldbus and one connected devices

DIFFERENCE BETWEEN BUS SYSTEM AND PROTOCOL

Bus systems

A bus system is the hardware transmission of (electrical) signals. These electrical levels and telegrams are usually standardized.

For the commissioning of a bus system a special commissioning software or a specially developed device is usually used.

Protocols

A protocol is the software technical definition of the telegrams in e.g. a bus system. The protocol describes the grammar, language and semantics of telegrams. The services are also defined in the protocols, e.g. subscribe, poll or report.

1.5 FIELD BUS SYSTEMS IN BUILDING AUTOMATION

KNX

KNX is an industrial communication system used in home and building control for the information-technical networking of devices (sensors, actuators, controlling devices, operating and monitoring devices). Its use is coordinated with electrical installation technology, thus ensuring functions and automated processes in a building.

The umbrella organization of the KNX system is the Konnex Association cvba (under Belgian law) which was founded in 1999. It is composed of the EIBA (European Installation Bus Association), EHSA (European Home Systems Association) and the BCI (BatiBUS Club International).

Currently, more than 500 members are represented in Konnex Association. These members are manufacturers from all application areas of home and building systems technology, including lighting, shutter control, security, heating, ventilation, air conditioning, monitoring, alarm systems, water control, energy management, IoT solutions, ETS apps, meter reading as well as household appliances, audio and other.

KNX is the successor of the European Installation Bus (EIB) and therefore adapted for use in electrical installations. Since 2003 KNX has been standardized in EN 50090 and in 2006 this standard was accepted as international standard ISO/IEC 14543-3.

A standard-compliant KNX connection enables the use of many different manufacturer devices. This enables planning across different trades, higher functionality as well as flexibility of the installation. The parameterization of the devices, which can be adapted at any time, also makes a new construction or conversion of an object easier.

Since KNX products are usually more expensive than devices for a conventional installation, KNX only makes sense if several trades are to be linked together or if the corresponding installation is to be adapted quickly and flexibly in the event of changes in use.

STUCTURE

The structure of a KNX installation is hierarchical and is a tree topology (Figure 32).

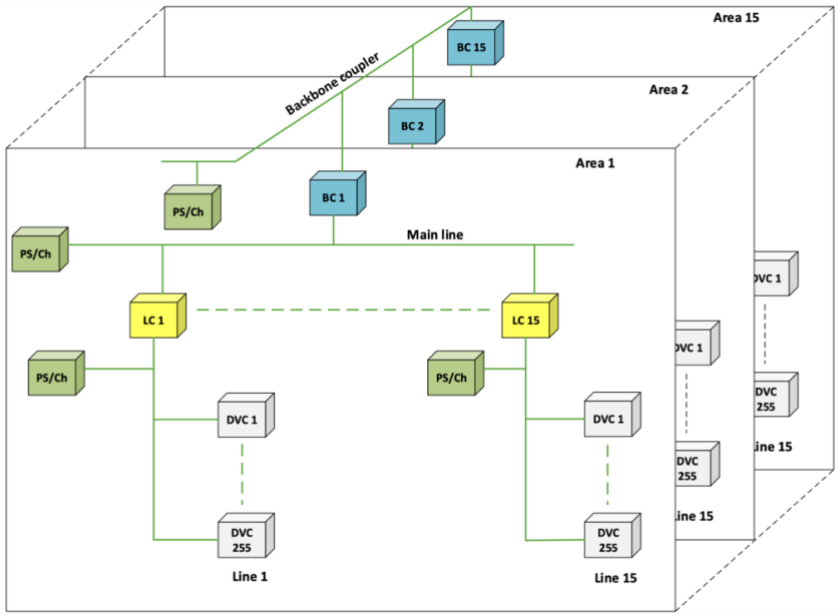

Figure 32: Full KNX Topology (Ivory Egg (AUST) Pty Ltd, 2021)

The lowest level is formed by the participants (e.g. actuator/sensor). These are connected to each other via lines. The lines are in turn connected to the main lines via line couplers. Together they form an area.

The main lines of the areas are each connected to the area line (backbone or main transmission line) via an area coupler.

This KNX structure can be mapped to a building structure. The backbone is the building. The areas form the floors of the building and the lines form the corridors on the floor.

In addition to the devices mentioned here, devices for the power supply and/or couplers are used as line amplifiers.

With a line repeater, a line can be extended to (gross) 256 stations, with one station for the line coupler and one for the line repeater. This leaves a maximum of 254 stations per line.

When using a line amplifier, the permissible total line length of 1000 m for a line must not be exceeded.

Each device also requires a unique physical address. This is necessary for data communication between the devices and for parameterization of the system.

The following sketch shows the information technology networking of devices with KNX. All devices are connected to the KNX bus and exchange data telegrams with each other.

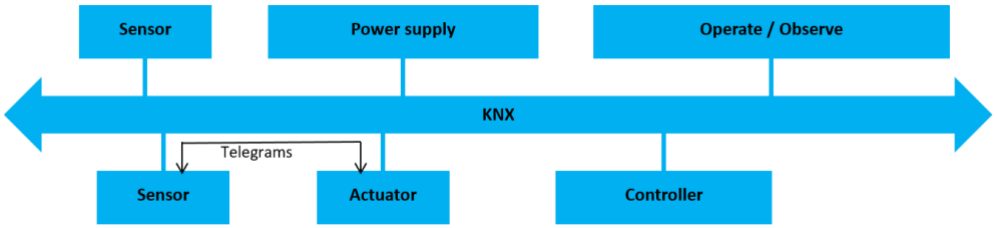

Figure 33: Information technology networking of devices with KNX

Here are several transmission media for the transmission of KNX data packets. Thereby KNX.TP (TP = twisted pair) is the most used variant, because it is usually the most favorable, if a cable laying is not forbidden (e.g. monument protection). Attention: In principle, TP cables are also used in other applications, KNX.TP means that the communication takes place via a 2-wire twisted pair cable.

The disadvantage of KNX.TP is the low speed of max. 9600 baud. The big advantage is the possible cable length of up to 1000 m.

KNX works with event-oriented telegrams. This means that communication only takes place if an event (e.g. pushbutton actuated) has also taken place. This leads to the fact that communication is reduced to the most necessary and the bus lines are not overloaded.

KNX.IP is usually only used if corresponding operating and monitoring stations are to be integrated. These are connected to the KNX bus via IP routers. KNX.IP can also be used to bridge long distances by using fiber optic cables*1.

KNX.PL uses the existing power grid in the building by superimposing the sinusoidal voltage of the power supply grid. KNX.PL is used when no additional wiring can be installed (e.g. listed buildings or special buildings such as churches, museums, etc.).

HNX.RF uses radio or infrared signals. A bus connection (cable) is not necessary, but the power supply must be guaranteed. KNX.RF has a short range and is therefore usually only used for extensions where cable laying is no longer possible.

*1 Fiber optic cables (FOC) are used in network technology when larger distances have to be bridged.

SOFTWARE

The ETS software (currently in version 5) is required for project planning, parameterization and commissioning of a KNX system. ETS stands for Engineering Tool Software and runs on Windows computers.

The KNX system is parameterized, there is no programming, as for example with a PLC, in the actual sense.

On the homepage https://www.knx.org/ you will find the current license models as well as many instructions, planning and training documents. The demo version, with which a maximum of 5 devices can be parameterized, is free of charge.

With the ETS eCampus (https://wbt5.knx.org/) you can take your first steps in the KNX world free of charge via a web-based training and receive a certificate upon successful completion.

LON

Besides KNX, LON is a common system in the building sector. LON stands for local operation network and is a universal field bus that is mainly used in building automation. LON was developed by the American company Echelon around 1990 and has been standardized in EN/IEC 14908 since 2008.

LON is in direct competition with KNX in building system technology, although both systems have a similar system approach. In some cases, the systems also complement each other, so that both systems can be used simultaneously. Especially in older buildings, LON is still strongly represented, whereas in new installations the trend is clearly towards KNX. LON has its main focus in room automation, especially for the control of lighting, blinds and HVAC.

The "intelligence" is provided by the Neuron chip developed by Echelon in the LON network. It is the heart of LON technology and is a processor system that performs various tasks. The Neuron chip, together with a few other components, forms a complete participant (node) in a locally operating network.

STRUCTURE

The Neuron chips are connected to the transmission network by means of a transceiver. This connection is the network interface.

There are different types of transceivers, among others for Twisted Pair (TP), Powerline (PL), Link Power, Infrared etc..

The structure in a LON is similar to that of KNX. The topology can be a ring, star, line or tree structure, or a combination of these.

Similar to KNX, a maximum of 127 nodes form a line and a maximum of 255 lines form a network. The maximum size of the LON is therefore 32,385 nodes. In line topology, a maximum extension of 2,700 m at a transmission rate of 78 kbit/s is possible.

SOFTWARE

The "LONMaker" tool from Echelon is used for parameterization and commissioning. A license fee (credit) of $5 is due per integrated device. This makes large installations quickly expensive.

In LONMaker several subdivisions in domain, subnet, line and node can be carried out. The parameterization is done with graphical objects and connection lines.

DALI

“DALI, or Digital Addressable Lighting Interface, is a dedicated protocol for digital lighting control that enables the easy installation of robust, scalable and flexible lighting networks.

DALI was originally developed to allow digital control, configuration and querying of fluorescent ballasts, replacing the simple, one-way, broadcast-like operation of 0/1-10V analog control.” (DIIA, Digital Illumination Interface Alliance, 2020)

DALI (as well as DALI-2 and D4i) is a trademark of DiiA ((Digital Illumination Interface Alliance) and is standardized in IEC 62386.

The DALI protocol is used exclusively in lighting technology and is used for bidirectional communication between lighting control products. A DALI system consists of at least one DALI controller, the 2-wire bus and a lighting control device. Depending on the controller, several lines (usually two) can be connected, each with a maximum of 64 lighting control units or sensors.

Electronic ballasts (ECGs) are usually used as lighting control devices, which have an interface for the DALI 2-wire bus in addition to the power supply for the luminaire.

Depending on the application, the 2-wire bus can be used for both communication and power supply of some devices (e.g. sensors).

During commissioning and each extension of the DALI system, each device is assigned its own unique address. By this addressing each device can be controlled individually as well as in broadcast. The devices can be grouped individually or in up to 16 groups. The grouping is

done by the commissioning software, no rewiring is necessary. In addition, up to 16 light scenes can be defined per line.

Due to the bidirectional digital communication not only a control between the devices is possible. DALI devices can also send feedback regarding errors, the status of a luminaire or requests for other information.

DALI devices can be connected via the existing electrical installation if a 5-core cable has been laid, which is usually the case. The three wires "phase, neutral and protective earth" are the power supply, the remaining two are used for the DALI bus (see picture).

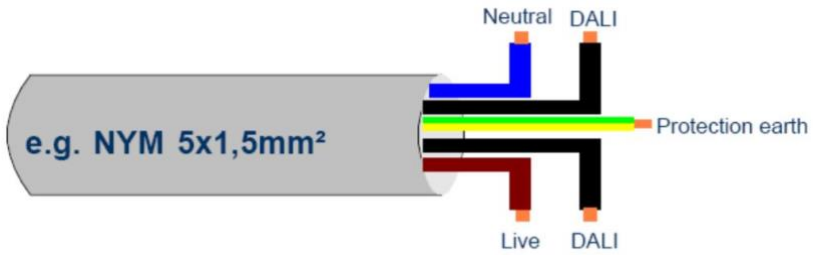

Figure 34: Wiring concept for DALI (Osram, 2021)

The DALI bus is protected against polarity reversal, which means that the wires can be reversed. The voltage on the bus is approx. 16 V.

Among other things, DALI also offers so-called emergency functions. If the voltage supply fails and returns, the DALI luminaires switch on automatically.

DALI AND DALI-2

“DALI-2 refers to the latest version of the DALI protocol.

Compared with DALI version-1, there are many new commands and features in DALI-2. While DALI version-1 only included control gear, DALI-2 includes control devices such as application controllers and input devices (e.g. sensors), as well as bus power supplies.

DALI-2 is focused on interoperability of products from different vendors, and the DALI-2 certification program confirms compatibility of products with the relevant specifications.” (Digital Illumination Interface Alliance, 2020)

Only Certified DALI-2 products are allowed to carry the DALI-2 logo issued by DiiA, which means interoperability and only DiiA members can certify their products. All certified products are listed in the DiiA product database. DiiA organizes regular plugfests where member companies can test the interoperability of their products with those of other manufacturers

DALI-2 certification involves verification of test results by DiiA. In contrast, DALI version 1 product compliance is based solely on self-declaration, which has led to interoperability problems in the market.

D4I

D4i (intra-luminaire DALI) is the standardization of DALI for luminaire interiors and adds a number of specific new functions to the existing DALI-2 range. By specifying power supply requirements and smart data capabilities, D4i enables intelligent LED luminaires.

The D4i specifications ensure that power is available to control devices, sensors or wireless communication devices attached to or integrated into the luminaire.

Meanwhile, D4i drivers in the luminaire can store and report a variety of data in a standardized manner.

D4i products are DALI-2 products with additional features. All D4i certified drivers and control devices are also DALI-2 certified.

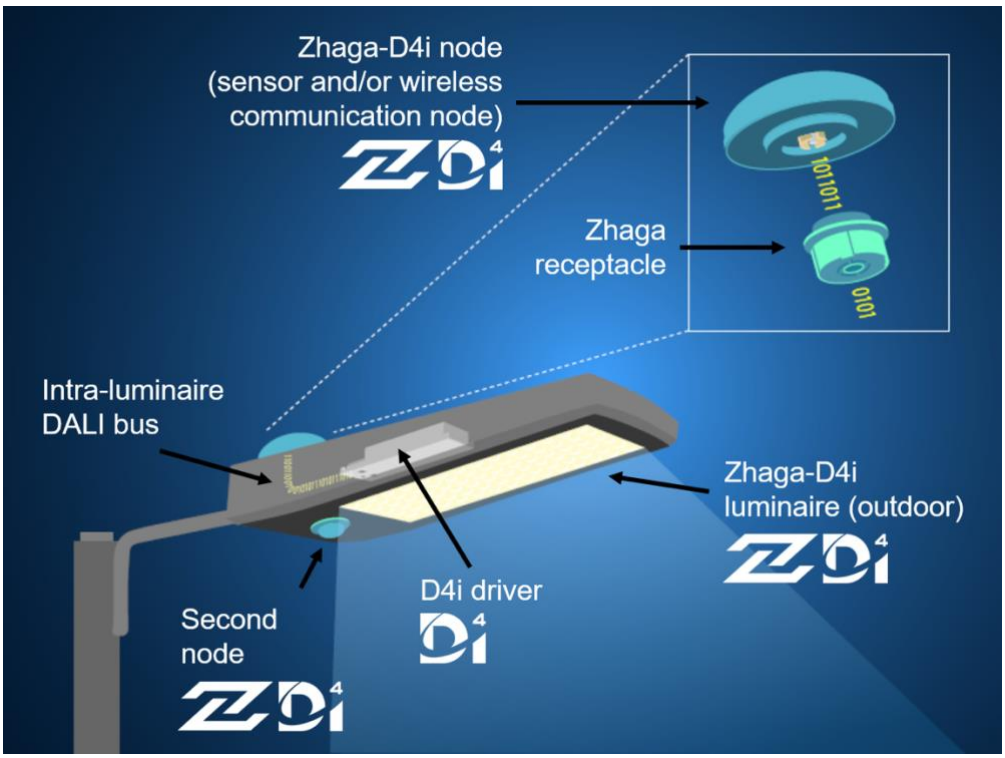

Figure 35: The new Zhaga-D4i interface standard for smart luminaires (Zhaga, 2020)

The picture shows the "smart" IoT luminaire with D4i standard certified by the company Zhaga and DiiA. You can find more information about this at: https://www.digitalilluminationinterface.org/zhaga-d4i/

DMX

Another field bus in lighting technology is DMX (Digital Multiplex). It is mainly used for effect lighting in stage and event technology.

With one control signal 515 channels can be controlled. A luminaire can have several channels such as brightness, color and lighting direction of multifunctional spotlights.

The basis for DMX is the classic RS-485 bus. In contrast to DALI, DMX is much faster in controlling the individual luminaires. This is due to the fact that the transmitter continuously sends data telegrams to the receivers, but these do not confirm the reception. It is therefore a unidirectional communication.

MP-BUS

The MP-Bus is a 2-wire bus from the company BELIMA and mainly networks HVAC actuators such as actuators, control valves or volume flow controllers in the field. The data exchange takes place as a master-slave system where the master can control and query up to 8 actuators per line. A line has a maximum length of 800 meters.

The actuators with MP-Bus interface usually have their own connections for sensors for temperature, humidity, absolute volumetric flow, relative volumetric flow, min./max. limits, angular position, operating status, fault messages or switch queries (ON/OFF), which can be queried via MP-Bus.

M-BUS

The M-Bus (Meter-Bus) is used for the acquisition of consumption data by means of energy meters of all types and is standardized in EN13757. The 2-wire bus operates on the master-slave principle, with the master requesting the data from the slaves (the energy meters). In addition to the 2-wire bus, radio transmission can also be used.

A master can query a maximum of 250 participants (slaves) on one line. The maximum extension of 4,000 meters is quite large, but data transmission is very slow at up to 960 baud, which is why process control using M-Bus is not possible.

Another advantage of the MP-Bus is the possibility of supplying power to the energy meters. Retrofits of energy meters without an M-Bus interface are also possible with M-Bus plug-on modules.

M-Bus devices are mainly used for the following measuring tasks:

- Electricity meter
- Water meter
- Gas meter
- Heat meter

M-Bus devices can be used for smart metering systems. According to § 2 No. 7 MsbG (Messstellenbetriebsgesetz), an intelligent metering system consists of the smart meter gateway and at least one modern metering device for recording electrical energy.

SMI

SMI (Standard Motor Interface) is the "DALI" for blinds and shutters. It is a 2-wire bus and has a maximum length of 350 m. A maximum of 16 motors can be connected per SMI bus.

The SMI interface is integrated directly in the respective drive/motor. Similar to DALI, the two free wire pairs of the five-wire power line can be used for the SMI bus. The SMI motor is equipped with an incremental encoder. This enables very precise control of the hanging height and slat angle. This is again important for blinds with sun position tracking.

In addition to control, the SMI bus also provides diagnostic functions. There are two different SMI types, SMI with 230 volts and SMI-LoVo with 24 volts power supply. Due to the different supply voltages, the two types must always be operated separately!

RADIO SYSTEMS

ENOCEAN

EnOcean is a manufacturer-independent standard for battery-free wireless technology. It is characterized above all by very low energy consumption, using the principle of "energy harvesting".

The sensors and actuators obtain the energy they need from motion, light and temperature.

Example: an EnOcean pushbutton generates just enough energy through pushbutton actuation (converting kinetic energy into electrical energy) to process and send its information.

In addition to the advantage of wireless technology (no wiring), EnOcean has the added benefit of requiring no batteries and therefore almost no maintenance. Pushbuttons and

switches can be mounted on glass walls of modern buildings, as with all radio-based solutions.

ZIGBEE

Zigbee is a standard for wireless networks with low data volume. Unlike EnOcean, Zigbee devices require an additional power supply (e.g. battery or power supply unit).

The name Zigbee comes from the "zig-zag dance" of honeybees (see: https://www.telkonet.com/what-is-zigbee/).

The advantage of Zigbee is the mixing of networks (see picture) and the resulting range of (theoretically) several kilometers.

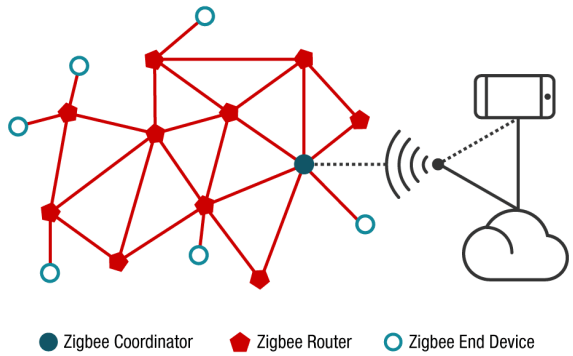

Figure 36: Zigbee Network

Zigbee is used by many well-known manufacturers and products such as Philips Hue, Osram Lightify, Google OnHub, etc., among others.

Z-WAVE

Z-Wave is a wireless communication standard from the companies Sigma Designes and the Z-Wave Alliance. It is mainly used, like most wireless standards, in home automation. However, in the course of Industry 4.0 and IoT, it is increasingly used in BA.

The big advantage of Z-Wave is its encrypted communication and low energy consumption. Z-Wave devices are both battery-powered (e.g. sensors, buttons, etc.) and connected via a mains voltage (e.g. blind control, light control, gateways, etc.).

1.6 NETWORK TECHNOLOGY AND PROTOCOLS

Today, modern network technologies are standard in every building and an integral part of the IT infrastructure. When we talk about network technology in a building, these are structures and systems for exchanging data from (information) technical devices. These structures and systems form the IT infrastructure (IT = information technology).

The IT infrastructure uses both hardware and software systems for data exchange and processing, which we will clarify in the course of this chapter.

The systems can be interconnected either by cables (wired networks) or by a radio standard (wireless networks). A combination of wired and wireless networks is also possible.

In chapter "General network technology", the general network technology is described first and in chapter "Network protocols in Building Automation", selected network protocols of building automation are shown.

GENERAL NETWORK TECHNOLOGY

A network is a connection of many IT devices. An example of such a network is shown in Figure 37. In this IT network, all computers are connected to each other via cable or radio. These connections must of course take place under certain rules and with the help of protocols. For this purpose, there are several standards in network technology and various devices that enable communication (and thus data exchange).

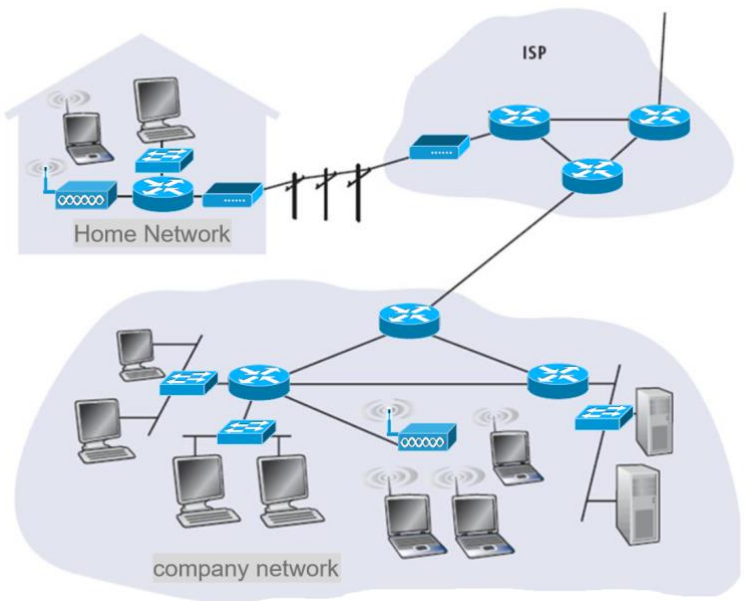

Figure 37: Example of a typical communication network (Wetherall, 2012)

The devices listed here are explained in the section "Hardware".

As already shown, networks are a connection of several (at least two) technical devices.

To ensure that the devices can communicate with each other as error-free as possible, several communication relationships and forms of communication have been defined.

- The communication relationships regulate who speaks to whom
- The forms of communication regulate who speaks when

COMMUNICATION RELATIONSHIPS

The relationships and forms can be explained, for example, using a group of people.

The simplest communication relationship is the unicast or dialog between two people. There is a sender (red) and a receiver (green). All other persons (blue) do not take part in the communication. A telephone conversation serves as an example, where the roles of the sender and receiver can change (communication form).

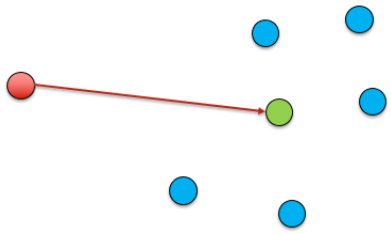

Figure 38: Unicast

The second communication relationship is the broadcast. This can be simply described by a lecture. The sender is, for example, a professor, and the recipients are the students.

Technically, you can think of broadcast with the example of radio or television. A sender broadcasts, and everyone listens. Normally, however, the sender does not know who is listening.

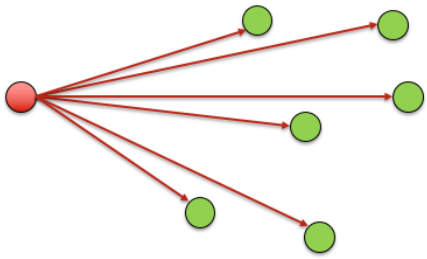

Figure 39: Broadcast

The third communication relationship is the multicast. As an example, you can again imagine a group of people. However, with multicast, the sender only addresses a specific group of recipients.

To do this, however, the sender must know exactly whom it is addressing. In the example of the group of people, the sender must address the recipients with a specific characteristic. Example: All students of the civil engineering program.

Technically, this is realized by addressing. Each participant (e.g., computer) has a unique address that must be known to the sender.

FORMS OF COMMUNICATION

The communication forms are divided into simplex, half-duplex and full-duplex.

Simplex is a so-called directional mode. Communication takes place in only one direction, from the transmitter to the receiver. Sensors, pagers, classic radio or television serve as examples.

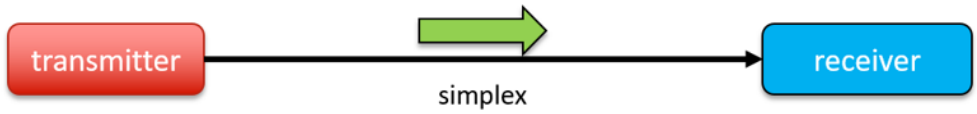

Figure 40: Simplex

In half-duplex, the transmitter can also be the receiver (and vice versa). Communication takes place in alternating mode. If one transmitter is active, all other participants are receivers.

As an example, you can imagine communication via two radios. The one who speaks is the transmitter, the other the receiver. The communication can be in both directions. If both participants talk at the same time, there will be errors in the communication.

In old computer networks, simultaneous sending was prevented via special protocols.

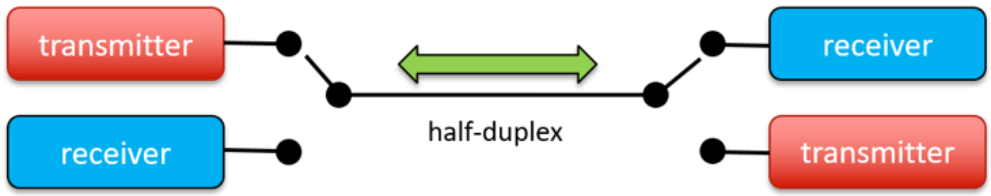

Figure 41: Half-duplex

Full-duplex (usually also just "duplex") is the opposite mode. Here, the participants are both transmitters and receivers at the same time. Communication is possible in both directions simultaneously.

Today's telephone and current computer networks serve as examples.

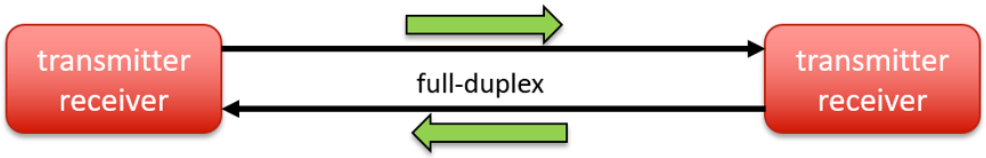

Figure 42: full-duplex

NETWORK ARCHITECTURE

In addition to the communication relationships and forms of communication, networks can also differ in their architecture.

In the peer-to-peer architecture (Figure XXX), all computers have equal rights and there is no hierarchy. In most cases, two computers communicate with each other in a peer-to-peer network. However, several computers can also be connected to each other.

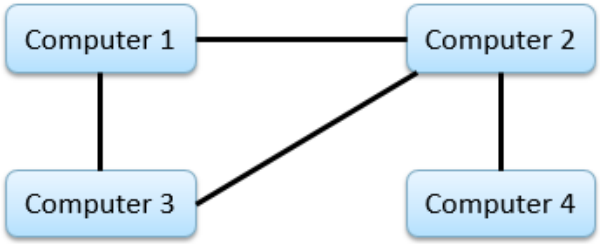

Figure 43: Peer-to-peer-Achitecture

In the example in Figure 41, computer 2 can communicate with all other computers, but computer 1 can only communicate with computers 2 and 3 and not with computer 4.

A peer-to-peer network is usually relatively fast and inexpensive because no additional hardware (e.g., switch) is required. Peer-to-peer networks are used almost nowhere today. They have been replaced by client-server networks.

The client-server architecture (Figure 44) is hierarchical. Almost all networks today are built on this architecture.

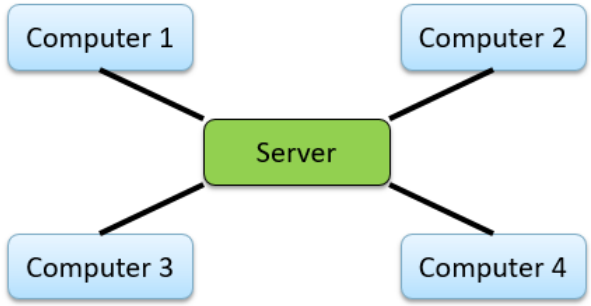

Figure 44: Client-Server-Architecture

In the client-server architecture, the clients (computers) always first establish a connection to a server and make corresponding requests there. The server evaluates these requests and delivers the corresponding response.

Advantages of the client-server architecture:

- Centralized maintenance and data backup, saving resources and costs
- Easily expandable
- Higher security through access control, as clients have to authenticate themselves at the server

Disadvantages of the client-server architecture:

- High acquisition costs, as a powerful server is required
- Total failure of the network in case of server failure (therefore secure server or design redundant)

NETWORK TOPOLOGIES

In topology, we consider the communication paths of the individual network nodes. Participants can be both clients and servers.

Networks are wired as a star or tree topology, whereby the tree topology is an extension of the star topology.

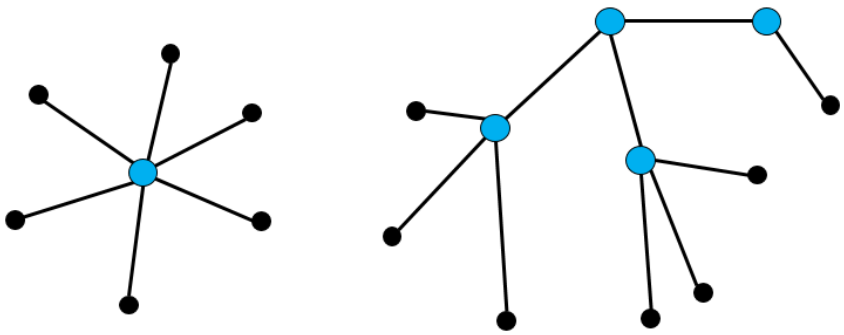

Figure 45: Star topologiy (left) and tree topology (right)

The topology describes the arrangement of the respective network components (hardware). Although it is shown similarly in the figures, it must not be confused with the network architecture, which describes the functionality of the network.

The star center is formed by a switch. This receives the requests from the network participants (senders) and forwards them to the receiver. Each participant is connected to the switch via a network cable. The switch knows the addresses of the participants, and communication is uni- or multicast.

The predecessor of the switch was the hub. This can still be found in older networks. A hub forwards all requests as a broadcast to all connected nodes. This sometimes led to increased (unnecessary) data traffic.

n a tree topology, two or more switches are connected together so that more subscribers can participate in the network.

NETWORK DIMENSIONS

Networks are subdivided on the basis of their technologies and spatial extents and ranges. The networks are not separate and can communicate with each other, e.g., a subscriber in a LAN is also a subscriber in a MAN or WAN.

The following subdivisions are indicative and not 100% delineated.

- PAN - Personal Area Network: personalisiertes Netzwerk, z. B. Bluetooth
- LAN - Local Area Network: lokales Netzwerk, z. B. Ethernet
- MAN - Metropolitan Area Network: regionales Netzwerk
- WAN - Wide Area Network: öffentliches Netz, z. B. ISDN
- GAN - Global Area Network: globales Netzwerk, z. B. das Internet

STANDARDIZATION

IEEE 802.3 Ethernet

The most important standard in today's network technology is IEEE 802 ("i tripple e" pronounced). It was created in the 1970s by a project group of the Institute of Electrical and Electronics Engineers (IEEE) and has been continued and expanded until today. 802 is the number of the project group for network standards.

The IEEE is an international organization of electrical and engineering professionals and experts and has over 423,000 members in over 160 countries (as of 2016).

The IEEE 802 standard is divided into several working groups. The most important are:

- 802.1 High Level Interfaces (Internetworking)
- 802.2 Logical Link Control
- 802.3 Ethernet (CSMA/CD)
- 802.11 Wireless LAN
- 802.14 Broadband cable television
- 802.15 Wireless Personal Area Network (e.g. Bluetooth)

Probably the best known standard is IEEE 802.3 with the title Ethernet. This defines the network as we currently use it. It uses the asynchronous media access method SSMA/CD (Carrier Sense Multiple Access with Collision Detection), in which several network nodes can access the transmission medium. The handling of collisions during signal transmission plays a major role here.

Several extensions already exist which, among other things, improve transmission speeds (e.g. 802.3z "Gigabit Ethernet") or define an additional power supply (e.g. 802.3af "Power over Ethernet").

IEEE 802.11 Wireless LAN

Another IEEE working group deals with the well-known WLAN standard. IEEE 802.11 exclusively standardizes communication in wireless networks.

In WLAN networks, the access point replaces the switch. While the switch is always wired, the access point distributes over the radio link.

A WLAN always has a network name (SSID = Service Set Identifier) with which the participants/clients can connect.

Various methods are available for addressing data packets and extending network coverage. The best known is the Wireless Distribution System (WDS), which connects several access points by radio. A WDS-capable access point receives the (possibly weak) radio signal, processes it and transmits it again with amplification. The access point also works as an amplifier (repeater).

If you are operating a WLAN, you should ensure that it is securely encrypted. The IEEE 802.11 standard offers several encryption options. The current encryption should at least use the WPA2 standard. Great importance should be attached to a secure key (more on IT security in Chapter XXX).

WPA2 is based on AES (Advanced Encryption Standard) and is considered to be largely secure.

The latest security standard is WPA3. However, this is currently only supported by a few devices.

The transmission speeds of the different WLAN standards are shown in Table 2 and are defined by the additional letters in the standard.

Table 2: Data transmission rate wireless LAN

Standard	Frequency band	Data rate
IEEE 802.11b	2,4 GHz	max. 11 Mbit/s
IEEE 802.11g	2,4 GHz	max. 54 Mbit/s
IEEE 802.11n	2,4 oder 5,0 GHz	max. 600 Mbit/s
IEEE 802.11ac	5,0 GHz	max. 6.936 Mbit/s
IEEE 802.11ad*	60,0 GHz	max. 6.757 Mbit/s

The technical communication of WLAN (and radio in general) takes place via electromagnetic waves. WLAN uses three frequency bands. A frequency band is a (usually small) section of the electromagnetic spectrum.

"Three frequency ranges are available for WLANs according to IEEE 802.11. The most commonly used range is 2.4 GHz, the second is 5 GHz, and the third is 60 GHz. All frequency ranges can be used worldwide without a license. This means that no fees have to be paid for use on private property. However, this also means that other radio technologies and radio networks are also active in these frequency ranges. The speed and stability of a radio network with IEEE 802.11 depends to a large extent on the intensity of the use of other radio technologies in the same frequency band." (Elektronik-Kompendium.de, 2020)

(Other radio technologies in this frequency band may include: Radio remote controls for garage doors, front door bells, home automation systems, etc.).

Since the 2.4 GHz frequency band has been heavily utilized for quite some time, the 802.11n standard was published in 2009, allowing 5 GHz to be used for the first time.

The 5 GHz frequency range is currently still underutilized and, compared to the 2.4 GHz range, offers a higher data transmission rate with a lower maximum extension.

ISO/OSI 7 LAYER MODEL

The ISO/OSI 7-layer model (Figure 44) has become established in network technology. Here, communication between two systems is divided into 7 layers. In each layer, there are one or more protocols that solve a specific subtask of the communication.

- ISO: International Organisation for Standardization
- OSI: Open System Interconnection

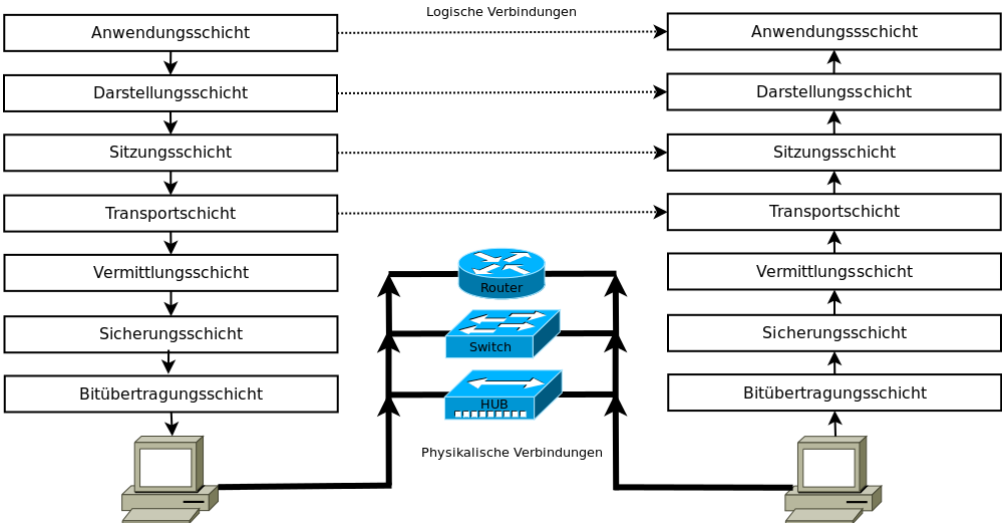

Figure 46: ISO/OSI 7-layer reference model (Baustelle:OSI-Referenzmodell, 2020)

The designation "OSI reference model" already indicates that it is not a standard that defines concrete network protocols. The OSI model only defines the functions of the individual layers and is thus a scheme for defining such standards, for example for the IEEE 802.3 standards presented. Each standard always covers only partial aspects of the OSI model.

The objective in defining the ISO/OSI standard was to create a reference model that enables different technical systems to communicate via different media and technologies and to provide compatibility. To achieve this goal, the OSI model uses a total of seven different layers that are hierarchically based on one another.

Layers one to four are also referred to as connection-oriented layers, since they regulate the actual communication. Layers five to seven are the application-oriented layers.

In most cases, a data communication is started directly from the application layer. The manually executed request is passed on from the application layer to the lower-level presentation layer, and once there, the presentation layer takes care of a syntax defined for the transport. As soon as the presentation layer has fulfilled its specified tasks, it passes the

data on again to the lower-level session layer. This procedure is repeated until the physical layer, where the individual bits are finally sent on their journey to the target system. After the bits arrive at the destination system, the procedure starts all over again in reverse order.

When two remote devices communicate, the individual layers only ever communicate with the same layer of the remote system. This means, for example, that the network layer of system one only ever "talks" to the network layer of system two. Otherwise, the network layer of system one does not communicate with any other layer of system two. The layers therefore basically remain among themselves, since they rely on the other layers to do their work.

If other intermediate stations are involved in the communication, additional passes through the OSI model are added. Network elements and intermediate stations are based on only a limited number of layers, depending on their function. For example, a router operates on layers 1 to 3.

Brief description of the OSI layers:

- 7th layer / application: Functions for applications, as well as data input and output.
- 6th layer / Representation: Conversion of the system-dependent data into an independent format.
- 5th layer / Session: Control of connections and data exchange.
- 4th layer / Transport: Assignment of data packets to an application.
- 3rd layer / switching: routing of data packets to the next node.
- 2nd layer / Securing: Segmenting the packets into frames and adding checksums.
- 1st layer / Bit transmission: Conversion of the bits into a signal suitable for the medium and physical transmission.

The ISO/OSI 7 layer model is very complex and will not be described in detail here.

TCP/IP PROTOCOL

Protocols are required for the exchange of data between two systems. Protocols consist of rules and formats (syntax) that determine the communication behavior (semantics) of the systems.

A protocol

- determines the flow of communication between the systems
- defines the structure of the communication, how the information is exchanged and how the communication is terminated
- assumes certain subtasks of the communication

In today's network technology, the TCP and IP protocols have particularly stood out. Both belong to a protocol family for switching and transporting data packets in networks.

The Transmission Control Protocol (TCP) is located on the transport layer in the OSI model. It is a connection-oriented protocol for application allocation and data flow control. In it, packet loss measures are defined by error handling.

The principle of operation can be described as follows (differentiation into send and receive):

- The sender receives the data packet from an application and splits it into several packets. It then provides these with a header and passes the data packets on to the IP protocol.
- The receiver receives the data packets and reassembles them. It passes the assembled data packet on to the corresponding application.

The Internet Protocol (IP) is located on the switching layer in the OSI model. It is responsible for addressing data packets with IP addresses. The IP address is comparable to the sender or recipient on a letter. IP addresses are divided into network address and host address, comparable with street and house number. The data packets can thus be routed to the correct network and the correct host. A distinction is made between IPV4 (IP version 4) and its successor IPV6 (IP version 6).

Figure 47 shows an example of the structure of an IPV4 data packet.

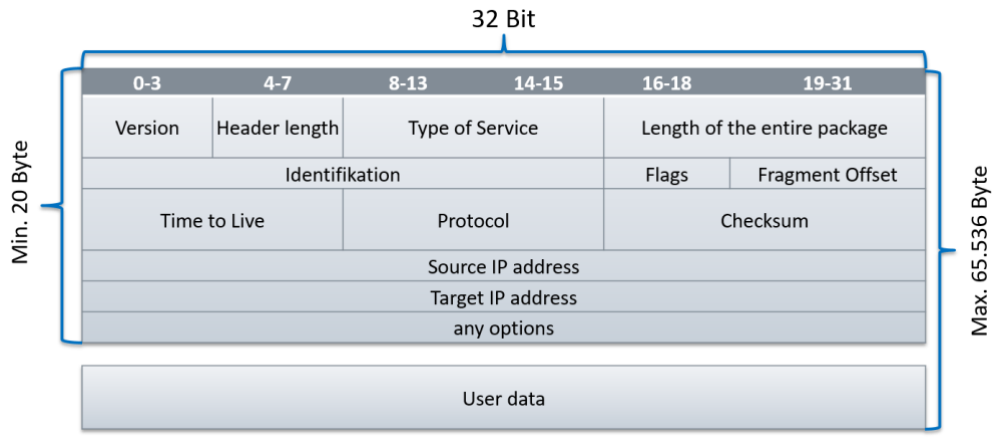

Figure 47: Example IPV4-Header

A distinction is made between header and user data.

The header contains all the information required for processing by the IP protocol (including the recipient and sender addresses). It is divided into several 32-bit blocks.

A data packet may have a maximum size of 65,535 bytes, whereby the header must be at least 20 bytes and the user data at least 8 bytes in size.

HARDWARE

In network technology, a distinction is made between passive and active network components.

The passive network components are mainly the cable routes and connections such as network cables, junction boxes and patch panels.

The active network components are devices that process and distribute the data, such as network cards, switches, access points and routers.

Network cable

Twisted pair cable (copper)

In the LAN, network devices are connected via network cables. These network cables have a special structure, which is shown in Figure XXX.

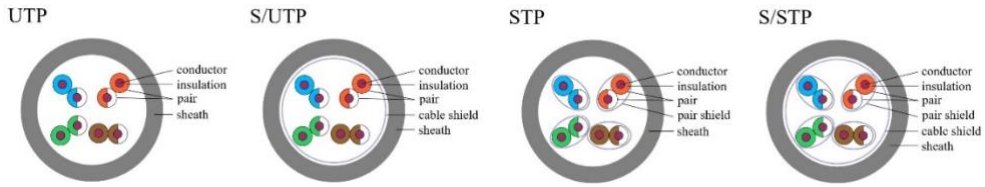

Figure 48: Twisted pair cable (Schwöbel, 2020)

Network cables are twisted pair cables (TP cables). This means that each of the four pairs of wires is twisted with different radii. This twisting is essential due to the high signal frequencies in the cores and the resulting magnetic fields that can lead to interference. In addition to the twisted cores, further shields are present in the structure of the cables. With increasing signal frequency, better shields are required

The designation system for twisted pair cables is standardized according to ISO/IEC-11801 (2002) and corresponds to the form XX/YZZ. Thereby:

XX stands for the overall shielding

- U = without shield (unshielded)
- F = foil shield (coated plastic foil)
- S = braided shield (wire braid)
- SF = braided and foil shield

Y stands for the wire pair shielding

- U = without shield (unshielded)
- F = foil shield (coated plastic foil)
- S = Braided shield (wire braid)

ZZ stands for the stranding type

- TP = Twisted Pair
- QP = Quad Pair

TP cables can be constructed as follows:

- U/UTP - Unscreened/Unshielded twisted pair cable
- S/UTP - Screened/Unshielded twisted pair cable
- U/FTP - Unscreened/Foiled twisted pair cable
- S/FTP - Screened/Foiled twisted pair cable
- F/FTP - Foiled/Foiled twisted pair cable
- SF/FTP - Screened Foiled/Foiled twisted pair cable

TP cables can be used up to a maximum line length of about 100 meters. Fiber optic cables are used for longer cable lengths.

TP cables are standardized differently depending on the country. The international standardization according to ISO/IEC 11801 has become the most widely accepted. The table shows the corresponding standards and designations as well as cable types and the maximum cable bandwidth.

Twisted pair cable - Categories

- EIA/TIA 568 (USA)
- ISO/IEC 11801 (international)
- EN 50173 (Europa)

Table 3: Categories network cable

EIA/TIA 568	ISO/IEC 11801	EN 50173	Type	Bandwidth
Cat. 5	Cat. 5	D	UTP	100 MHz
Cat. 6	Cat. 6	E		250 MHz
Cat. 6A	Cat. 6_A	E_A	STP	500 MHz
-	Cat. 7	F	S/FTP	600 MHz
-	Ca. 7_A	F_A		1000 MHz
-	Cat. 8	G		2000 MHz

Fiber optic cable

Fiber optic cables are used for long cable lengths and fast signal transmission in high-speed LAN and storage area network applications.

The cores consist of plastic, quartz or glass fibers via which light pulses are transmitted. Fiber optic cables are very sensitive to mechanical stress. They must not be bent under any circumstances, as this would destroy the cores.

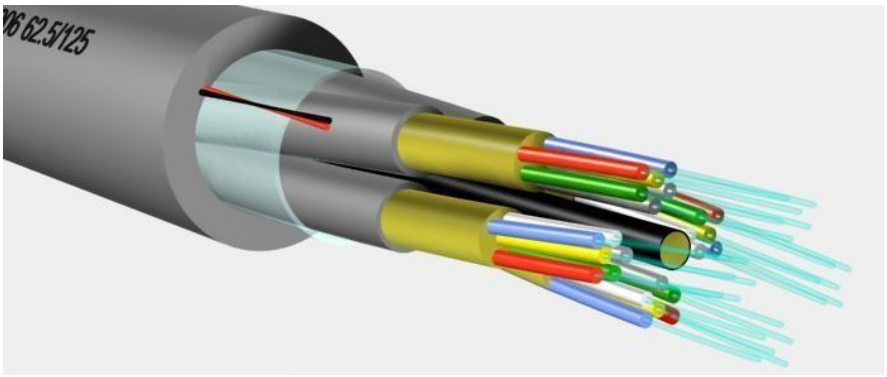

Figure 49: Structure of fibre optic cab (Srleffler, 2020)

A distinction is also made between multimode and singlemode fiber cables. The difference between singlemode and multimode fiber optic cables is mainly in the fiber core diameter, the wavelength, the light source and the bandwidth.

Installation cables and patch cables

The network cables are additionally divided into installation cables and patch cables.

Installation cables are used for permanent installation in the building. Copper cables (TP cables) are connected to a patch panel or a network junction box. Fiber optic cables are connected to an FCT (Fiber Connector Tray) distribution panel.

Patch cables are used for the direct connection of network devices and are therefore equipped with pre-assembled connectors.

The network cabling is structured according to EN 50173-1 and is divided into primary, secondary and tertiary areas.

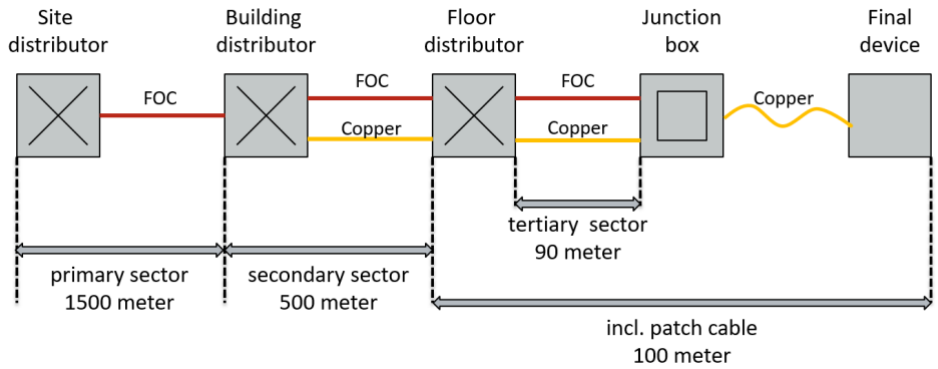

Figure 50: Structured cabling according to EN 50173

Junction box and patch panel

The network socket and the patch panel are the connection points for structured cabling with copper cable.

The patch panel is the (passive) distributor (see star point of the topology) and is usually located in an IT or server room. The network socket is the connection point for the respective end device. The cable between the network socket and patch panel is an installation cable. The cable from the network socket to the end device or from the patch panel to the router or switch is a patch cable.

Cable, socket and patch panel should be of the same category (see Table 3). The following applies: Category overall system = smallest category of a single system.

Network Interface Card

The network interface card (NIC) is the interface between a terminal device (e.g. computer or PLC) and the network cable.

Each network module has a unique address, the MAC address (Media Access Control address), which is used to uniquely identify the device.

Figure 51: NIC (Echoray, 2020)

Hub and Switch

Switches or hubs are coupling elements that connect several hosts in a network. In an Ethernet network based on the star topology, a switch serves as a distributor for the data packets.

Hubs are no longer state of the art and are therefore rarely encountered. Therefore, mainly the switch is considered at this point.

Switches come in different sizes, depending on the maximum number of network cables to be connected. The connections are called ports. The smallest switches have four ports, while large switches can have 48 ports.

A switch can switch direct connections between the connected devices, provided that the ports of the data packet receivers are known to it. If not, the switch broadcasts the data packets to all ports.

When the reply packets come back from the receivers, the switch remembers the MAC addresses of the data packets and the corresponding port, and then sends the data packets only there.

A hub does not remember the addresses of the devices connected to its ports. It always sends all data packets as a broadcast and thus limits the bandwidth of a network.

While a hub limits the bandwidth of the network, when using a switch, the full bandwidth of the end-to-end network connection is available when connecting two hosts.

Layer 2 and Layer 3 Switches

A switch operates on layer 2 or 3 of the OSI model and is therefore called a layer-2 or layer-3 switch.

Layer-2 switches are usually simple and inexpensive models. Their configuration cannot be changed, they have no additional functions and are therefore used in smaller networks.

A layer-3 switch is an extension of the layer-2 switch. They are a combination of router and switch. Layer-3 switches are used in larger networks and can be configured for different functions (e.g. VLAN, security and monitoring).

VLAN = Virtual LAN: Using VLAN, several different networks can be created on one switch. The networks are separated from each other. VLANs are mostly used to separate applications where certain user groups are not allowed to access all networks.

Example: The GA network is (should be) separated from the other networks (e.g. accounting). Possible structure: VLAN1 = general network; VLAN2 = accounting network; VLAN3 = GA network.

Router

A router connects multiple networks using different protocols and architectures. A router is often located at the outer boundaries of a network to connect it to the Internet or another, larger network.

A router uses an internal routing table to decide which path a data packet takes. This is a dynamic process that can accommodate failures and bottlenecks without the intervention of an administrator.

A router has at least two network ports. It operates on the network layer (layer 3) of the OSI layer model.

The task of a router is a complex process that can be divided into 4 steps:

- Determination of the available routes
- Selection of the most suitable route, taking into account various criteria
- Establishing a physical connection to other networks
- Adapting the data packets to the transmission technique (fragmentation)

A router usually has two ports, one for the LAN side and one for the WAN side. Often the ports are labeled LAN and WAN. LAN always means the local network with private IP addresses, while the WAN side indicates the public network.

MODBUS

Modbus is a manufacturer-independent, open (communication) protocol and not a bus.

Modbus has three different operating modes:

- Modbus RTU: (Remote Terminal Unit) Here the data is transmitted directly in binary form to, for example, a PLC. This is the standard Modbus transmission mode.
- Modbus ASCII (= American Standard Code for Information Interchange; is a standard 7-bit character encoding): No binary sequences are transmitted, but ASCII characters. Thus the telegram is directly readable for humans. However, the data rate is lower than with Modbus RTU.
- Modbus TCP/UDP: very similar to Modbus RTU, but TCP/IP data packets are transmitted.

The basis of Modbus RTU and ASCII is the RS485 bus. Modbus RTU is also used as an interface between the automation and field level.

Modbus TCP is used in the TCP/IP network and is mostly used as an interface between management and automation level and for communication between automation level devices.

Due to its stability and ease of implementation, Mobus is still a widely used protocol today, having found its way into building automation via manufacturing and process automation.

The data exchange in a Modbus takes place via the master/slave procedure.

"In this procedure, the bus control unit, the so-called master, establishes the connection to the passive participant, the slave. The slave responds immediately to a data request from the master (immediate response) (see figure).

The master usually establishes the connection to each slave cyclically (polling). This means that an up-to-date image of the process to be controlled is always stored in the master. Priorities can be assigned by polling some slaves several times within a cycle.

This method has the advantage that the bus connection of the slaves is very simple and therefore cost-effective, since all the required intelligence is implemented in the master. The times required when data must be exchanged between two slaves can be problematic. In this case, the master sends a data request to the signaling slave, which responds immediately. This information must be processed in the master or in the controller and transmitted to the receiving slave.

This means that in extreme cases the cycle time is required for both the data request and the transmission. In addition, the processing time by the master/controller must be taken into account. Thus, the duration of this data transmission may be many times longer than the cycle time." (Gerhard Schnell, 2019)

Modbus does not require any additional software for commissioning and parameterization. Data is exchanged via object types in the Modbus protocol. These basic object types are:

- Discrete Inputs = digital inputs of 1 bit length.
- Coils = Digital outputs of 1 bit length
- Input Register = Analog inputs of 16 bit length
- Holding Register = analog outputs of 16 bit length

In addition, one or more functions are defined for each basic type.

OPC

OPC (Open Platform Communications) is the interoperability standard for secure and reliable data exchange in industrial automation and other industries. It is platform-independent and ensures the seamless flow of information between devices from different manufacturers. The OPC Foundation is responsible for the development and maintenance of this standard.

The OPC standard is a set of specifications developed by industry vendors, end users and software developers. These specifications define the interface between clients and servers, and between servers and servers, including access to real-time data, monitoring of alarms and events, access to historical data, and other applications.

When the standard was first published in 1996, its purpose was to abstract PLC-specific protocols (such as Modbus, Profibus, etc.) into a standardized interface that would allow HMI/SCADA systems to communicate with a "middleman" that would convert generic OPC read/write requests into device-specific requests and vice versa.

Originally, the OPC standard was limited to the Windows operating system. The acronym OPC was therefore derived from OLE (Object Linking and Embedding) for process control. These specifications, now known as OPC Classic, have been adopted across a wide range of industries including manufacturing, building automation, oil and gas, renewable energy, and utilities.

With the introduction of service-oriented architectures in manufacturing systems came new challenges in security and data modeling. The OPC Foundation developed the OPC UA specifications to address these requirements while providing a feature-rich, technologically open platform architecture that is future-proof, scalable, and extensible.

Advantages of the new OPC UA specification are:

- Platform independent (e.g. RaspberryPi).
- OPC servers can now be operated on PLC controllers, Windows computers are no longer necessary
- Caching of data in the server: Interruption of the communication link does not lead to data loss
- "real" security
- Connection to ERP systems as well as to the cloud

PROFIBUS AND PROFINET

Profibus and Profinet are protocols that have their origin and main application in industrial automation. They are rather rarely used in building automation.

Profibus was developed by the Siemens company and is used for communication between PLC systems and the components of the automation and field level.

Profinet is the further development of Profibus on Ethernet basis. With Profinet, higher transmission rates and diagnostic functions are possible.

BACNET

BACnet stands for Building Automation and Control Network and is a data protocol for the exchange of data and the networking of various systems and products in building automation.

"BACnet" (Building Automation and Control Network) is the communication protocol for building automation developed by the American Society of Heating, Refrigeration and Air-Conditioning Engineers (ASHRAE) and standardized in 1995, which allows devices and systems to exchange information with each other. The common language BACnet is used worldwide in numerous building automation systems and has also been standardized as DIN EN ISO 16484-5 since 2003.

BACnet arose from the need to be able to address the most diverse automation and control components in a building with a uniform, standardized data communication protocol. This is intended to ensure desirable goals such as interoperability and manufacturer independence.

Before the introduction of BACnet, building automation was often characterized by proprietary technologies from the various manufacturers. For example, the heating control system of manufacturer A could not communicate with the control center software of manufacturer B. The individual trades, such as air conditioning, ventilation, lighting or

hazard alarm technology, were often planned independently of each other and provided without suitable interfaces for the mutual exchange of information and for connection to a common control center. This resulted in considerable disadvantages for the building owner. Either he had to do without uniform control and monitoring of all automation equipment and the resulting synergies, or he had to commit himself to a single manufacturer and purchase a complete solution from him.

BACnet offers an open and manufacturer-independent communication protocol that enables the mixed operation of components from different manufacturers and thus promises more market transparency and competition." (Hermann Merz, 2016)

BACnet is now recognized worldwide and is represented in Europe by the BIG EU (BACnet Interest Group Europe, European trade association for the application of the global BACnet standard ISO 16484-5).

The BACnet standard, as well as much further information can be obtained from the website http://www.bacnet.org/.

The current BACnet document (2019) is structured as follows and consists of 1157 pages in total:

- 24 chapters with 693 pages
- ANNEX A-S with 304 pages
- Addendum ad, ae, af with 160 pages
- Draft: Addendum i, aa, ai, aj, ak, al, am, an

In May 2020, there were 1232 manufacturers of BACnet products worldwide. A vendor-ID is assigned to each manufacturer whitch can be retrieved via http://www.bacnet.org/VendorID/BACnet%20Vendor%20IDs.htm.

Manufacturers of BACnet products can prove that their devices comply with the BACnet standard ISO 16484-5 by performing conformance tests at a recognized and accredited testing laboratory. Tests are performed uniformly according to the BTL (BACnet Testing Laboratory) Test Plan and the BACnet test standard ISO 16484-6.

The Protocol Implementation Conformance Statement (PICS) describes only the properties of the BACnet device (e.g. transmission media, profile, supported types of objects, BIBBs, character sets etc.).

BACnet test labs:

- BTL Lab Atlanta/USA
- DIAL GmbH Lüdenscheid / Germany
- MBS GmbH Krefeld / Germany
- iHomeLab Horw/Switzerland

A further certification is offered by AMEV (Arbeitskreis Maschinen- und Elektrotechnik staatlicher und kommunaler Verwaltungen). The AMEV certificate is available in two versions:

- Profile A with simple BACnet functions
- Profile B with extended BACnet functions

The AMEV Testat confirms a certain functional range of a BACnet device and certifies only the hardware (with a software/firmware status). It is not a certification of service providers or system integrators.

BACnet products (hardware and software) are often tested for interoperability at so-called Blugfests (or Plugtest). At these plugfests, the manufacturers and developers of the products come together and test their own products with those of other manufacturers according to the BACnet standard.

Data transmission

BACnet uses two standards for data transmission:

- BACnet IP; transmission via Ethernet
- BACnet MS/TP; transmission via RS485 (MS/TP = Master-Slave/Token-Passing

BACnet IP is often used for communication between the management and automation level as well as for communication between different controllers (e.g. PLC, heating controller etc.). For BACnet IP, the individual devices must have a network connection for communication via the TCP/IP network. In addition to the IP address, each BACnet IP device receives a BACnet ID.

BACnet MS/TP is a simple and cost-effective transmission technology, which is particularly suitable for smaller controllers and operating elements (left picture) with low data transmission rate requirements.

Both transmission standards can be interconnected via special BACnet routers. The data transmission with BACnet IP is extremely efficient and reduces the network load compared to e.g. the Modbus.

BACnet Terms

Native: A device that can be implemented directly in a BACnet environment without using a gateway

Profil: Defines a special class of devices, means which BIBBs are generally supported (B-BC= BACnet Building Controller).

BIBBs (BACnet Interoperability Building Block): Defines certain functions. e.g.: "The device processes messages about alarms and other events" and whether this function acts as client or server.

PICS (Protocol Implementation Conformance Statement): Document that describes the properties of a BACnet device (e.g. transmission medium, profile, supported object types, BIBBs, character sets).

Objects and properties

Interoperability between manufacturers, system integrators and customers is modeled in BACnet by means of a collection of objects.

A BACnet device is described exclusively via the objects and the object properties as well as the services with which the objects and object properties communicate with each other.

An object is an abstract data structure in which information is stored as so-called object properties. In the simplest case, an object can also be imagined as a table. The information in an object can be e.g. data of a connected sensor. In addition to the actual measured value, a lot of other information are provided.

Table 4: Properties of the Analog Input Object Type (EN ISO 16484-5, 2017)

Property Identifier	Property Datatype	Conformance Code
Object_Identifier	BACnetObjectIdentifier	R
Object_Name	CharacterString	R
Object_Type	BACnetObjectType	R
Present_Value	REAL	R
Description	CharacterString	O
Device_Type	CharacterString	O
Status_Flags	BACnetStatusFlags	R
Event_State	BACnetEventState	R
Reliability	BACnetReliability	O
Out_Of_Service	BOOLEAN	R
Update_Interval	Unsigned	O

Units	BACnetEngineeringUnits	R
Min_Pres_Value	REAL	O
Max_Pres_Value	REAL	O
Resolution	REAL	O
COV_Increment	REAL	O
Time_Delay	Unsigned	O
Notification_Class	Unsigned	O
High_Limit	REAL	O
Low_Limit	REAL	O
Deadband	REAL	O
Limit_Enable	BACnetLimitEnable	O
Event_Enable	BACnetEventTransitionBits	O
Acked_Transitions	BACnetEventTransitionBits	O
Notify_Type	BACnetNotifyType	O
Event_Time_Stamps	BACnetARRAY[3] of BACnetTimeStamp	O
Event_Message_Texts	BACnetARRAY[3] of CharacterString	O
Event_Message_Texts_Config	BACnetARRAY[3] of CharacterString	O
Event_Detection_Enable	BOOLEAN	O
Event_Algorithm_Inhibit_Ref	BACnetObjectPropertyReference	O
Event_Algorithm_Inhibit	BOOLEAN	O
Time_Delay_Normal	Unsigned	O
Reliability_Evaluation_Inhibit	BOOLEAN	O
Property_List	BACnetARRAY[N] of BACnetPropertyIdentifier	R
Interface_Value	BACnetOptionalREAL	O
Fault_High_Limit	REAL	O[8]
Fault_Low_Limit	REAL	O
Tags	BACnetARRAY[N] of BACnetNameValue	O
Profile_Location	CharacterString	O
Profile_Name	CharacterString	O

In BACnet there are not only the object properties shown in the table, but further various data contents with different meanings. Some of the properties provided in the objects are optional.

A distinction is therefore made between mandatory properties, which must be readable (R) or writeable and readable (W), and optional properties (O) (see third column of the table). The optional properties can be combined with R and W if necessary. If the predefined objects or properties are not sufficient, non-standard extensions can be introduced. This

makes it possible to follow technical developments that have not yet gone through the standardization process.

The BACnet objects represent the basis for the building automation functions. The BACnet standard defines object types that cover typical building automation requirements. In addition to simple analog and digital input/output objects, these are also more complicated objects for the control of systems, for operating calendars and for trend recordings. BACnet defines 61 standard types (ISO 16484-5:2017) of objects. Tabelle 5 gives a list of 18 common standard objects with an example of use.

Table 5: Standard BACnet Objects (Swan, 2021)

OBJECT	EXAMPLE OF USE
Analog Input	Sensor input
Analog Output	Control output
Analog Value	Setpoint or other analog control system parameter
Binary Input	Switch input
Binary Output	Relay output
Binary Value	Binary (digital) control system parameter
Calendar	Defines a list of dates, such as holidays or special events, for scheduling.
Command	Writes multiple values to multiple objects in multiple devices to accomplish a specific purpose, such as day-mode to night-mode, or emergency mode.
Device	Properties tell what objects and services the device supports, and other device-specific information such as vendor, firmware revision, etc.
Event Enrollment	Describes an event that might be an error condition (e.g., "Input out of range") or an alarm that other devices to know about. It can directly tell one device or use a Notification Class object to tell multiple devices.
File	Allows read and write access to data files supported by the device.
Group	Provides access to multiple properties of multiple objects in a read single operation.
Loop	Provides standardized access to a "control loop."
Multi-state Input	Represents the status of a multiple-state process, such as a refrigerator's On, Off, and Defrost cycles.
Multi-state Output	Represents the desired state of a multiple-state process (such as It's Time to Cool, It's Cold Enough and it's Time to Defrost).
Notification Class	Contains a list of devices to be informed if an Event Enrollment object determines that a warning or alarm message needs to be sent.
Program	Allows a program running in the device to be started, stopped, loaded and unloaded, and reports the present status of the program.
Schedule	Defines a weekly schedule of operations (performed by writing to specified list of objects with exceptions such as holidays. Can use a Calendar object for the exceptions.

Services

Communication between devices takes place by means of services that access the objects. A simple case would be, for example, the query of a temperature sensor via the associated analog input object. The querying station uses the ReadProperty service to get Present_Value of an object with a certain Object_Identifier as address. With an additional numbering of the messages the allocation of the answers to possibly several inquiries is ensured. The service ReadProperty belongs to the confirmed services, which require a response in contrast to unconfirmed services.

The services available with BACnet are divided into the following five groups:

- Object access services (see Tabelle 6)
- Alarm and event services
- Device and network management services
- File access services
- Virtual terminal services

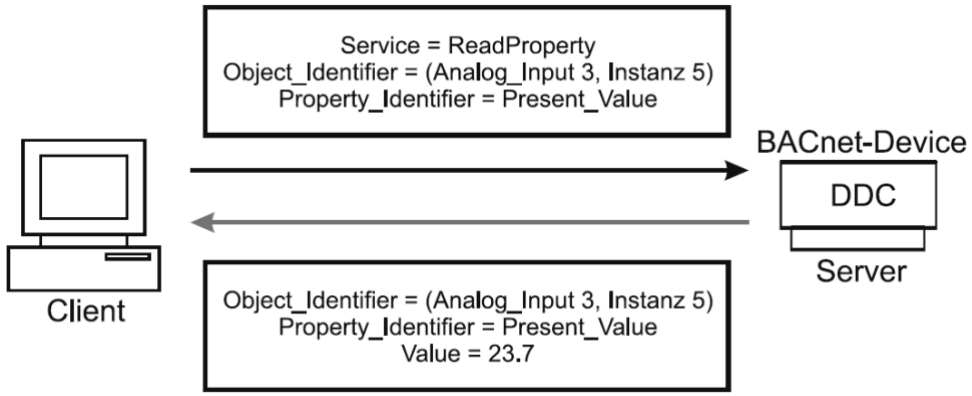

Figure 52: Example for the query of a BACnet device (Hermann Merz, 2016)

The Object Access Services provide the means to read, modify and write Properties, and to add and delete Objects.

Table 6: Object Access Services

SERVICE	DESCRIPTION
AddListElement	Adds one or more items to a property that is a list
RemoveListElement	Removes one or more items from a property that is a list
CreateObject	Used to create a new instance of an object in the serving device
DeleteObject	Used to delete a particular object in the serving device
ReadProperty	Returns a value of one property of one object
ReadPropertyConditional	Returns the values of multiple properties in multiple objects
ReadPropertyMultiple	Returns the values of multiple properties of multiple objects
WriteProperty	Writes a value to one property of one object
WritePropertyMultiple	Writes values to multiple properties of multiple objects

Device profiles

Each BACnet device is assigned a defined device profile, depending on its function and application.

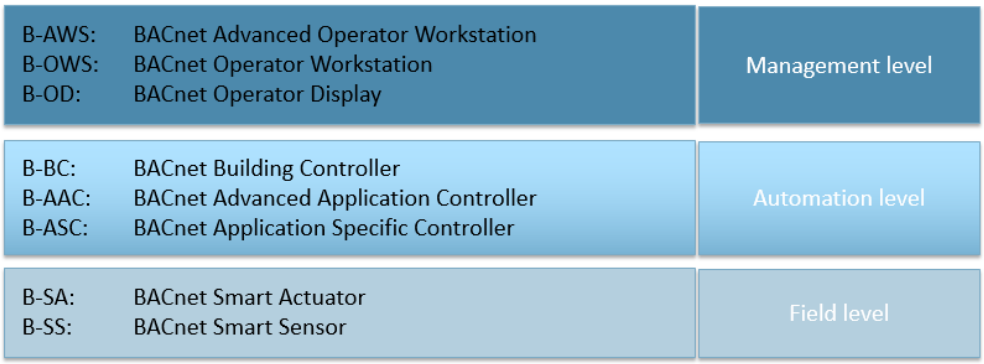

Figure 53: BACnet - Device profiles

Each device profile represents a defined subset of the BIBBS, which can be extended by the manufacturer with additional services.

Interoperability area (IOB's)

The BACnet standard defines a large number of functions for building automation, which are divided into five so-called BACnet interoperability areas (IOB) for better comprehensibility and structuring. For example, there is an IOB that deals with all the necessary functions for alarm and event management, or an IOB for schedules. Each IOB is in turn assigned several interoperability building blocks, so-called BIBBs (BACnet Interoperability Building Blocks – see 4.2.4.6), are assigned to each IOB.

The five IOBs describe BACnet services that are important for the operation of BACnet systems:

- DS (data sharing)
- AE (alarm and event management)
- SCHED (scheduling)
- T (trending)
- DM (device and networkmanagement)

Interoperability Building Blocks (BIBBs)

The BIBBS are a collection of BACnet services within an interoperability area (IOB). Thereby a functionality (client/server) is assigned to these services. The Abbildung 22 shows an example of a BIBB with the IOB "DS (data exchange)", the service "RP (read)" and the functionality "A (client)".

The functionality specifies who is the "requester (=client)" and who is the "responder (=server)".

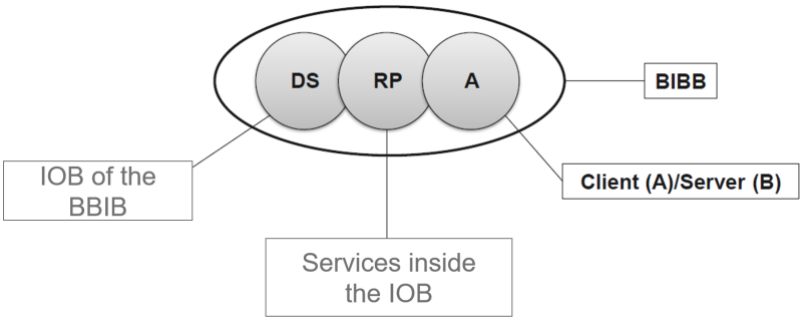

Figure 54: General example BIIB

Example for reading a value

A temperature value is to be read from a sensor connected to a PLC.

The client makes a request to the server for a specific property. The server reads the value from the sensor and replies to the client with the corresponding value.

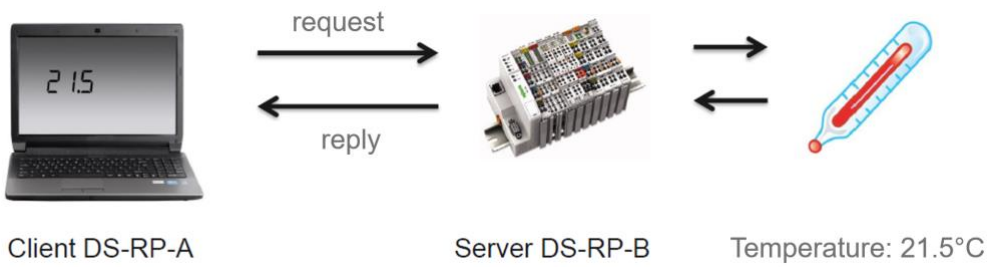

Figure 55: BIBB example for reading a value

For the data exchange, one device must act as client (A), and the other as server (B). This means that in order to be able to perform this request, the client must have implemented the BIBB DS-RP-A. The server, on the other hand, must support the BIBB DS-RP-B so that a response is possible at all.

Example for writing a value

The brightness of a light connected to a PLC is to be changed.

The client requests the server to write a supplied value (brightness) into a specific property. The server allows to change a property and executes the request of DS-WP-A. (WP = write property)

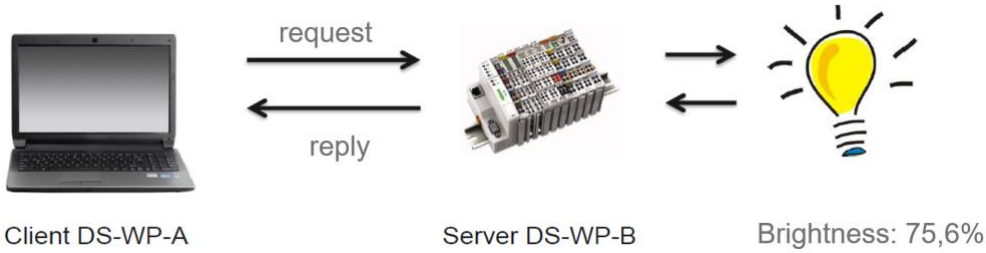

Figure 56: BIBB example for writing a value

The client must have the BBIB DC-WP-A integrated, the server the BBIB DS-WP-B.

Problem areas

However, BACnet does not only bring advantages. Due to the complexity and the abundance of information to be processed, different problem areas can arise during the life phases of a BACnet system.

One problem area is certainly the constant further development of BACnet. Thus, since the Bacnet Version 1 Revision2 from 2001 to Version 1 Revision 19 on 2016, a total of 6 valid versions have appeared.

Another problem area is the increasing number of object types as more and more trades are integrated into BACnet. This leads to the fact that there is a certain know-how in the BA industry, but the manufacturers are specialized in their own products. An overall view is hardly possible.

When planning a BACnet system, the budget must be adjusted in the tendering process, since BACnet engineering is in some places more expensive than classic engineering in the BA

1.7 IT SECURITY AND STANDARDIZED "OPEN" COMMUNICATION PROTOCOLS

IT SECURITY

Nowadays, more and more devices are being connected to a network. This connectivity also affects more and more to the building automation. While a few years ago most devices such as PLC or DDC were not connected to a (TCP/IP) network, today most (new) devices are connected via modern networks. At that time there was no (big) danger of an attack on these devices, because they were not accessible from outside the building. This has changed until today. In the meantime, there is a high risk of attacks on control systems in important plants and buildings. Therefore, protection of these systems has become more and more important and must also be considered in building automation.

CHECK YOUR SYSTEMS (SHODAN)

Before we start with the information about IT-Secutity, let's take a look at an interesting tool that allows us to get information of possible weaknesses in systems that are connected to the Internet.

Shodan (https://www.shodan.io/) is the world's first search engine for devices connected to the Internet.

Shodan can be used to find devices and systems that are permanently connected to the Internet. Shodan is also referred to as a search engine for the Internet of Things (IoT). It searches the Internet for open TCP/IP ports and allows filtering the found systems according to certain terms and criteria. The search engine can be used for security analyses or hacking. Devices and systems that can be found include surveillance cameras, servers, smart home systems, industrial controllers, traffic light and traffic control systems, and various network components that are also used in GA systems.

With Shodan you can search specifically for network protocols. If you want to perform a search, you need to register for free or log in using your Google, Twitter, Facebook or Windows Live account. With the free search, you only have a certain number of searches available per day.

Try it out. Go to https://www.shodan.io/explore/category/industrial-control-systems, and you'll be redirected to the Industrial Control Systems search page (see Figure 57). You should be familiar with a protocol or two that you can search for from the previous lecture sessions.

We will further explain the search and the corresponding results on the next three slides. Please note that when you search, the search results may look different because Shodan's database is constantly changing.

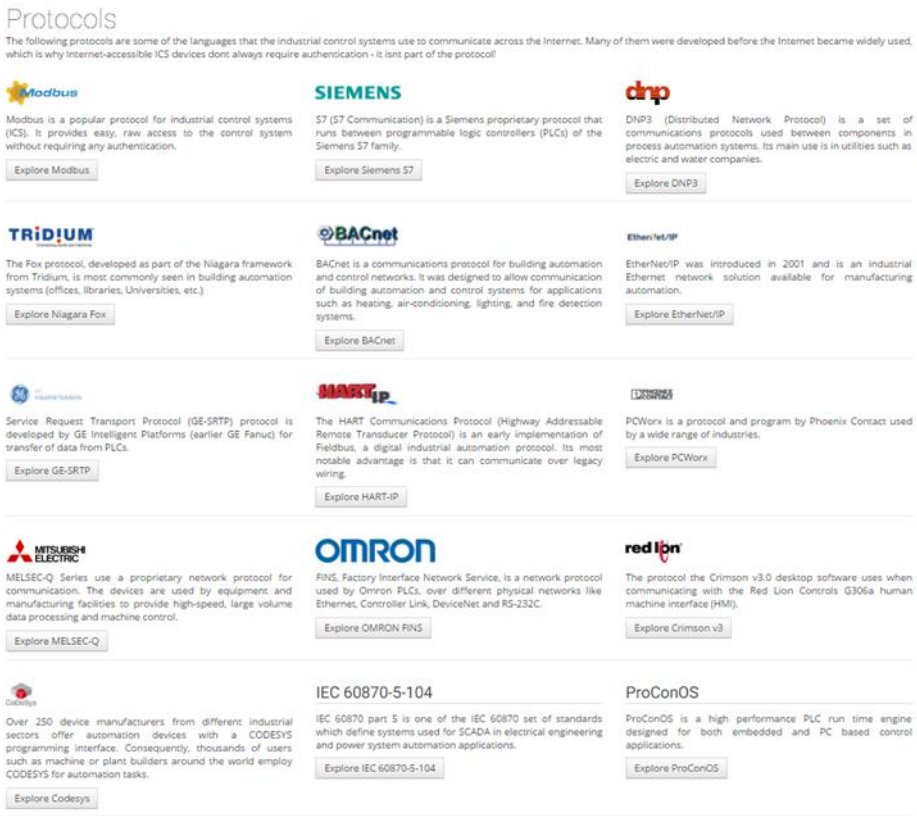

Figure 57: Sceenshot from Shodan search for industrial-control-systems

As an example, a search for BACnet devices in Germany was performed.

If you click on BACnet on the search page, SHODAN will automatically search for devices with TCP/IP port 47808, which is the default network port for BACnet.

You can also filter the results by a country. In this example, Germany was selected. If the searched country is not included in the list (left side - TOP Countries), you can select the country manually with the additional search entry "country: "DE"".

As a result, this search listed 254 BACnet devices that are connected to the Internet (see Figure 58). You can see the IP addresses of the devices and the companies where the devices are connected.

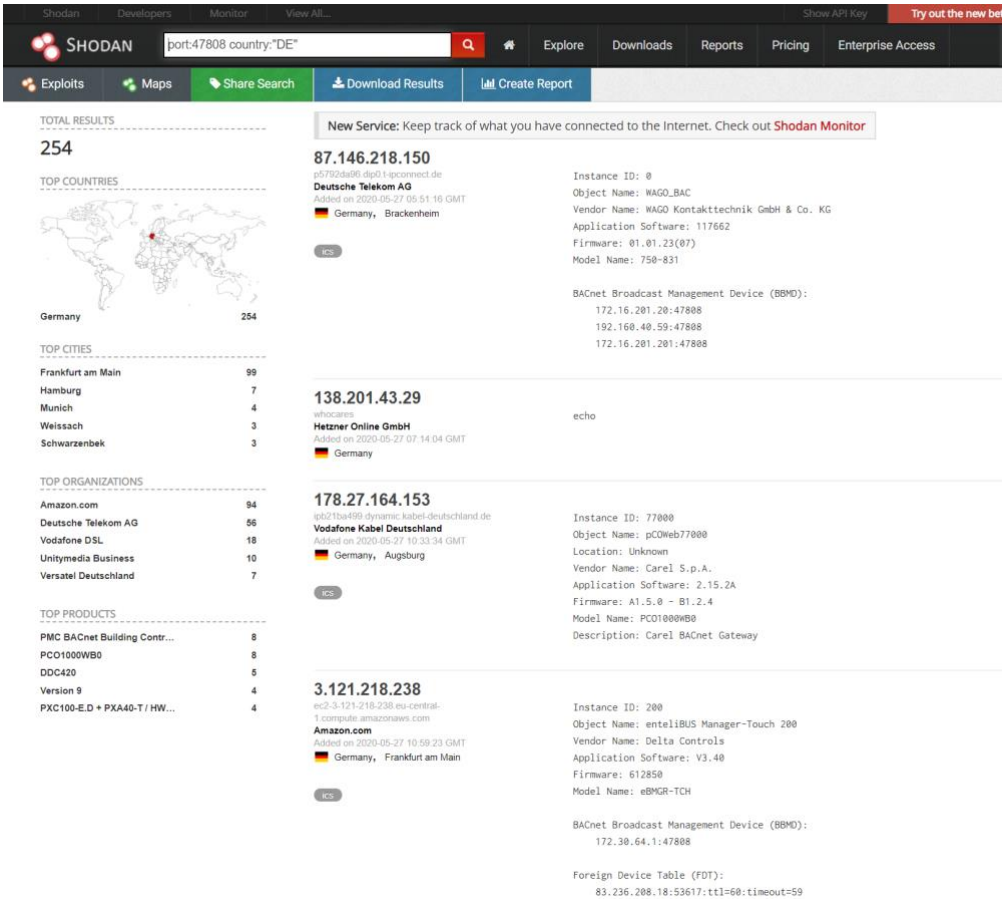

Figure 58: Shodan search for BACnet devices in Germany

Let's take a closer look at the first search result (see Figure 59). You can see on the right side that this is a device from the WAGO company. You can see the application software version (117662), the firmware version (01.01.23(07)), the model name (750-831) and the IP addresses of the device.

A hacker has thus already been able to gather a lot of (free) information to target a device. He can, since he knows e.g. the firmware, launch targeted attacks on vulnerabilities of the device. But you as a consumer can also use this tool to check whether you have a possible security leak in your system.

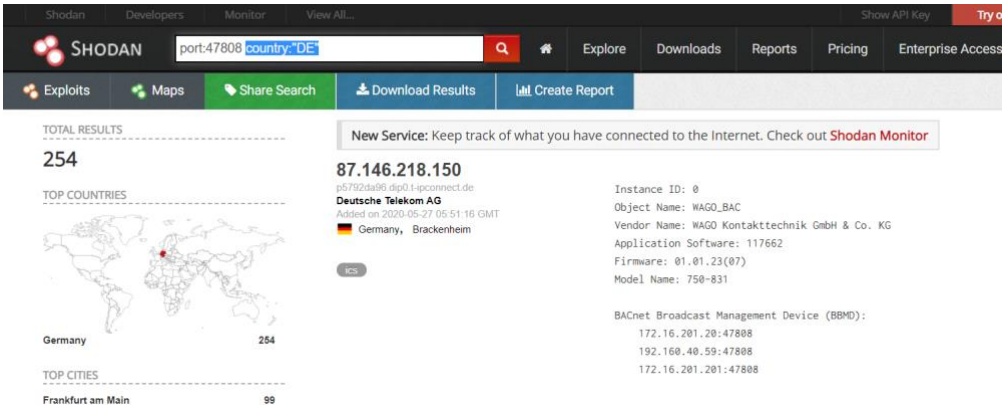

Figure 59: Shodan search example

THE CHALLENGE OF ETHERNET-BASED NETWORKS IN BA

Building automation in the IT environment is increasingly threatened by damage scenarios such as sabotage, spying and the installation of malware. If unprotected, this can lead to data manipulation, data loss and the failure of building automation with consequences such as personal injury, restriction of business operations (e.g., loss of production, unusability of the building) or financial losses.

However, processes that focus overall on security against network attacks from external and internal sources are few and far between. The reason for this is that in building technology, largely unprotected systems encounter a complex IT world.

However, the connection of the BAC with the technical facilities of a building (HVAC systems, lighting, access control, fire doors, etc.) results in an expanded dimension in the consequences of this threat compared to general IT. Not "only" data can be manipulated or changed, an unwanted access can have an impact on the security-relevant technical equipment of the building. If there is criminal intent, the consequences can be correspondingly severe.

The significance of the threat depends heavily on the type and use of the affected building. Not all buildings are equally interesting for attacks and equally sensitive to their consequences. BA systems control and regulate critical infrastructures, among other things, which can cause major economic damage or personal injury in the event of a cyber attack.

Security precautions must therefore be adapted to the risk. A project-specific risk analysis is essential in any case.

Ethernet-based infrastructure offers great advantages for BA networks. These include:

- Interfaces to BA systems are standard in IT hardware.
- Information is available to multiple systems / applications.
- Large infrastructures can be aggregated using WAN standards.

In terms of security, however, this results in the following disadvantages:

- Access to the BA infrastructure is (too) easy to establish Security risk.
- Standard protocols also give unauthorized persons the opportunity to manipulate security risk.
- In the worst case, IT and BAC have a negative impact on each other. Security standards are higher in IT while BAC prefers open systems.

This results in a conflict of objectives between the convenience and security of a BAC system (see Figure 60).

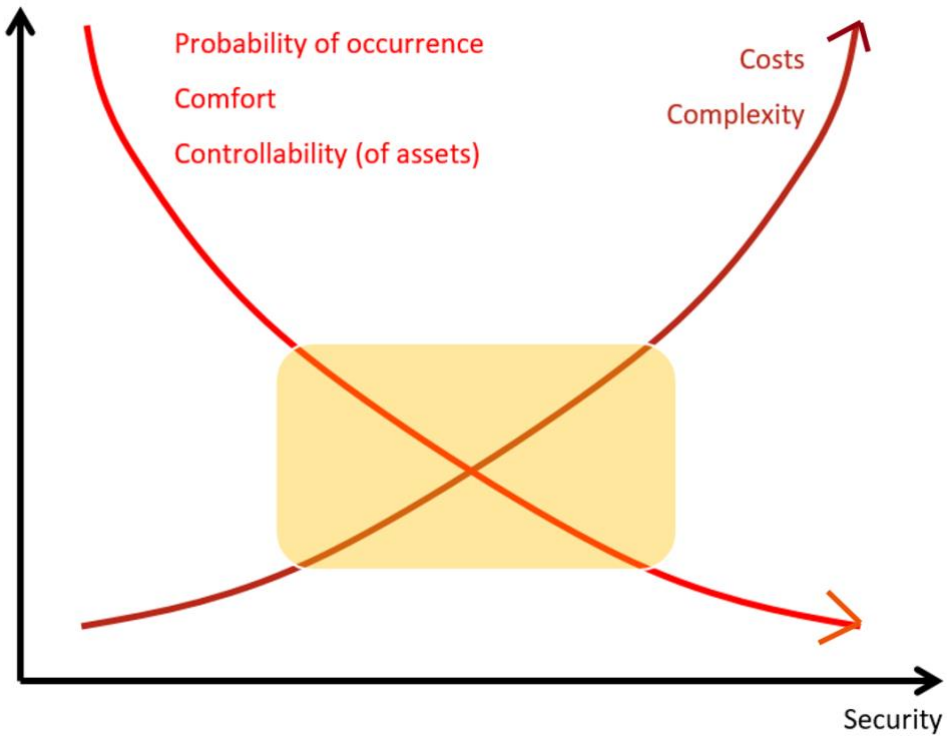

Figure 60: conflict of objectives between the convenience and security of a BAC system

In summary, this can be described as follows:

- The higher the security requirements, the greater the expense and complexity.
- Increasing complexity may be associated with losses in comfort and controllability.
- A balance must be found that is within the legal requirements and yet keeps the BAC system usable and controllable.

Which threats from the IT environment can also pose threats to BAC?

A distinction is made between two threat scenarios:

- Damage or threats within the network
    - Access to the BAC system for undirected or unconscious manipulation
    - Tapping of data and information by employees (consciously and unconsciously)
    - Deliberate disruption or manipulation of the system or equipment
    - Use of default passwords
- Damage or threats from outside the network
    - Poorly configured firewall and thus unauthorized access from the outside
    - Service notebook or USB stick of a technician (thus, e.g., installing malware)
    - Carelessly configured remote access of a system part (see slide 20 ff.)
    - UPnP (Universal Plug and Play) for manufacturer-independent control of devices (see)

A shell model (see Figure 61) is often used to better analyze vulnerabilities. Based on this model, guidelines for the individual areas regarding IT security should be defined.

Example:

- There must be no network interfaces on the building shell (no physical access from the outside).
- The physical network is divided into several networks (with access rights according to the application (e.g. BAC only)
- The BAC is only integrated in one VLAN (other applications and users do not have access to this VLAN)
- The control cabinets are protected from access (no access to the technical room for unauthorized personnel)
- The PLC is protected (e.g. by a password)
- The sensors and actuators have a tamper contact (an alarm is triggered if the sensors are tampered with)

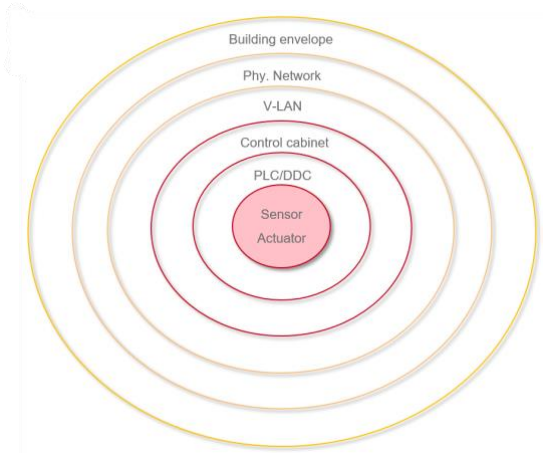

Figure 61: Shell model in BAC

PROBLEM FIELD: PASSWORDS

A big problem in IT security (not only in BAC) are passwords.

Users often use a password that is too simple. Also, the default passwords of technical systems are often not changed. This is a risk, because these passwords can be cracked within seconds by special programs.

- As a general rule, the longer the better.
- A good password should be at least eight characters long. With WLAN encryption methods such as WPA2, for example, the password should be at least 20 characters long. Here, so-called offline attacks are possible, which also work without a standing network connection.
- As a rule, all available characters can be used for a password, for example upper and lower case letters, digits and special characters (space, ?!%+...).
- Not suitable as passwords are names of family members, the pet, the best friend, the favorite star, birth dates and so on. The complete password should not be found in dictionaries, if possible. It should also not consist of common variants and repetition or keyboard patterns such as "asdfgh" or "1234abcd".
- Adding simple digits to the end of the password or using one of the common special characters $! ? # at the beginning or end of an otherwise simple password is not recommended.
- Use a password manager to manage your different passwords well. - and your strong password to secure it. This way you only have to remember one good password and you can still use very strong passwords that are different everywhere.

A strong password can be "shorter and complex" or "long and simple". But how long and how complex should it be at least? The following examples provide orientation:

A password is strong if it is, for example:

- 8 to 12 characters long and three character types are used
- 20 to 25 characters long and two character types are used (for example, a sequence of words)
- characters long, two character types are used, and it is also secured by multi-factor authentication (for example, a fingerprint, app confirmation, or PIN). This is generally recommended, but cannot be used everywhere.

PROBLEM FIELD: UPNP

UPnP (Universal Plug and Play) uses the Internet Gateway Device (IGD) protocol to provide an easy way for the user to instruct routers to open ports and forward requests from the Internet to a computer (or device) that is connected to the Internet.

UPnP should only be enabled on network interfaces for the local network and should not be accessible from the Internet. In January 2013, the security company Rapid7 from Boston announced that they had been searching for UPnP devices on the Internet in a 6-month project. They found 6,900 products from 1,500 manufacturers among 81 million IP addresses that responded to UPnP requests from the Internet. 80% of the devices are home routers for Internet access, other devices are printers, webcams and surveillance cameras. The UPnP protocol can be used to access or manipulate these devices.

BAC PROTOCOLS AND IT SECURITY

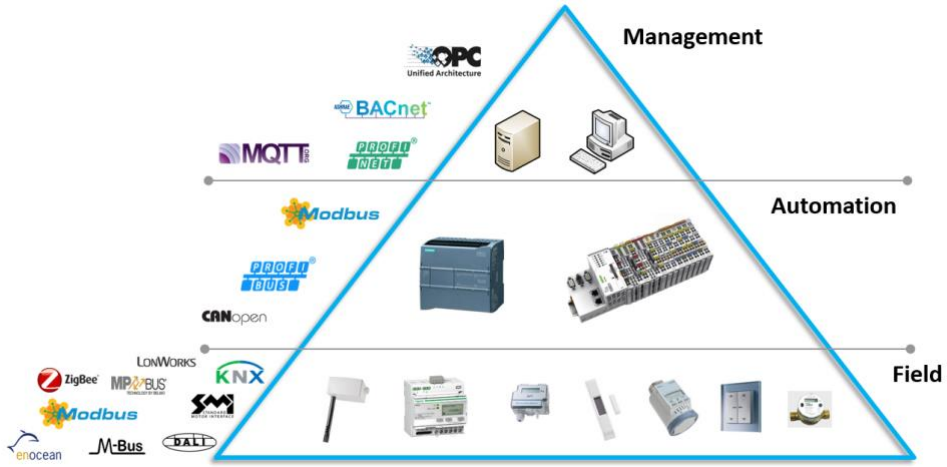

Figure 62: Automation pyramid with protocols and bussystems

MODBUS

Modbus has no special security mechanisms. Neither a password nor a certificate is required. If one is connected to the corresponding network, one can listen to the communication in the Modbus with free tools. Since Modbus communicates via the TCP/IP port, it is possible to block this port for all other network participants (e.g. via a firewall).

BACNET

Like Modbus, BACnet has no security mechanisms. If one is connected to the network, it is possible to access and manipulate the whole BACnet system with free tools.

Due to the large number of tools used by BACnet, it is almost impossible to seal it off using a firewall. Therefore it is even more important that the corresponding network (Ethernet) is protected (e.g. by VLAN, certificates or strong passwords).

OPC

The classic OPC does not have any security mechanisms either. OPC-UA can be protected by certificates.

KNX

The classic KNX does not know any security mechanisms like passwords or certificates, therefore new installations should be secured with KNX Secure.

An access to the KNX bus via e.g. the twisted pair cabling is possible at many places in a building. E.g. simply remove the cover at a switch and connect a notebook with the KNX.TP using an adapter.

To close these security gaps, KNX Secure was introduced in 2016. KNX Secure enables a secure connection between the participants in an IP network (KNX IP Secure) and the participants in the twisted pair bus (KNX DATA Security) (see next slides).

KNX IP secure

KNX IP Secure allows messages sent by KNX devices to be authenticated and encrypted in IP networks. This ensures that KNX tunneling or routing messages cannot be read or manipulated on the network level.

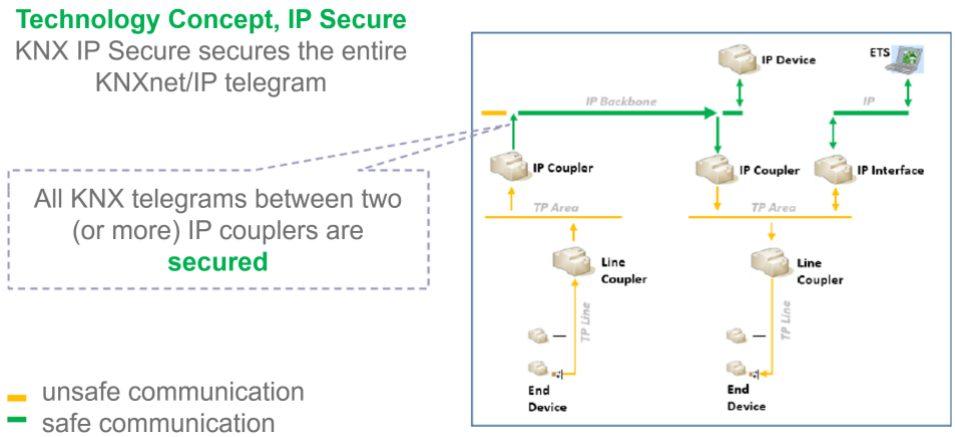

Figure 63: KNX IP secure

With KNX IP Secure, a secured connection is established in the following way:

- Both client and server generate a combination of an individual public/private key. This is called asymmetric encryption.
- The client sends the server its public key in clear text.
- The server responds with its public key in plaintext and appends the result of the following calculation: it calculates the XOR value of its public key, encrypts this with the device code (to authenticate to the client), and encrypts this a second time with the calculated session key. The device authentication key is either assigned by the ETS during configuration or is the tool key. If a visualization wants

to establish a secure connection with the respective server, it must be provided with the device authentication key.

- The client performs the same XOR operation, but authorizes itself by encrypting first with the server's password and second with the session key. It should be noted in the operation that the encryption algorithm used (Diffie Hellmann) ensures that the session key of the client and the server are identical. If a visualization wants to establish a secured connection with the respective server, it must be provided with the passwords of the server.

For encryption of KNX network traffic, KNX devices allow encryption according to AES-128 CCM algorithms using a symmetric key. AES 128 is considered a very secure encryption method

KNX data secure

KNX Data Security ensures that selected messages sent out by KNX devices are authenticated and/or encrypted independently of the KNX medium.

KNX Data Secure devices use a longer KNX telegram format for the transmission of the authenticated and encrypted data. However, this has no effect on the response speed of the devices. With KNX Data Security devices are protected in the following way:

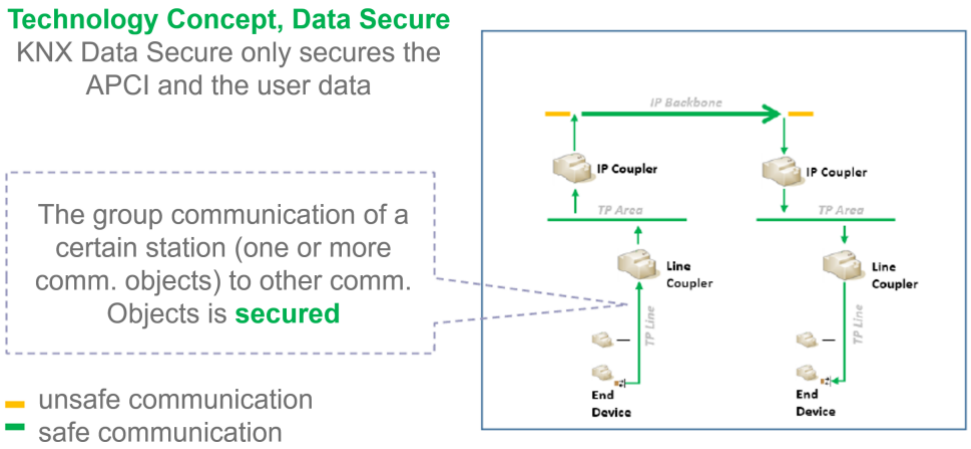

Figure 64: KNX data secure

A device is delivered with a device specific "Factory Device Set up Key (FDSK)".

- The installer enters this key into the configuration tool (ETS) (this process is not done via the bus).
- The configuration tool generates a device-specific tool key.

- Via the bus, the ETS sends the tool key to the device that is to be configured. The transmission is encrypted and authenticated with the original and previously entered FDSK key. Neither the tool key nor the FDSK key are sent over the bus in plain text.
- The device will only accept the tool key for further communication with the ETS after the previous action. The FDSK key is no longer used for further communication unless the device is reset to the delivery state: this deletes all set safety-relevant data.
- The ETS generates as many runtime keys as are required for the group communication that you want to protect.
- Via the bus, the ETS sends the runtime keys to the device that is to be configured. The transmission is done by encrypting and authenticating it via the tool key. The runtime keys are never sent over the bus in plain text.

REMOTE ACCESS

This section covers possible procedures for remote access to IT systems. By means of remote access, the corresponding IT system can be accessed from outside the network.

PORT FORWARDING

Port forwarding is the technology whereby a computer waits for a connection to be established on a specific port and forwards the data packets to another computer in the LAN.

This means that access is not made directly to the computer in the local network, but to a specific port on the router. The router forwards the access to the corresponding port of the target computer. The packets that the computer sends back must also be processed. It replaces the IP address and port number of the computer with the IP address and forwarding port on the router.

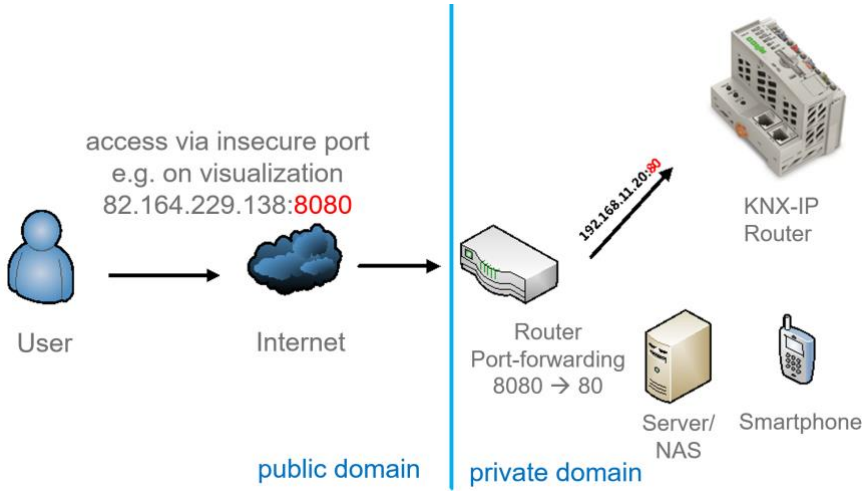

Figure 65: Example port forwarding

Functional example:

A user calls from a public network the web page with the visualization (IP address 82.165.229.138) and the port (8080). The router in the target network is configured so that all calls to this IP address with port 8080 are forwarded to the IP address of the visualization (in the example the PLC - 192.168.11.20) with port 80. The visualization answers in the opposite direction.

PORT Forwarding has the disadvantage that there is no further authentication. Anyone who knows the IP address and port has access.

In addition, a separate port is required for each device that is to be accessible via port forwarding more devices more open port larger security gap.

A little more security is provided by the additional use of HTTPS and TLS (Transport Layer Security = protocol for encrypting data transfers on the Internet). However, these only secure the connection. It is not an additional authentication.

VIRTUAL PRIVATE NETWORK

The most commonly used technique to securely access a local network remotely is to connect via an encrypted VPN (Virtual Private Network) tunnel.

The VPN refers to a virtual private (self-contained) communications network. Virtual in the sense that it is not a separate physical connection, but an existing communication network used as a transport medium. The VPN is used to connect participants of the existing communication network to another network.

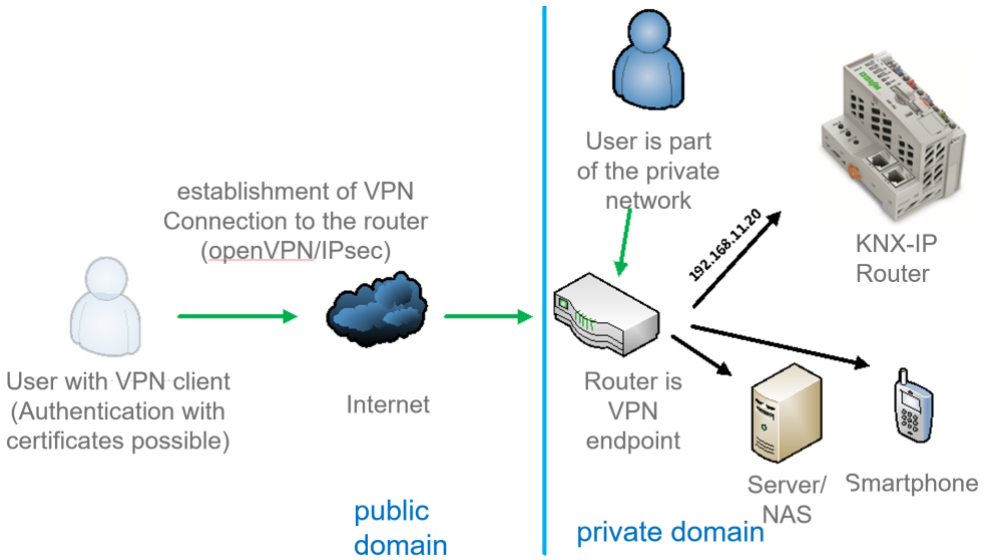

Figure 66: Example VPN

For example, an employee's computer can gain access to the company network from home, just as if he were sitting in the middle of it. From the point of view of the VPN connection, the intervening networks (his home network as well as the Internet) are reduced to the function of an extension cable that connects the computer (VPN partner) exclusively to the assigned network (VPN gateway). He now becomes a part of this network and has direct access to it. The effect is comparable to plugging the computer network cable to the network assigned by VPN.

This process works regardless of the physical topology and network protocols used, even if the assigned network is of a completely different type.

Depending on the VPN protocol used, the resulting benefits of a VPN can be supplemented by encryption, which enables tap-proof and tamper-proof communication between the VPN partners. Establishing an encrypted (virtual) network over an unencrypted network can be an important criterion, sometimes even the main reason for using a VPN.

The major advantage of VPN over port forwarding is the secure and encrypted connection. Authentication takes place via certificates or username/password. With VPN, any number of connections to the target network are theoretically possible.

Various protocols are available for the technical implementation. IPsec and SSL are often used.

VPN with Ipsec:

IPsec ensures the authentication, integrity and confidentiality of IP packets. Many routers support IPsec as a VPN protocol, and there are IPsec clients for Windows, Linux and Mac OS X. IPsec operates on OSI layer 3, but many network components cannot cope with this and do not forward IPsec (intentionally or unintentionally). Thus, it can happen that no IPsec tunnel can be established from a public hot spot.

SSL VPN:

Secure Sockets Layer (SSL) is an encryption protocol. Some vendors use SSL to establish VPNs. Since SSL is transmitted over IP and TCP like other traffic, there are no transmission problems even in restrictive networks. The open source software OpenVPN is based on SSL.

There are also VPN solutions for access via web browser. In this case, the user accesses an SSL appliance with a browser. The browser provides access to data and applications in the corporate network.

VPN security:

From today's perspective, the VPN protocols IPsec and SSL can be classified as secure. The known attacks on HTTPS or SSL are man-in-the-middle attacks with forged certificates. Such attacks on VPN tunnels are not possible, because both VPN appliance and VPN client recognize the false certificate and do not establish a tunnel.

Stolen or improperly deleted notebooks or VPN routers are more problematic. The certificates used on these devices must be revoked immediately (keyword Certificate Revocation List CRL). Trojans, viruses and other malware on a user's notebook can also enter the company network without appropriate protection.

STANDARDIZED "OPEN" COMMUNICATION PROTOCOLS

There are more and more manufacturers of (smart) systems for home or building automation. Many systems work well in themselves, all are sustainable, smart and "i-like". However, interoperability with other systems is usually difficult to achieve.

Therefore, only standardized protocols should be used:

- Protocols are (in part) standardized worldwide.
- interoperability is guaranteed
- very many products from different manufacturers for one protocol
- know-how in the (building) industry is widespread
- Building services and industry use the same protocols in some cases

Disadvantage of some protocols is the high integration effort and the partly necessary, protocol specific engineering tools (e.g. ETS, LONMaker).

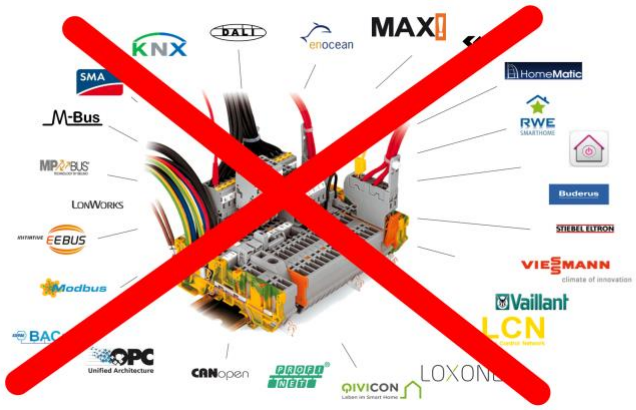

Figure 67: no universal connection of all protocols

However, it is also important to note that there is (still) no universal connection of all protocols (see Figure 67).

LIST OF FIGURES

LIST OF TABLES

REFERENCES

Baustelle:OSI-Referenzmodell. (19. 08 2020). Von http://wiki.ubuntu-forum.de/index.php?title=Baustelle:OSI-Referenzmodell abgerufen

Commission, I. E. (11. 01 2021). Electropedia: The World's Online Electrotechnical Vocabulary. Von http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=351-44-02 abgerufen

Digital Illumination Interface Alliance. (21. 10 2020). DALI-2 versus DALI version-1. Von https://www.dali-alliance.org/dali/comparison.html abgerufen

DIIA, Digital Illumination Interface Alliance. (21. 10 2020). Introducing DALI. Von https://www.dali-alliance.org/dali/ abgerufen

Dougsim, C. B.-S.-s. (11. 01 2011). Von https://commons.wikimedia.org/wiki/File:Industrial_control_loop.jpg#/media/File:Industrial_control_loop.jpg abgerufen

Echoray, C. B.-S. (12 2020). Network interface card. Von https://commons.wikimedia.org/w/index.php?curid=1972301 abgerufen

Elektronik-Kompendium.de. (12. 05 2020). WLAN-Frequenzen und WLAN-Kanäle. Von https://www.elektronik-kompendium.de/sites/net/1712061.htm abgerufen

Gerhard Schnell, B. W. (2019). Bussysteme in der Automatisierungs- und Prozesstechnik; Grundlagen, Systeme und Anwendungen der industriellen Kommunikation. Springer Vieweg Verlag.

German Federal Ministry of the Interior, f. C. (2015). Bewertungssystem Nachhaltiges Bauen (BNB). Von https://www.bnb-nachhaltigesbauen.de/fileadmin/steckbriefe/verwaltungsgebaeude/neubau/v_2015/BNB_BN2015_416.pdf abgerufen

Hermann Merz, T. H. (2016). Gebäudeautomation: Kommunikationssysteme mit EIB/KNX, LON und BACnet. Carl Hanser Verlag GmbH & Co. KG.

Homm, U. (13. 01 2021). RS-232. Von https://commons.wikimedia.org/w/index.php?curid=18444954 abgerufen

Ivory Egg (AUST) Pty Ltd. (13. 01 2021). KNX Wiring and Topology. Von https://www.ivoryegg.com.au/essential_guides/knx-wiring-and-topology abgerufen

Osram. (13. 01 2021). DALI Professional-FAQ. Von https://www.osram.com/media/resource/HIRES/333539/osram-dali-pro---faq.pdf] abgerufen

Schwöbel, U. (17. 09 2020). Von By Original: Uwe Schwöbel (de:Datei:UTP-Kabel.png)English translation: Deelkar (File:UTP-cable.png)Vector conversion: Svgalbertian. - de:Datei:UTP-Kabel.png, GFDL, https://commons.wikimedia.org/w/index.php?curid=8825122 abgerufen

Srleffler. (15. 08 2020). Von https://commons.wikimedia.org/w/index.php?curid=7029424: By Buy_on_turbosquid_optical_break_out.jpg: Cable masterderivative work: Srleffler (talk) - Buy_on_turbosquid_optical_break_out.jpg, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=7029424 abgerufen

Swan, B. (11. 01 2021). The Language of BACnet-Objects, Properties and Services. Von http://www.bacnet.org/Bibliography/ES-7-96/ES-7-96.htm abgerufen

VDE, D. D. (2003). DIN EN 61131-1, Speicherprogrammierbare Steuerungen Teil 1. Beuth Verlag GmbH,.

VDI. (2019). guideline series 3814 Part1. VDI Verlag.

Wetherall, A. S. (2012). Computernetzwerke. Pearson Verlag.

Zhaga. (03 2020). Zhaga-D4i certification. Von https://www.digitalilluminationinterface.org/data/downloadables/1/8/5/joint-zhaga-d4i-certification-program-v14_mar-2020.pdf abgerufen

The views and opinions expressed in this publication are the sole responsibility of the author(s) and do not necessarily reflect the views of the European Commission.

Co-funded by the Erasmus+ Programme of the European Union