CHALMERS

Building Automation Systems Design

Guidelines for Systems with Complex Requirements

Master of Science Thesis in the Master's Programme Structural Engineering and Building Performance Design

JOHAN KENSBY
RASMUS OLSSON

Department of Energy and Environment
Division of Building Services Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Göteborg, Sweden 2012
Master's Thesis E2012:01

MASTER'S THESIS E2012:01

Building Automation Systems Design

Guidelines for Systems with Complex Requirements

Master of Science Thesis in the Master's Programme Structural Engineering and Building Performance Design

JOHAN KENSBY

RASMUS OLSSON

Department of Energy and Environment
Division of Building Services Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY

Göteborg, Sweden 2012

Building Automation Systems Design
Guidelines for Systems with Complex Requirements

Master of Science Thesis in the Master's Programme Structural Engineering and Building Performance Design

JOHAN KENSBY

RASMUS OLSSON

Examensarbete / Institutionen för Energi och Miljö,
Chalmers tekniska högskola E2012:01

Department of Energy and Environment
Division of Building Services Engineering
Chalmers University of Technology
SE-412 96 Göteborg
Sweden
Telephone: + 46 (0)31-772 1000

Building Automation Systems Design
Guidelines for Systems with Complex Requirements

Master of Science Thesis in the Master's Programme Structural Engineering and Building Performance Design

JOHAN KENSBY
RASMUS OLSSON
Department of Energy and Environment
Division of Building Services *Engineering*
Chalmers University of Technology
Master's Thesis E2012:01

ABSTRACT

Buildings today are becoming more and more advanced and the demands on building services are increasing. A modern building is expected to provide a number of services with high security, energy efficiency and convenience. For a building with complex requirements due to the activity, such as a hospital, the services provided are even more advanced and the requirements on them are higher. This implies for the need of a building automation system. These systems come with a cost and have some drawbacks. This thesis will take on the task to study how to benefit from the possibilities with building automation systems while minimizing the drawbacks. The aim is to find guidelines for how to design, procure and manage a building automation system in a hospital in an effective way.

The thesis contains a theoretical part, describing the general architecture and functions of a building automation system. Further treated is the different technologies that supply this function and handles communication.

Interviews and participation in meetings with people working with building automation systems in hospitals and other buildings with complex requirements due to the activity has been carried out. This has resulted in a part that contains their collection of knowledge, experiences and opinions on these systems. Many of the main issues with building automation systems are treated, like how to avoid dependency on a small group of people and how to ensure the function of several systems that integrate with each other.

The last part of this thesis contains guidelines useful when designing, procuring and managing building automation systems with complex requirements. They are based on conclusions from the previous part and the authors own opinions. Some of the guidelines treat what type of technology that is suitable for different systems, how to coordinate a system and how to ensure future function, compatibility and access to service.

KEY WORDS: Communication protocol, Building automation system, Integration, Control, HVAC, Protocol, Modbus, BACnet, KNX, LonWorks, OPC, SCADA, Procurement, PLC, RTU, Field bus, Guidlines.

Design av Byggnadsautomationssystem
Rekommendationer för System med Speciella Krav
Examensarbete inom Structural Engineering and Building Performance Design
JOHAN KENSBY, RASMUS OLSSON
Institutionen för Energi och miljö
Avdelningen för Installationsteknik
Chalmers tekniska högskola
Examensarbete E2012:01

SAMMANFATTNING

Byggnader blir idag mer och mer avancerade och kraven på installationerna ökar. En modern byggnad förväntas förse oss ett antal funktioner med hög säkerhet, energieffektivitet och bekvämlighet. För en byggnad där verksamheten ställer speciella krav, såsom ett sjukhus, är dessa funktioner ännu mer avancerade och kraven på dem är ännu högre. För att tillgodose dessa behov krävs i många fall ett byggnadsautomationssystem. Dessa system komplicerar en byggnad och har vissa nackdelar. Denna avhandling utreder hur vi kan dra nytta av möjligheterna med byggnadsautomationssystem och samtidigt minimera nackdelarna. Målet är att hitta riktlinjer för hur man designar, upphandlar och förvaltar ett byggnadsautomations-system i ett sjukhus på ett effektivt sätt.

Avhandlingen innehåller en teoretisk del, som beskriver uppbyggnaden och funktionen för ett byggnadsautomationssystem. Vidare behandlas de olika tekniker som levererar denna funktion och hanterar kommunikationen i systemet.

Intervjuer och deltagande i möten med människor som arbetar med byggnads-automation på sjukhus och andra avancerade byggnader har genomförts. Detta har resulterat i ett avsnitt i avhandlingen som innehåller deras samlade av kunskap, erfarenheter och åsikter om dessa system. Här behandlas bland annat hur inlåsning undviks och hur funktionen av flera system som integrerar med varandra säkerställs.

Den sista delen av denna avhandling innehåller riktlinjer som är användbara vid design, upphandling och förvaltning av byggnadsautomationssystem med komplexa krav. De är baserade på slutsatser från föregående delen och författarnas egna åsikter. Några av riktlinjerna behandlar vilken typ av teknik som är lämplig för olika system, hur man ska samordna ett system och hur man kan säkerställa framtida funktion, kompatibilitet och tillgång till service.

NYCKELORD: Byggnadsautomation, Integrering, Kontroll, Styr och övervakning, HVAC, Protokoll, Modbus, BACnet, KNX, LonWorks, OPC, SCADA, Upphandling, PLC, DUC, Fältbuss, Riktlinjer.

Contents

1 INTRODUCTION 1

1.1 Purpose 1

1.2 Scope and method 1

1.3 Disposition of the thesis 2

2 BUILDING AUTOMATION SYSTEMS 3

2.1 Field level 3

2.2 Field network 4
2.2.1 Hard wiring 4
2.2.2 Field bus 4
2.2.3 Power line connection 5
2.2.4 Wireless connection 5

2.3 Automation level 6

2.4 Primary network 6
2.4.1 Network switch 7

2.5 Secondary network 8

2.6 Management level 8

3 COMMUNICATION STANDARDS 10

3.1 OSI-model 10

3.2 Building automation protocols 11
3.2.1 Internet Protocol 11
3.2.2 Modbus 12
3.2.3 BACnet 13
3.2.4 KNX 13
3.2.5 The LonWorks protocol 14
3.2.6 Other building automation protocols 14

3.3 Communication between different protocols 15
3.3.1 OPC 15
3.3.2 Drivers 17
3.3.3 Gateway 17

4 COMMUNICATION INFRASTRUCTURE 18

4.1 Primary network 18

4.2 Protocols 19

4.3 Communication between different protocols 20

4.4 Wireless communication 20

5 INTEGRATION 22

5.1 When to integrate and to what extent 22
5.2 Large and advanced building automation systems 24
5.3 Choice of control units 25

6 ORGANIZATION 26
6.1 Procurement process 26
6.2 Responsibility of the function of a building automation system 27
6.3 Operation of a building automation system 28

7 GUIDELINES FOR BUILDING AUTOMATION SYSTEMS WITH COMPLEX REQUIREMENTS 29

8 REFERENCES 31

APPENDIX

Preface

This thesis should be seen as a collection of knowledge, experiences and opinions from people working with building automation system applications in hospitals and other buildings with complex requirements due to the activity. Interviews and participation in meetings have been carried out from June to October 2011.

We want to thank our supervisor Anders Trüschel for guidance and feedback on our work. Also, we would like to thank our examiner Jan Gustén for providing us with valuable contacts and for letting us use his office as a workspace. Finally, we are thankful towards all the people that freely shared their knowledge in interviews, let us participate in their meetings and provided us with material. They are all listed below.

Göteborg January 2012

Johan Kensby

Rasmus Olsson

Special thanks to:

Kalle Skoglund	Totalinstallation AB
Martin Liesén	Keylogic
Jan Wallsby	Keylogic
Mathias Ranhage	Ramböll
Mikael Grietze	SWECO Systems AB
Anders Björling	Siemens AB Industry Sector
Mikael Thörner	Siemens AB Infrastructure & Cities Sector
Ingemar Lundgren	Västfastigheter
Ulf Larsson	WSP Elteknik
David Silfverblad	WSP Elteknik
Joakim Sörensen	WSP Elteknik

Nomenclature

Automation level	Part of the building automation system where the advanced controllers that regulate the devices at Field level is located.
ASCII	*American Standard Code for Information Interchange*. A way of representing letters and characters in computers.
BACnet	*Building Automation and Control networks.* Building automation protocol.
BAS	*Building Automation System*. A system that controls and monitors building services.
CRC	*Cyclic Redundancy Check.* Method for calculating checksums to validate data that is transferred over a network.
DALI	*Digital Addressable Lighting Interface.* Building automation protocol.
Daisy chain	A topology for connecting nodes in a chain network.
Driver	Implemented software to translate between hardware and software.
Ethernet	Network technology for computer Local Area Networks.
Field bus	A main bus to connect Field level devices in a building automation system. Either in a trunk topology or with a daisy chain.
Field level	Part of the building automation system where the devices that physically control or detect building functions are located.
Field network	The network between the Automation level and the Field level in a building automation system.
Gateway	Node in a network that translate between different protocols.
GPL	*GNU General Public License.* Is a copyright license for free software.
Half-duplex	Communication in both directions but only in one direction at a time.
Hard wire	Each device in the Field level is connected by a separate cable.

HMI	*Human Machine Interface.* User interface for interaction between human and machine. The term applies both to where humans give input to the system (like switches etc.) and where the system gives output to the human (like displays etc.).
I/O	*Input/Output.* Refer to communication between a device in the building automation system and the surroundings, for example a temperature sensor or a human.
Internet	Computer network for communication extending the entire world.
IP-address	Unique address to a node in a network.
KNX	Building automation protocol.
LAN	*Local Area Network.* Computer network located in a building or to a limited area.
LRC	*Longitudinal Redundancy Check.* Method to validate data sent in a bit stream.
LonWorks	Building automation protocol.
M-bus	*Meter bus.* Building automation protocol.
MAC-address	*Media Access Control address.* Physical address of a device in ta network, works as a unique identifier.
Management level	Part of the building automation system where the devices that manage and monitor the function of the devices in the Automation level and Field level are located.
Master/Slave	A master-device initiates communication by requesting data from a slave-device, which respond with the requested data.
Microsegmentation	A technique to isolate two nodes in a network to avoid data collision.
Modbus	Building automation protocol.
Neuron chip	Licensed microchip for LonWorks.
OPC	Is used in a building automation system for translation from a specific protocol to a standard interface.
OSI-model	*Open System Interconnection model.* Reference model to a layered framework for communication in networks.
PL	*Power Line.* Medium over which data signals can be transferred in a building automation system.
PLC	*Programmable Logic Controller.* Digital computer, which is a part of a building automation system and located in the Automation level.
Primary network	The network between the Management level and the Automation level in a building automation system.

Protocol	Rules for communication in a network, often based on the OSI-model.
Public Procurement Act	Swedish law that regulated procurement for the public sector.
Radio frequency	Medium over which data can be transferred in a building automation system.
Router	Device to connect two networks.
RTU	*Remote Terminal Unit*. Microprocessor controlled device, which is a part of a building automation system and is located in the Automation level. The Swedish term RTU is DUC, Data Under Central.
SCADA	*Supervisory Control And Data Acquisition.* A system that can be a part of the building automation system to store data and make set points to PLCs and RTUs. The system is located in the Management level.
Secondary network	A network that is connected to the Primary network but communication is made with a different protocol.
Switch	A network device that makes it possible to connect many nodes in a Local Area Network.
TCP/IP	*Transmission Control Protocol over Internet Protocol.* A protocol for data transmission over IP networks.
Trunk topology	A main bus cable to which nodes can be connected.
Twisted pair	Medium over which data signals can be transferred in a building automation system.
WLAN	*Wireless Local Area Network.* Wireless Computer network located in a building or to a limited area.
Z-wave	Building automation protocol.
ZigBee	Building automation protocol.

1 Introduction

Buildings are becoming more and more advanced and the demands on building services are increasing. A modern building is expected to provide conditions for a number of services with high security, energy efficiency and convenience. For a building with complex requirements due to the activity, such as a hospital, the services provided are even more advanced and the requirements on them are higher. Many of these services benefit from communicating with each other, sharing functions and being monitored together. To control and monitor several building services in an efficient way, a more or less advanced building automation system is required. There are advantages with using an advanced building automation system.

- Monitoring of several systems from one place
- Sharing of alarms
- Interaction for more efficient control strategies
- Remote service etc.

Experiences have shown that there are also drawbacks.

- Higher level of competence is required
- Larger risk of becoming dependent of services from one company
- Higher investment costs etc.

To benefit from the advantages and to avoid the drawbacks is not a simple task. For several major building automation projects, this task has not been fulfilled in a satisfying way. This thesis will take on this task and study how to benefit from the possibilities with building automation systems while minimizing the drawbacks.

1.1 Purpose

The purpose of this thesis is to find guidelines for how to design, procure and manage a building automation system in a hospital in an effective way.

1.2 Scope and method

In order to achieve the purpose of this thesis, a description of a general building automation system has been established. Also, a study of the communication standards used in building automation system has been carried out. These parts (Chapter 2 and Chapter 3) can be seen as the theoretical part of this thesis that is required in order to present the results. They are primarily based on literature studies. For parts where the literature is deficient or ambiguous, knowledge gaps have been filled with help of those persons who were interviewed during the work with this thesis.

The following part (Chapter 4, Chapter 5 and Chapter 6) is based on interviews and participation in meetings with people working with building automation systems in hospitals and other buildings with complex requirements due to the activity. All the persons that have contributed to this part of the thesis are listed in the Preface. This part should be read as a collection of their knowledge, experiences and opinions on building automation systems in hospitals and other buildings with complex

requirements due to the activity. This section of the report will not contain any references to whose the opinions are, this because of two main reasons.

- Problems with sensitive nature are discussed and this is a solution to avoid identify people who address these problems which can lead to misunderstandings.
- Most of the opinions are shared by several persons and disagreed by some; this will make the chapter so full of references that it will be difficult to read.

The final part (Chapter 7) is a direct answer to the purpose of this thesis. This analysis is based on the results from the previous parts (Chapter 4, Chapter 5 and Chapter 6). The analysis is here taken one step further and provides the authors suggestions for guidelines for how to design, procure and manage a building automation system in a hospital in an effective way.

The main focus in this thesis is large hospitals and it has been the basis of all interviews. Nevertheless the results of this thesis are more general than that since many buildings with more or less complex requirements due to the activity have similar building automation systems and face the same problems.

1.3 Disposition of the thesis

Chaper 1: The first chapter is an introduction to the thesis where the purpose and scope is presented; it is also short description how the work has been carried out.

Chaper 2: In this chapter are the principle parts of a building automation system described. This is a theoretical part of the thesis.

Chapter 3: The third chapter in the thesis is about communication standards and different protocols that can be used in a building automation system. This is a theoretical part of the thesis.

Chapter 4: This chapter is based on interviews and addresses the problems with infrastructure of a building automation system, which include the Primary network, protocols, communication between different protocols and wireless communication.

Chapter 5: This chapter is based on interviews and addresses the problems with integration, when systems should be integrated and how far it should be taken.

Chapter 6: This chapter is based on interviews and addresses the problems with the procurement process and the operation of the system. It also treats the question about responsibility if the system does not work as planned.

Chapter 7: This chapter contains guidelines useful when designing, procuring and managing building automation systems with complex requirements. They are developed with a hospital in mind, but many of them are general and apply to other systems with more or less complex requirements. The guidelines are based on conclusions from the chapters 4 to 6 and the authors own opinions.

2 Building automation systems

A building automation system is a system that controls and monitors building services. These systems can be built up in several different ways. In this chapter a general building automation system for a building with complex requirements due to the activity, such as a hospital, will be described. Real systems usually have several of the features and components described here but not all of them. They may also have specific solutions that are not described in this chapter.

When defining building automation systems, it is advantageous to divide the system into levels. There is no uniform way of defining and naming these levels in a system. For the purpose of this thesis will all devices be divided in three levels and three networks connecting them as shown in Figure 2.1. In this chapter, the function of all parts in a building automation system will be defined from a bottom up approach, starting with Field Level.

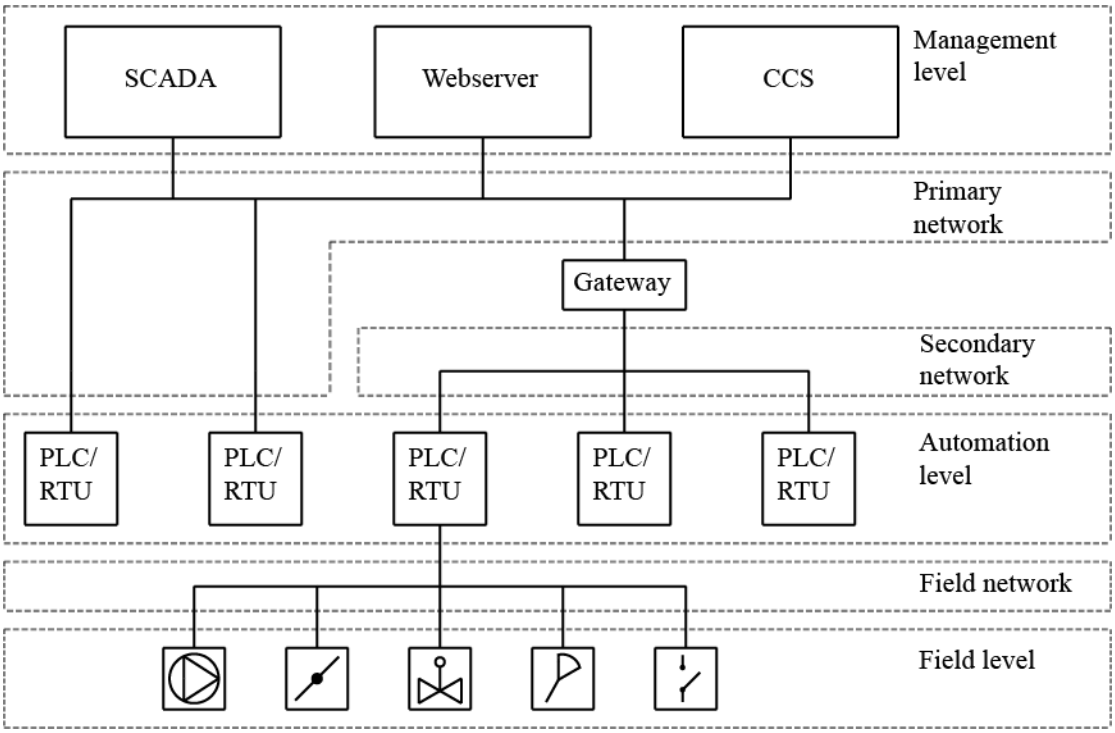

Figure 2.1 Principal architecture of a building automation system.

2.1 Field level

The Field level consists of all devices that physically control or detect the building functions. They are devices like actuators, motion sensors, smoke detectors, valves, dampers, fans, card readers, motors, sprinklers, light switches, hospital specific equipment etc. Most of these devices do not have any "intelligence" of their own. They either send their status or react to control signals.

In the very most basic system, Field level devices are not connected to anything and are controlled manually. For simple automatic control, a control device can be connected to a sensor for example a light switch connected to a motion sensor. These

solutions work fine for many applications, but for more advanced building services systems a more advanced control system is usually desired. This is usually achieved by connecting the Field level devices to a more advanced controller in the Automation level through a Field network. The Field level devices then act, as slaves while their Automation level controllers are masters. There are also Field level devices that connect to a building automation system in other ways. For example an outside weather station could be connected to the Primary network, either directly or through a gateway.

2.2 Field network

The Field network is the network that connects the Field level with the Automation level. The main purpose with this network is to connect the actuators, sensors and other Field level devices to a PLC, Programmable Logic Controller, or RTU, Remote Terminal Unit, in the Automation level. The physical connection between the two layers can be of four various types.

- Hard wired
- Bus system
- Power line
- Wireless

One or more of these four types will be the backbone of a Field network. A building automation system usually contains several Field networks.

2.2.1 Hard wiring

If the devices in the Field level are connected by hard wiring, each device is connected by an individual cable to an individual port on an Automation level device, Marshall (2001). What type of signals that is sent over the Field network depend on what devices that form the system. For example a common way to control a valve is to supply a voltage between 0 V and 10 V. This is an analogue control signal that tells the valve what position it should have. A more advanced example could be an outside weather station hard wired to a PLC via some sort of data cable. The signals sent in this example consist of digital data. Hard wiring is usually a satisfying solution for systems with a limited number of connections.

2.2.2 Field bus

Another solution is to connect the Field level devices through one or several Field busses, Marshall (2001). A Field bus usually consists of twisted pair copper cables for communication. Power supply can either be connected separately to the devices or included in an extra wire in the bus cable. The wires are either split in connection boxes in a trunk topology or connected in a daisy chain as shown in Figure 2.2.

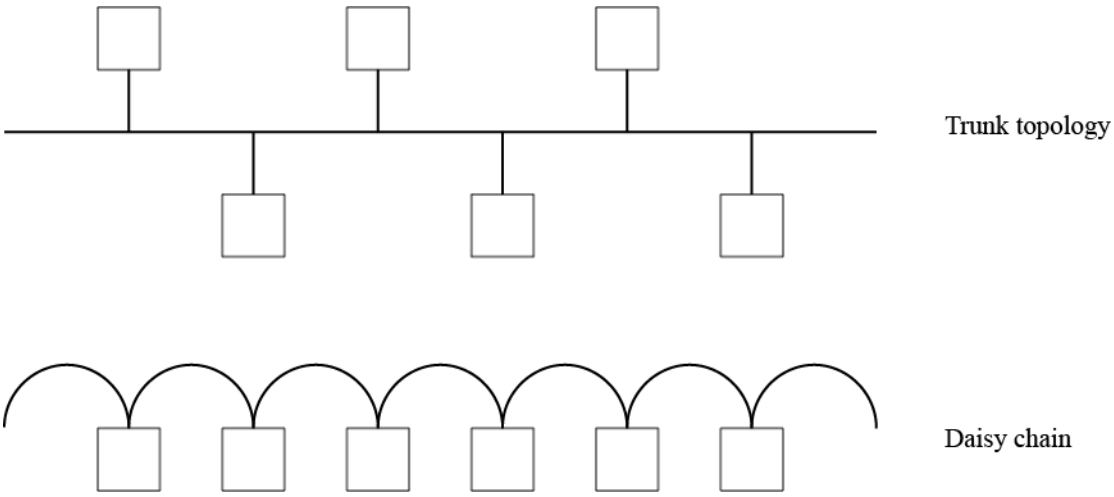

Figure 2.2 Trunk topology, the devices are connected to a main bus cable with another cable. Daisy chain, the main bus cable is directly connected to each device.

The Field bus can be compared with a Local Area Network. In a Field bus no switches are needed in intersections where the devices connect to the main cable. This because the signal reflection is much less of a problem when data is transferred at low bit rates. An Local Area Network on the other hand has a bit rate of about 100-1000 megabit per second. This means that if there would not be any switches to split and isolate the communication between two nodes, the network would have a constant overflow of reflecting signals.

Due to the lack of switches, all devices along the bus receive messages sent over the cable but only the addressed devices reacts to it. Common bit rates for these types of networks are around 1-40 kilobit per second, less than a thousandth of a common Ethernet network. This is enough for most appliances since a common message only consists of a couple of bytes. The numbers of components that can be connected in one bus vary from tens to thousands depending on the protocol used, cable length and connection types.

2.2.3 Power line connection

Some communication standards also support power line communication through the 230 V/50 Hz cables that connect regular electrical sockets, ZVEI (2006). The signals can share the same infrastructure since the data communication uses a significantly higher frequency band of 95-125 kHz. In order to avoid signal reflection, bit rates are usually kept low, at approximately 1 kilobit per second. The architecture and principal function of the network is similar to a Field bus system.

2.2.4 Wireless connection

The far most common wireless communication technology for Field networks is radio frequency in the middle frequency band (868 MHz). Data is transmitted by modeling frequency, phase or amplitude of the radio waves, ZVEI (2006). Common range for a transmitter is around 30 m horizontally in a building with lightweight partition walls

made of for example timber and gypsum. The range can be greatly reduced if the walls contain metal, are made of concrete or if there are other special circumstances. Amplifiers can be used to extend the range; often they are included in the transmitters in the Field level devices.

2.3 Automation level

The Automation level includes all the advanced controllers that controls and regulates the Field level devices in real time. Today, these controllers are usually digital and based on microprocessors, Levermore et al. (2000). This makes it possible to freely program them with:

- Proportional control
- Integral control
- Differential control
- Any other logic control or combination of logic controls

The controllers can be divided into two categories:

- PLC – Programmable Logic Controller and
- RTU – Remote Terminal Unit

A PLC works similar to a modern computer[1]. It can be feely programmed to act on any number of input data and control any number of output data as long as it has sufficient processing power and ports. A PLC can often be expanded with racks containing I/O ports connected to one of the PLCs internal buses. There are also more advanced PLCs, often called Soft-PLC. They run on a more advanced operating system (like Windows) and can be connected to a display and a keyboard. A RTU usually has less processing power and fewer ports then a PLC. This is because a RTU is built for a specific task and is dimensioned accordingly. It is common that a RTU is shipped pre-programmed so that the user only has to adjust it. In most other aspects are PLCs and RTUs similar and there is not a strict boundary between the classifications. It is common that the manufacturer of a unit includes a control system containing a RTU, a Field network and all Field level devices necessary. This is commonly referred to as a entity unit with integrated control.

In the simplest case a PLC or RTU works as a standalone unit with no interaction with other PLCs, RTU or equipment in the Management level. In order to communicate, a PLC or RTU can either be connected to the Primary network and communicate through a SCADA system or CCS, Central Control Station or have a small local peer-to-peer network in which a limited amount of PLCs or RTUs can communicate.

2.4 Primary network

The primary network is also commonly referred to as Backbone or Management network. The primary network connects the Automation level and the Management

[1] Interview with Martin Liesén and Jan Wallsby 2012-09-01

level in the building automation system. A primary network can either be separated or shared with the regular LAN, Local Area Network, in a building. Usually these networks communicate over twisted pair cables (ISO 8802-3) like in most networks in offices and homes. Communication over WLAN, Wireless Local Area Network, is also a possibility. These networks handle much larger amounts of data at higher bit-rates then the network types described in previous sections. Common bitrates are in the span of 10 – 1000 Mbit.

2.4.1 Network switch

A network switch is used in a LAN connect a number of nodes and allow them to communicate with each other (Cisco Systems, Inc., 2009). To identify nodes in a network the switch uses the MAC-address, also called physical addressing. This corresponds to the data link layer in the OSI-model, as described in Section 3.1. To reduce the risk of data collision in a network a switch uses microsegmentation so only two nodes are in contact at the time as shown is Figure 2.3.

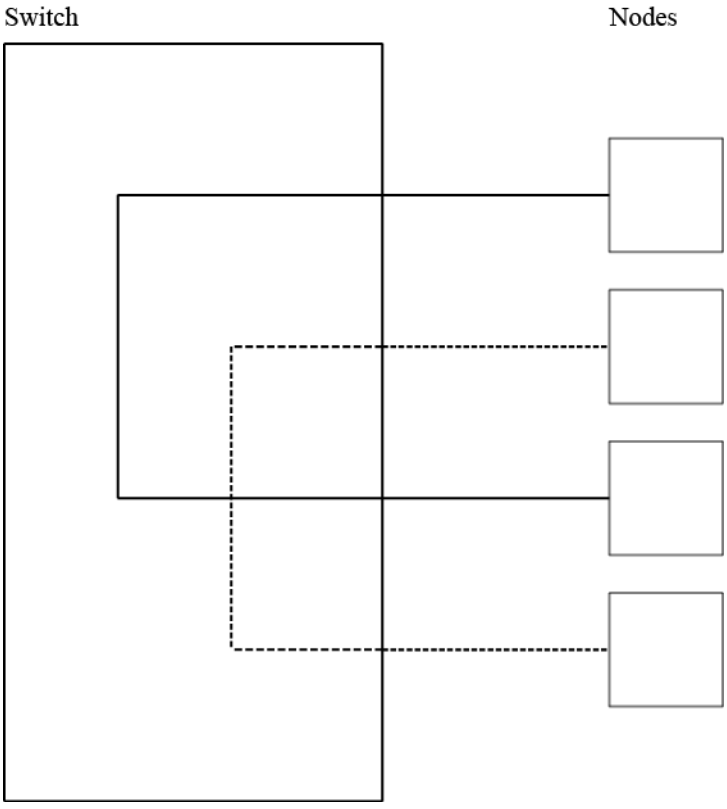

Figure 2.3 Description of microsegmentation in a switch.

There are two other categories of switches working in different layers in the OSI-model, data link layer with network layer features and multilayer switches. In the network layer IP addresses is used as identification, this can also be referred to as logical addressing. A multilayer switch can either switch the data on MAC-address or route the incoming data with IP addresses.

2.5 Secondary network

Secondary networks connect the Automation level and the Primary network. This means that the network is a sub-network to the Primary network. The purpose with a secondary network is to gather devices in the building automation systems Automation level that operate with a protocol that is different from the protocol in the Primary network and connect those devices to the rest of the building automation system. A building automation system must not have a Secondary network if it is possible to design it with just one protocol. There can be a number of Secondary networks attached to one Primary network.

2.6 Management level

The Management level includes all devices that manage and monitor the Building automation system and that interact with personnel and the Internet. Examples of these devices can be.

- Databases that log activity
- Web servers
- Operator's panels
- CCS – Central control station
- Servers that translate messages into different protocols.

A web server is an access point to a Building automation system that can be used for several different purposes. It allows remote maintenance, the possibility to send alarms to service personnel, the possibility to read the status about several systems at one place etc.

Depending on how centralized or decentralized a system is a CCS can have different roles. In a centralized system, a CCS can handle a large part of the real time control with PLCs and RTUs mostly working as nodes that only acquire and send data. In a decentralized system, a CCS does not perform any real time control and the PLCs and RTUs should be able to operate on their own if the contact with the CCS is interrupted. The CCS coordinates the PLCs and RTUs and may perform cascade control.

Cascade control means that the control is divided into two levels; one level is controlling a varying set-point for the other level, Levermore et al. (2000). For example a PLC is controlling the climate in a room. One of the parameters it can control is the supply air temperature. Rather than directly controlling the devices in the air handling unit, it controls the set-point for a second PLC. This second PLC then runs its own control loop that controls the devices in the air handling unit so it supplies the set-point temperature. Cascade control can be performed in several ways.

- Between several control functions within one PLC or RTU
- By a PLC, RTU or CCS on a PLC or RTU
- Manually by personnel on a PLC or RTU

Cascade control is also commonly referred to as master-submaster control or reset control.

All of the features described for Management level can be implemented in a SCADA system. SCADA stands for Supervisory Control And Data Acquisition, Bailey D. Wright E. (2003). SCADA is neither a brand nor bound to any specific technology; it includes all solutions that fulfil the function of "supervisory control and data acquisition". The simplest SCADA system is a person that manually adjusts set points etc. for PLCs and RTUs and logs their performance. For a building with complex requirements due to the activity, such as a hospital, a more advanced SCADA system with more functions is usually used. There are many technical solutions for SCADA systems available on the market that provides these functions.

3 Communication standards

When computers communicate they do that by exchanging data. In order to transmit data and establish a communication link, a protocol is needed. A protocol is basically a set of rules, for communication in a network between computers, Sharp (2008). The rules are of such manner that if they are not followed the communication will fail. The function of protocols is to enable communication between systems and ensure that data reach its destinations. In order to send a message over a network a lot of different protocols are used, they have all different tasks in the process of sending the message. For example there is a protocol to transport the message and one to route it to the correct location. These different types of functions are described in a framework called the OSI-model.

The term protocol is used to describe single protocols and protocol suites. A single protocol is limited to one level in the OSI-model described below. A protocol suit includes several protocols and operates in several layers in the OSI-model.

3.1 OSI-model

The OSI-model, Open Systems Interconnection model, is a layered framework for communication in networks, ISO/IEC (1994). It is an ISO-standard developed by the International Organization for Standardization. The model consists of seven layers; each layer has its own special functionality from physical hardware to software applications. The layers are designed so that they have a direct interaction with the adjacent layer below. Information is passed from a higher to a lower layer, where the lower layer process and add its own special tags to the information before it passes it on to the next layer. Information tags could be, destination address, source, checksum, etc.

Layer 7 – Application Layer
This layer represent the information. The purpose is to ensure that two application programs can communicate over a network.

Layer 6 – Presentation Layer
This layer take care of how the information is presented. This is where the data types from the application layer are defined and translated.

Layer 5 – Session Layer
The Session Layer function is to establish, manage and terminate connection between two nodes (computers).

Layer 4 – Transport Layer
Defines how the data should be transferred and what protocol that should be used, for example TCP. The transport layer is responsible for data transfer between source and destination processes.

Layer 3 – Network Layer
Makes sure that data has the right address, for example the correct IP address. The Transport layer transfers data between systems in a network, the source and destination of the data is defined by network layer addresses. To make the transfer of data possible in the network, routers and switches are used.

Layer 2 – Data Link Layer

Representing the network that is used for example Ethernet. Here are the bits from the physical layer transformed into frames. The layer can then transfer these frames between two hosts.

Layer 1 – Physical Layer
This is the physical medium over which digital signal is transmitted, for example twisted pair, optical cable or wireless.

3.2 Building automation protocols

There is a lot of building automation protocols developed. Some of them are more widely spread and more used than others. The protocols are also designed for different network levels as shown in Table 3.1.

Table 3.1 Comparison of what protocols that is used in the Primary network or the Field network.

Protocol	Primary network	Field network
Modbus		
- ASCII		X
- RTU		X
- TCP	X	
BACnet		
- IP	X	
KNX	X	X
LonWorks		X
TCP/IP	X	

3.2.1 Internet Protocol

The Internet Protocol is included in the Internet protocol suite also known as Transmission Control Protocol over Internet Protocol, TCP/IP. The stack of the Internet protocol suite is a collapsed or a simplified version of the OSI-model, this can be seen in Figure 3.1. The top three layers are reduced to one, which have adopted the name Application layer. This layer is followed by Transport layer, Network layer and finally by the Link layer that is a combination of the two lowest layers in the OSI-model, Samjani (2002).

OSI reference model	TCP/IP stack	Protocol
Application Layer	Application Layer	HTTP, FTP
Presentation Layer		
Session Layer		
Transport Layer	Transport Layer	TCP, UDP
Network Layer	Network Layer	IP
Data Link Layer	Link Layer	
Physical Layer		

Figure 3.1. OSI/Internet protocol suite stack.

The main purpose of the Internet Protocol is to route packets over Internet with help of routers. It has an addressing system to make it possible to send a packet from one end computer to another one. This is based on the fact that both end computers have seperate fixed IP addresses. All data about the routing is encapsulated in the header of the packet. Routers on the Internet just forward the packets using the known information in the header.

In building automation systems TCP/IP is usually used in the Primary network. Either as pure TCP/IP or letting IP be the carrier to other protocols like Modbus or BACnet.

3.2.2 Modbus

Modbus is a protocol used in both industrial manufacturing environment and building automation systems, for communication in a master-slave system. Modicon developed the protocol in 1979, Hollinger (2011).

There are mainly three versions of the Modbus protocol.

- Modbus ASCII
- Modbus RTU
- Modbus TCP

To read more about the different Modbus versions see Appendix A.

Since the Modbus protocol is developed for master-slave communication it works according to polling principles. That means that the master is asking questions to the slave to detect changes in values or alarms. Modbus is used in both the Primary network and the Field network depending on which version that is used.

Modbus Organization has since 2004 been handling the Modbus protocol. The protocol is released as open software and all documentation and specifications can be downloaded without any charge. Members of Modbus Organization can also download development tools and samples of implementations.

Modbus Organization does also perform testing and certification of products developed for Modbus ASCII, RTU and TCP. It is not mandatory to apply products for testing and certification, which mean that products can be sold as a Modbus product without following the standard implement rules.

3.2.3 BACnet

BACnet is an acronym for Building Automation and Control Networks. The BACnet protocol was developed by the American Society of Heating, Refrigerating and Air Conditioning Engineers, ASHRAE. The reason to develop the protocol was to meet the requirements for communication in building automation, Levermore et al. (2000). The protocol was first released as an ANSI/ASHRAE standard 1995 and since 2003 is BACnet also an international and European standard.

BACnet is an object-oriented protocol triggered by events. This means that there is no communication between devices until something happens or changes. BACnet is mainly used in the Primary network.

BACnet is released under GPL and has no license. BACnet International is the international organization that looks after the interest of BACnet such as future development, meetings where products are tested in networks. There are sub groups to BACnet International that are located in countries all over the world, like BACnet Interest Group – Sweden (BIG-SE). BACnet International also has an organization for testing and listing of tested products, BACnet Testing Laboratories (BTL).

For more information on the BACnet protocol see Appendix B.

3.2.4 KNX

KNX is a worldwide standard for communication between building technology systems, KNX Association (2011). It is an OSI-based network communication protocol, which was developed from three previous standard protocols EIB, EHS and BatiBUS. The KNX protocol has four different medias over which it can be transmitted.

- Twisted pair
- Power line
- Radio frequency
- IP networks

For more information about how KNX works with the different medias see Appendix C.

The KNX protocol is event triggered like BACnet. It is used in both Primary and Field network.

To be able to get all the documentation and specification of KNX, a membership with the KNX Association must be established. This membership works as a payment or a license to use development tools for KNX. KNX Association provides testing and certification of products developed for KNX. The main reason to certify products is to ensure that the product will be compatible with other third party developed products. Products tested by KNX Association will also be branded with the KNX logotype as a confirmation that the product follows the standard.

3.2.5 The LonWorks protocol

The LonWorks protocol is also known as the LonTalk protocol. The protocol is used in LonWorks networking platform, Levermore et al. (2000). It was developed by Echelon Corporation and was accepted as an ANSI standard in 1999 (ANSI/CEA-709.1-B). The protocol is based on the OSI-model and uses all of the seven layers.

The LonWorks protocol can operate according to master-slave principle or directly without a central controller. The protocol is used in the Field network.

The LonWorks protocol itself comes without license requirement and it is possible to implement the protocol to any microprocessor. However Echelon Corporation sells the Neuron chip, which has the LonWorks protocol implemented. In the past was it required to purchase the Neuron chip to be able to use the protocol.

To read more about the LonWorks protocol see Appendix D.

3.2.6 Other building automation protocols

The list of building automation protocols existing today is very long. There are both commercial and proprietary protocols that can be added to that list. Some of the protocols are developed for specific tasks like only handling the light in a room or a building. Some of the protocols are developed to be specifically used with wireless technology. Here will some of the more common protocols be listed.

DALI

DALI is an acronym for Digital Addressable Lighting Interface. It was developed for advanced control of lightning in buildings. The protocol is released as an open standard. There are gateways, which can connect DALI networks with for example KNX or BACnet systems.

Z-wave

Z-wave is a communication protocol designed for building automation, using radio frequency, Z-wave Alliance (2011). It is primarily used in private homes but other applications are also available. The standard is a result of 200 companies in Z-wave Alliance that have agreed on using the same standard for their products. The products range from lighting, alarms, HVAC, monitoring, locks, irrigation, sunshade, entertainment systems etc.

ZigBee

ZigBee is mostly for small residential buildings. It is using similar technology as Z-wave, based on radio frequency. Examples of products are temperature sensors and electrical switches. The protocol is license free as long it is not used in commercial buildings.

M-bus

M-Bus, which is short for Meter-Bus, is often confused with Modbus. M-Bus is not really a building automation protocol. It is used in buildings to remotely reed the electrical meters and collecting measurement data from sensors. The protocol is designed to mark the data with time stamps and record from what device it origins.

3.3 Communication between different protocols

When installing and configuring a building automation system is it preferable if all network levels and systems are communicating with the same protocol. It is very few building automation systems that are designed or even possible to design in a way that only one protocol can be used for the entire system. There are various ways of handling communication between parts of a building automation system that use different protocols.

3.3.1 OPC

Originally OPC stand for OLE for Process Control, where OLE stands for Object Linking and Embedding. Since more technologies than the original OLE technology is supported, the OPC Foundation no longer considers OPC an acronym.

OPC is a combination of hardware and software, which can be installed into a building automation network as a translator from different protocols to a standard interface.

For example if a simple network is built with three devices all using different protocols and a data acquisition database see Figure 3.2. The data acquisition database must then have the ability to understand all of the three protocols to be able to gather data. If an HMI, Human Machine Interface, also should be installed to the network that one must also know all three protocols for the system to work. This can be seen in Figure 3.3.

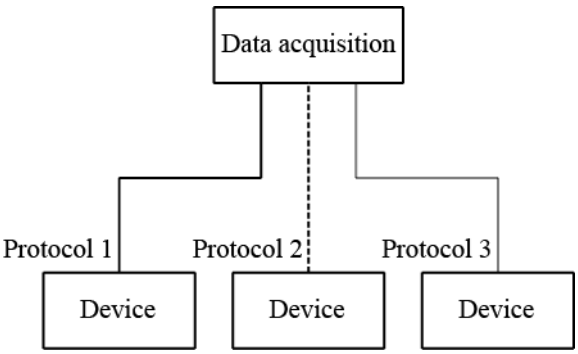

Figure 3.2 System with three devices using three different protocols, which are connected to a data acquisition device.

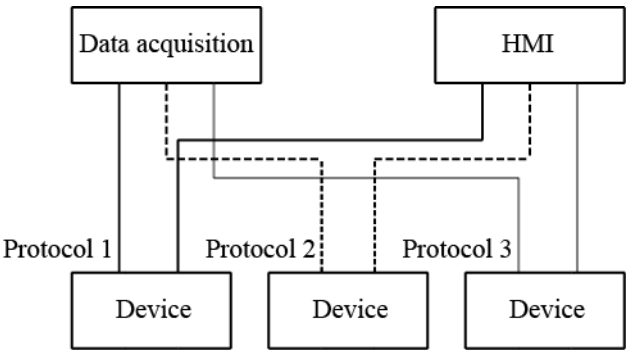

Figure 3.3 System with three devices using different protocols, which are connected to a data acquisition device and a HMI.

As can be seen in Figure 3.3 the complexity is increasing rapidly with a lot of wires and many devices that must be programmed to understand the different protocols. One way to make the building automation system less complex can be to use one or more OPC servers. An OPC server can be chosen of the shelf and in that case more than one must be used in order to take care of all three protocols. However, if some programming is performed only one OPC server might be enough. These two cases can be seen in Figure 3.4 and Figure 3.5.

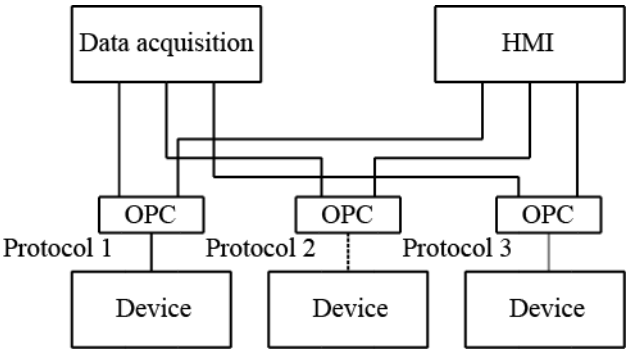

Figure 3.4 System with three devices using different protocols connected to three OPC servers, which translate the protocols into a standard interface.

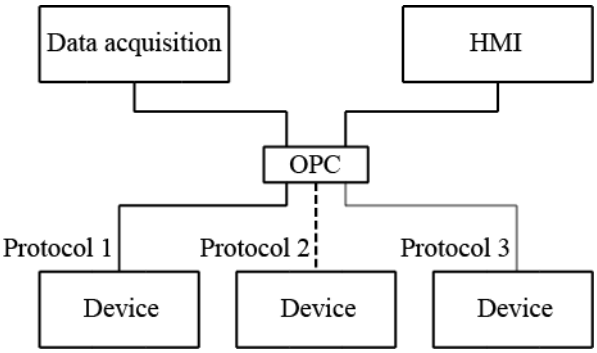

Figure 3.5 System with three devices, using different protocols, connected to one OPC server.

3.3.2 Drivers

Drivers are software implemented on a PLC, RTU, server or any other device where translation between software and hardware is necessary. A driver is implemented to understand and know all details about how data from a certain device sent by a specific protocol should be interpreted. This means that for example data acquisition software does not need to know anything about a device as long as it has a driver installed to take care of the translation.

3.3.3 Gateway

A gateway is a piece of hardware, software or a mix between those. The purpose of a gateway is to translate between two networks using different physical media and protocols, for example between a Modbus RTU network and BACnet/IP network. This means that devices in the two different networks can communicate, even though they use different protocols. Gateways are commonly used when an IP based Primary network should be connected to either an IP based Secondary network or to a serial based Field network.

A gateway is designed to operate in the four top layers of the OSI-model to convert all necessary data in order to pass it on to a new network type.

4 Communication infrastructure

This chapter and the following two chapters is based on interwiews and participation in meetings with the persons listed under "Special thanx to:" in the Preface. The content in the following chapters should be seen as a collection of knowledge, experiences and opinions of these people.

To be able to setup a building automation system a well-planned communication infrastructure is necessary. In order to make a proper analysis, a definition of communication infrastructure is required. For the purpose of this thesis, a proper definition of communication infrastructure in a building automation system would be: All hardware and software that enables communication between devices. This will for example include: cables, ports, gateways, switches, drivers and OPC servers.

4.1 Primary network

Almost all buildings with complex requirements due to the activity have an Ethernet network using the Internet Protocol to provide a data connection to all parts of the building. Most of the major protocols for building automation can use the Internet Protocol as a carrier. This means that in many cases the same communication infrastructure can be used for both the Primary network for the building automation system and for the regular Ethernet network in a building. This will save large amounts of wiring.

These two systems have usually been kept separated. The main reason for the separation has been because network engineers have been restrictive with access to the Ethernet network with regards to security. The issue with security is of different dignity in buildings depending on what kind of business is taking place there. For example a residential building does not have so strict regulations regarding safety as a hospital or a large company.

Today, there are no technical barriers for the two networks to use the same communication infrastructure. Technical solutions are available that overcome the security issues mentioned earlier, for example encryption or emulating several separated networks on the same equipment. Still, there is a resistance in many organisations for making this transmission mostly due to lack of knowledge of and trust in the solutions available.

Sahlgrenska University Hospital in Gothenburg is facing this transition. Today the hospital has two separated communication infrastructures, one for building automation and one administrative network for traffic related to the activity in the building. The administrative network at Sahlgrenska has recently been migrated from being local at Sahlgrenska to be a part of the wide area network in the region of Västra Götaland. The plan for the future is to include the building automation network at Sahlgrenska University Hospital in the same communication infrastructure. The main reasons for this transition are.

- Increase the redundancy of the network, making it less vulnerable to communication errors.
- Make it more cost efficient.
- Create one comprehensive system where all information can be accessed.

A new building is being constructed at Sahlgrenska University Hospital, BOIC - Bild- och interventionscentrum (Center for images and intervention). This will be the first building at the hospital where the building automation system and administrative network share one communication infrastructure.

4.2 Protocols

There are a lot of different protocols, which can be used in building automation systems. There is no right or wrong when protocols are chosen to the system. The protocols should satisfy the demands that are required for the system and they should be easy to work with. Even though there are many available protocols on the market, the professionals who work with these tasks seem to have the same idea about which protocols that are most commonly used within building automation systems today. There are generally four protocols, which are favoured by the professionals. The most commonly used protocols in Sweden today are Modbus, BACnet, KNX and IP based versions of these.

There are trends in which protocols that are used. For example ten years ago, the LonWorks protocol was one of the most common. Today LonWorks is rarely used in new installed building automation systems. It is still an important protocol since many older systems communicate with it. These systems are in need of regular updates and service. The reason why this protocol is not among the most common ones today is hard to pinpoint. One reason could be that the requirement of either an implemented chip or a licensed Neuron chip in every device. This standardizes the communication but leaves gaps in how data is defined.

Why this problematic can be explained by an example: A sensor sends its temperature data to a control unit. The licensed chip in the control unit interprets that it has received a temperature. The sensor could be set to Celsius and the control unit set to Kelvin and these settings can not be modified in a simple way. A simple mathematic formula in the communication could fix this problem but it is difficult since the licensed chip is standardized in a way that makes it difficult to modify. Issues like this can occur when LonWorks products from several producers are used together. This is one reason why many people in the business find LonWorks difficult to work with.

Modbus is a commonly used protocol with both benefits and disadvantages. It is easy to use and work with. The developers like it because it is so easy to modify. This is the same reason why it has disadvantages. Just because it is easy to modify make it easy to do create systems and functions that are not following any standard. This might turn into a problem when other devices are installed in the same system and the devices do not understand each other.

KNX is a protocol that is good when it comes to systems in residential buildings or parts of a larger system. It can easily become complex and hard to work with but for small systems is it a good choice. This makes it suitable for integration at room level and especially integration with electrical applications.

BACnet is a growing protocol standard. It has interest groups in many countries and a lot of companies develop products, which communicate with BACnet.

4.3 Communication between different protocols

The easiest way to ensure the communication is to use one protocol. Then there will be no conflicts or translation problems. This does not mean that the same protocol must be used in all layers of the building automation network. For example it is common to have an IP protocol in the Primary network. Then in Secondary networks, and Field networks other protocols are used. There is often a need for translating between different protocols in a building automation system. Basically, this can be done in three ways as described in Section 3.3.

Drivers are a good way of translating between a few units that need to communicate and use different protocols. With an increasing number of units and protocols used, the number of drivers needed for translations will grow very rapidly, making it an unsuitable solution. Drivers for the purpose of translating between protocols are only recommended for small systems and special applications like hard wiring a fire alarm to a PLC or RTU handling the emergency ventilation.

For a more complex system, gateways or an OPC server might be a better solution. They both have their pros and cons, which can be explained by an example: Several PLCs and/or RTUs that use different protocols need to communicate, this can be solved in several ways. One solution is to use gateways to translate between different protocols. Another solution is to install an OPC server. The solution with gateways is usually a larger investment than the solution with an OPC server. When changes have to be made to the system or major service is required, there are maybe 20 people in Gothenburg that can program these gateways. The only one that has the competence to make changes to the OPC server is the person who initially programmed it. If another person should be contracted to program this OPC server, he or she would need many hours to gain understanding of the system and would be highly reliant on adequate documentation of the system. There are examples of systems that are so heavily dependent on one person that even after this person has changed job, he or she is still bought in as an external consultant when work has to be performed on the system.

4.4 Wireless communication

There is technology, which can handle wireless communication over radio frequency or WLAN, but it is rarely used in building automation. The only fairly common appliance is lighting. The main advantages with using wireless communication are that sensors, switches etc. can be placed anywhere and less wiring is needed. The systems can be more flexible if radio frequency or WLAN is used, for example sensors can easily be moved if they are unsuitably placed. Wireless sensors can also be used to communicate with systems that are located in such way that it is inconvenient to use cables. Investment costs could be reduced on cables and the work to make the layout of them.

In many projects, there is a resistance against wireless technology. One drawback is limitations in range. Investigations have to be made of where to place nodes so all devices can connect to the network. This can be more difficult in for example a hospital compared to an office since there might be lead in the walls that cut off communication. Another drawback is that batteries have to be changed. For many appliances this needs to be done once every ten years. Even though it is not often it might require a significant work effort if the system is not well documented. The

person performing the work needs to know where all devices are, what batteries they are using etc. There might also be a security issue with having antennas in a building automation system. It is possible but very rare that a building automation system is hacked, mostly because there is no motive for doing it. But if the Primary network is shared with an Ethernet network containing sensitive information (for example patient journals), hackers are a more severe problem. The security issue is much less severe for wireless Field networks then for wireless Primary networks. This is because possible intrusions only affect a limited and less vulnerable part of a building automation system.

5 Integration

For the purpose of this thesis a proper definition of full integration would be subsystems working together as one system. This implies that one system has full access to all data and functions of the other systems. Integration can also occur to lesser extent, where some functions of two or several systems are coordinated. Common examples of this type of integration are entity air handling units with integrated control that lets other systems control their set points but do not allow access to individual valves and sensors. Integration can also occur on several levels in a system. On a local level (for example a surgery room), system integration can for example mean that there is feed-forward control that increases the cooling power when heavy heat emitting equipment is turned on. On a more building wide level, system integration can mean that for example when the fire alarm starts a set of events are triggered.

- Emergency ventilation is turned on
- Doors are unlocked
- Elevators are sent to a certain floor
- Evacuation ways are lit up etc.

The ambition and opinion of how integrated all the systems in a hospital should be varies between different projects and people in different positions. One common idea is that the systems should be simple and invisible for the users. It is also important that those who actually will use the systems daily and those who serve them have their say when the system is being designed.

Since every function that is integrated between different sub-systems will make the system more complex, the gain has to be weighed against the extra costs and increasing complexity of the system. If a system is complex and the users lack the competence to operate it properly, there is a risk that the system won´t be used in an optimum way. It might even perform worse than separate sub-systems would, due to functions being used in the wrong way or shut off to simplify the control.

5.1 When to integrate and to what extent

So what system can and should be integrated, and to what extent? The opinions on this question are highly dependent on who is asked.

The market supplies a broad range of products and solutions that opens opportunities for building automation systems with high integration and advanced functions. The term “intelligent buildings” is popularly used by suppliers. Their general opinion outwards is that all functions benefits from being integrated. Examples with some possibilities with a high level of integration are shown in Figure 5.1.

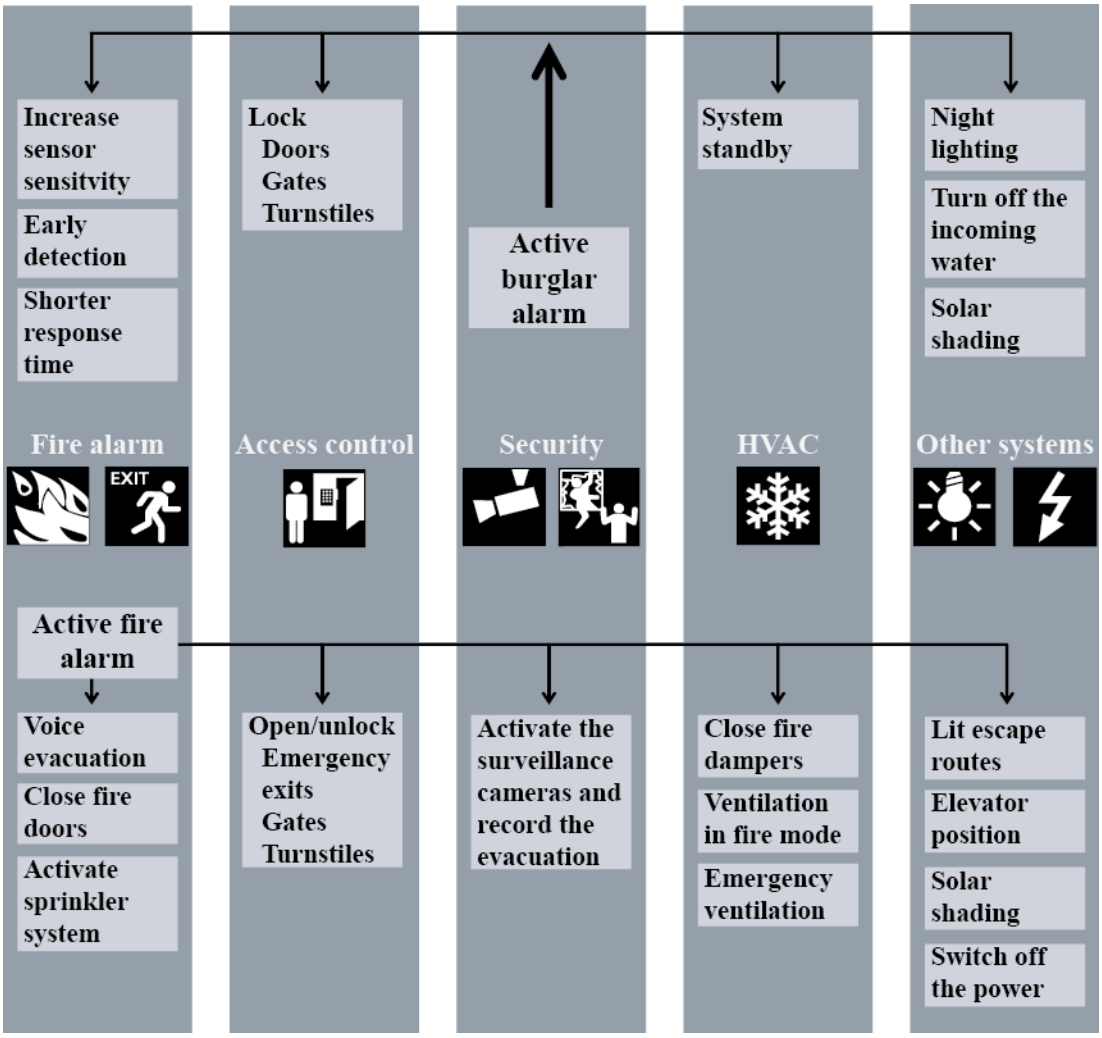

Figure 5.1 Example of a burglary alarm and a fire alarm with integrated functions in a building automation system. Based on figure from Siemens Building Technologies, Inc. (2005)

Even though many opinions differ, there are some points that many people working with building automation agree on. One is that there is a large gain in integrating control of systems that might counteract each other. Examples of these systems are those controlling the temperature in for example a surgery room. Due to the high requirements on temperatures and airflows, these types of complex rooms often have several heating and cooling systems. It is preferable to have all those systems controlled by one PLC or at least that the PLCs controlling the systems are able to communicate smoothly.

For convenience and energy saving purposes, it is often beneficial to integrate lighting with an access system so that lights are automatically shut on or off when a section of a building is unlocked or locked. The integration can be handled in two ways. The access system either sends a control signal to the lighting system, the access system simply shuts down the power to the lighting system or else works the access system as control system for the lighting system. If no really advanced functions are required, then do not make the system more complex than necessary. Many access systems can act as controllers for the lighting in an area, so if there is no need to for special applications (for example adjust color of the light) then this solution usually works just fine.

For most other parts of a building automation system, the opinions of what to integrate are divided. This has to be evaluated from case to case if integration is beneficial.

5.2 Large and advanced building automation systems

Very large projects that require advanced building automation systems are sparse in Sweden. It is mostly when a major hospital or industry is constructed that one of these systems is designed. Every project is unique in its kind and there is often a lack of experience in working with these projects. Construction of a major hospital in Stockholm, New Karolinska Solna, has begun in 2011. The building automation systems are now in the planning and procurement phases.

At New Karolinska Solna the ambition was initially to create a building with a full integration of all technical systems. This integration was not only planned to include systems controlling the indoor climate but also elevators, robots transporting medications, message system, laundry etc. "The world's most modern building" have been used to describe the project. In a later stage in the planning process, the level of integration was reduced to not include control functions for many systems. The aim now is to have a full integration on room-level and a SCADA system for the whole hospital that handles surveillance and alarms. There were two main reasons for the change of aim.

- The cost was too high.
- Lack of competence in the design stage, there were not enough companies that can perform a contract of this size.

The total cost of a system is affected by many factors and can be hard to predict. One factor making it extra difficult for larger projects requiring a high level of integration can be explained by a dilemma. Since all large contracts in building automation are unique, there is no standard for how to integrate all subsystems. This is especially true for hospitals, since they have special demands and equipment. The integration of a number of subsystems then requires a large amount of manual labor for programming, testing and trimming. It has to be specified for every PLC and RTU what values to obtain from other sub-system and what values to send. If the sub-systems are from different manufacturers, the values and messages might not be in the same format and has to be converted. This is common even if the sub-systems use the same protocol and are similar on the paper. The extent of this problem is dependent on what protocol being used. Conversion between formats requires extra labor and increases the risk of errors which increases the cost. To simplify the system and reduce this cost, it could be specified in the procurement that PLC and RTU with integrated control should be supplied from the same manufacturer, or at least follow a validated standard for communication. This might have complications in the procurement process and will be treated further in Section 6.1.

A related problem has been experienced during the construction of a hybrid ward, combined ward for surgery, x-ray etc. at Sahlgrenska University Hospital. In this case a PLC was used to control electrical installations and a RTU was used to control ventilation and heating. Quite high levels of integration between these two devices were needed. The PLC and the RTU were from different manufacturers and were programmed separately. When the system was tested several of the integrated

functions did not work satisfactory. To solve these issues, drivers for how one device interprets messages from the other one had been written manually. Other problems encountered where set-points set in the PLC, sent to the RTU and then changed in the RTU without being changed in the PLC. This resulted in the operator's panel showing obsolete data about the system. These errors is a result of gaps in the requirement specification, it was for example not specified where data should be stored in the system. Problems like those described here are fairly common in larger building automation projects.

5.3 Choice of control units

There is a rapid technological progress in technical equipment used in hospitals today. Many of the devices installed today have a lifespan shorter than 10 years before more modern ones will replace them. Since there are many of these devices in a surgery, and even more in a hybrid ward, the set of equipment is often altered. It is also desired that the personnel in the room can read the status of all devices and control some of them from one HMI. This imposes extra demand on the room-wide control system. In these types of advanced rooms, it is preferable to integrate systems using a PLC rather than a RTU. This is because a PLC has better opportunities to be modified and be expanded. Since processing power is relatively inexpensive compared to labor it might even be a good idea to oversize a PLC in order to ensure future compatibility.

Another ongoing trend in building automation is the increasing use of entity units with integrated control, described in Section 2.3. They have several advantages compared to separated control systems:

- The price is usually lower for a entity unit with integrated control then for buying the unit and the control system separately.
- There is less need for designing a control system since this is already partly done by the manufacturer.

There are also disadvantages with entity units with integrated control compared to separated control systems. The main points are:

- There might be limited capabilities to customize and connect extra devices to the RTU controlling the system.
- The system is limited to the predefined RTU and its communication capabilities; this limits the protocols to select from for communication with other RTU/PLC and SCADA-system, what kind of data that can be accessed from other systems etc.

These pros and cons make entity units with integrated control a good choice in buildings where the activity is not subjected to change over foreseeable future and does not require special customizations. They are not so common in hospitals but many believe that they will be more common in the near future. This is due to the products being more developed and the disadvantages are becoming less fragile.

6 Organization

In order to construct and operate a building automation system in a good way, there is a lot to think about. Many of the problems encountered are results of deficient system documents and procurements.

6.1 Procurement process

The Public Procurement Act governs procurements concerning hospitals. In a public procurement process, the standard is that consultants specify the function of a PLC or RTU and that the contractors can pick any unit that fulfills this function. High requirements are then put on the consultants designing the system to specify the functions so that the contractor ends up installing a system that satisfy the customer. The complexity of this task is increasing with increasing integration. It is simpler to integrate functions between PLCs and RTUs using the same protocol and even simpler if they are certified by the same standard. So why not put these requirements in the systems document?

- The range of products to choose from is narrowed which can be a problem due to less competition and higher prizes in the procurement process.
- There are problems for the public sector with specifying too narrow requirements in the procurement since it may exclude suppliers and violate the Public Procurement Act.

This dilemma is a major issue in many building automation projects. What often happens is that consultants write vague specifications in the systems document and miss to specify several important functions. According to the Public Procurement Act, contracting authority may not impose greater requirements on the supplier than is necessary and may be considered appropriate for the procurement. If a supplier have been disadvantaged due to this principle or any other part of the Public Procurement Act not have been followed, they may take legal action against the contracting authority. So basically, requirements in the systems document have to be well motivated.

Prescribing that several PLCs or RTUs come from the same manufacturer may be difficult to motivate but is has been done in special occasions. It has been prescribed for the room level integration in hybrid wards in Sahlgrenska University Hospital, BOIC - Bild- och interventionscentrum (Center for images and intervention). Prescribing what protocol a PLC or RTU should use for communication is easier to motivate because it can simplify communication and reduce the need for drivers, gateways, OPC-servers and programming without excluding too many suppliers from the procurement. These prescriptions are common in larger building automation projects where integration is required. But the fact that several PLCs and RTUs have the same native protocol does not imply that they communicate without errors and need for translations. How well integration works is also dependent on what products are used, how they are programmed etc.

A common way of handling a procurement process in hospitals is to procure a general contractor that then procure contracts for each sub category like electricity and HVAC Even if other parameters are taken into consideration and weighted, the totally dominant parameter when choosing general contractor in a public procurement

process is the total cost. There need to be very special circumstances for a contracting authority not to choose the contractor who offers the solution with the lowest total cost. The total cost can be divided into two subcategories, investment costs and operating costs. A general contractors undertakings varies, operation for a number of years may or may not be included in the procurement. If not included, it may be difficult for the contracting authority to get an overview of the total costs. This may in the worst case result in a solution with low investment cost, but high total cost. So what key factors decide the operating costs of a building automation system?

- The need for service.
- Availability and cost of competent people that can serve the system as described in Section 4.3.
- How easy it is to make changes in the system for future appliances.

These points once again stress the importance of competent consultants writing the system documents. They need to have knowledge about how easy it is to serve and make changes to different systems.

If operation and service of a system is not included in a contract, a contractor will aim for the solution with the lowest investment cost that fulfills the function specified in the system documents. If there are gaps or errors in the systems document, the control system contractors are free to neglect them in the procurement process. Then in a later stage of the project, they can sell extra equipment and consulting hour to solve the problems. Views are divided on how common and how intentionally this behavior is. Major control system contractors have been accused for dumping the price on contracts and neglecting gaps and errors in the systems document to be able to sell extra equipment and consulting hour at high prices. The result is problematic systems and high costs.

6.2 Responsibility of the function of a building automation system

A related topic is responsibility. Who will take the extra costs when a building automation system is not working as intended? For the case described in the previous paragraph, it is most common that the contracting authority will take the extra cost. If the problems are a direct cause of errors in the system documents, then the consultants who wrote it can be held responsible. Even though this is a possibility, it is rarely used in practice. The main reasons are that it is often complicated cases with many parts involved and nobody really wants to risk being involved in a legal twist. If the building automation system fails to provide a function that is described in the system documents, then a contractor is responsible. Since there are usually several contractors involved in a building automation project, it may be difficult to clarify who is responsible. This is especially true for functions that require integration and even worse if there are several contractors for the control of integrated units. The most common is that a control contractor finds an error and tries to correct it. Even if the error is not due to this contractor, he will usually end up solving the error, spending extra hours that may be difficult to invoice. If the error is due to a malfunction in a product or a product not meeting the specifications, it will often be the case that the burden of proof lays on the control contractor. To simplify this problematic, it is recommended to only use one control contractor for several PLC and RTUs that

integrate. The other case would be having the HVAC contractor programming a HVAC RTU or PLC and having the electrical contractor program an electrical PLC or RTU. If they require integrated functions and they fail it will be a difficult task hold one of them responsible.

The earlier an error is found, the cheaper it is to correct it. In order to find errors before a building automation system is put into service, a coordinated testing should be preformed. It could be specified in the procurement that all contractors should take part in coordinated testing of their systems. To avoid twist and extra costs it is also important to clearly state the boundaries of the responsibilities of all contractors. This is often deficient in many procurements processes.

6.3 Operation of a building automation system

The service organization for a hospital has generally a higher level of competence and more knowledge about their building automation system then service organizations for office and residential premises. There are usually service personnel with competence for all the separate systems like elevators, electricity, HVAC etc. It is also common to have personnel with fairly high control competence. What is usually lacking is systems integration competence. For work in the building automation systems requiring this competence, the service organizations are usually highly dependent on buying these services. Since a large part of the systems are so complex that only the control contractor can work in them efficiently, the service organization will be more or less bound to one or a few persons for these services.

There are three actions that can be taken to make a service organization less dependent on a few people.

- Design systems that do not require a large effort to gain understanding of.
- Demand adequate documentation of the system.
- Demand copies of the source code used in the software.

These last two points are often lacking in many projects for several reasons. First of all, the contractors can benefit from not handing out documentation and source code and are therefore not so willing to hand out source code for their products. Documentation are usually done and handed out, but for complex systems there are many makeshift solutions, workarounds and fixes that are poorly documented and will take any other person than the author a large effort to gain understanding of.

7 Guidelines for building automation systems with complex requirements

This chapter contains guidelines useful when designing, procuring and managing building automation systems with complex requirements. They are developed with a hospital in mind, but many of them are general and apply to other systems with more or less complex requirements. The guidelines are based on conclusions from the chapters 4 to 6 and the authors own opinions.

- *Use a legitimate level of integration.* For many applications it is enough with a lesser level of integration. So chose an as simple solution as possible that fulfills the desired function. For example simple local control of lighting by an access card terminal instead of a more advanced lighting control system with remote control etc.
- *Chose solutions, products and protocols for which there is broad competence available.* This will make a system less dependent on a few persons and companies for service and modifications. For example use one protocol in the Primary network and connect Secondary networks and devices that have other native protocols through gateways. It might be a higher investment cost then other solutions with drivers or OPC but the system will be simpler to gain understanding of and it is easier to find competent service personnel.
- *Chose control units that can handle future alternations where it might be needed.* In a hospital environment the operation is subject to change and so are the building services systems. Therefore PLCs that can be reprogrammed, modified and expanded is often a good solution. On the other hand, for systems that are not subject to future alternation a solution with a entity unit with integrated control can save costs.
- *Share communication infrastructure for the Primary network with the regular LAN.* Large investment costs can be saved by this implementation and today there is no mayor technical limitation for implementing this in a safe way. Only communication infrastructure with special demands should be kept separated, for example fireproofed cables for the fire alarm.
- *Do not make a system that is too complicated for the service personnel working in the building.* The competence of service personnel in hospitals is generally higher than in many other areas but it has its limitation, often regarding integration. If possible, involve the personnel in the design of new systems. They often have good knowledge of what systems that is convenient and reliable in the everyday operation of a building.
- *Involve control and monitoring consultants early in the design process.* In many cases it is just a simple handover from the consultants designing the systems that should be controlled. These consultants often have little knowledge of control and monitoring. By involving control and monitoring consultants earlier better solutions can be designed instead of try solving worse solutions with unsatisfactory results.

- *Use one control contractor for all systems, which have a high level of integration with each other.* There can still be different suppliers of the components but only one contractor should perform the programming. This will reduce the risk for malfunctions and if they occur, it will be simpler to hold one responsible.
- *Appoint a coordinator for the building automation system.* This is especially important for projects involving many contractors and requires a higher level of integration. The main gains are that problems can be discovered earlier and conflicts over responsibilities can be avoided.
- *Perform a coordinated testing of the building automation system.* It is a good idea to have all involved contractors performs a coordinated testing to find errors and ensure the function of a system before is put into use. This responsibility could be put on the coordinator mentioned in the previous paragraph.
- *Secure access to source code.* If possible, demand copies of source codes. Since many companies are very restrictive with handing out their solutions, this is often not possible. To ensure access to source codes in the case of closure of a supplier, it is a good idea to write a contract stating that, a copy of the source code should be stored in a safety deposit box to which the customer gains access in case of a closure of the supplier.

8 References

Publications:

Bailey D. Wright E. (2003): *1 – Background to SCADA*. BEng, Bailey and Associates, Perth, Australia.

Echelon Corporation. (1999): *Introduction to the LonWorks System*. Echelon Corporation, Palo Alto, USA.

ISO/IEC (1994): *ISO/IEC 7498-1 Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.* ISO/IEC, Geneva, Switzerland.

Levermore G. et al. (2000): *Building control systems*. CIBSE, London, United Kingdom.

Marshall P. (2001): *A Comprehensive Guide to industrial networks.* Sensors Magazine, June 2001. Also available at: http://www.perrymarshall.com/articles/industrial/part-1/

Samjani A. (2002): *Mobile Internet Protocol.* Potentials IEEE*,* Vol. 20, No. 1, February/March 2001.

Sharp R. (2008): *Principles of Protocol Design.* Springer-Verlag, Berlin Heidelberg, Federal Republic of Germany.

ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (2006): Handbok *för Hem- och fastighetsautomation.* ZVEI, Frankfurt, Federal Republic of Germany.

Online sources:

Hollinger C. (2011): *Automation, Integration & Standard Protocols*. Available at: http://www.ctashrae.org/Hartford%20ASHRAE.ppt [Accessed 8 August 2011].

KNX Association (2011): *KNX Standard.* Available at: http://www.knx.org/knx-standard/introduction [Accessed 15 December 2011].

Sena Technologies, Inc. (2002): *Introduction to MODBUS*. Available at: http://www.sena.com/download/tutorial/tech_Modbus_v1r0c0.pdf [Accessed 28 November 2011].

Siemens Building Technologies Inc. (2005): *BACnet Information Guide*. Available at: http://www.buildingtechnologies.siemens.com/bt/us/SiteCollectionDocuments/sbt_internet_us/2726_754.pdf [Accessed 5 December 2011].

Z-Wave Alliance (2011): *Z-Wave Start.* Available at: http://www.z-wave.com [Accessed 29 June 2011]

Appendix

APPENDIX A – MODBUS

APPENDIX B – BACNET

APPENDIX C – KNX

APPENDIX D – THE LONWORKS PROTOCOL

Appendix A – Modbus

Modbus is a protocol used in both industrial manufacturing environment and building automation systems, for communication in a master-slave system. Modicon developed the protocol in 1979, Hollinger (2011).

There are mainly three versions of the Modbus protocol.

- Modbus ASCII
- Modbus RTU
- Modbus TCP

The ASCII and RTU version is transmitted over a Modbus serial network as compared to Modbus TCP where the protocol is used over an Ethernet network and in this case the protocol is defined as a server-client protocol.

Serial Modbus is designed to send messages between master and slave devices in a network. The master is often a RTU or a PLC. The slave device could be I/O transducer, valve or any other intelligent measuring device. This concludes that serial Modbus is used for communication over the Field network in a building automation system. Modbus works in that way that only one device can transmit on the network at a time and it is always the master that initiates the communication. The master could either request data from a specific slave device or instructs it to perform a certain task by sending a Modbus message. If a request or an instruction is sent to a slave device it must reply to the master. The master could also send out a message to all devices it is connected to, so called broadcasting. In this case the master does not wait for a reply from any device.

A Modbus message is placed in a message frame and this contains.

- Start
- Address
- Function
- Data
- LRC/CRC (error checking)
- End

Modbus ASCII

If the system is configured for ASCII transmission the character byte in the message frame is represented by two ASCII characters, Sena Technologies, Inc. (2002). This mode for transmission allows relatively long time intervals, up to one second, between two characters without creating an error. The slave devices monitors the network constantly for a message start character, represented by a ":". When a slave device receives a start character, it analyses the address field to determine if the message is addressed to that specific device.

Modbus RTU

Two 4-bit Hexadecimal characters represent the 8-bit message byte in a Modbus RTU network. In this transmission mode there is no character to represent a start of the message sent, instead the start of a message is represented by a silent interval of 3.5 character times. That is 3.5 character times is the time of one character at the baud rate used in the network multiplied by 3.5. As for the ASCII mode all slave devices monitor the network for the start of a message and when a silent period matching the requirement for a start of a message the devices then analyses the address field to see if the address is a match to its own address.

Error checking

There is two ways of perform error checking.

- Parity checking
- Frame checking

Parity checking is used for simple error detection. The device could be set for, even, odd or no parity. What it does is that it counts the number of 1-bits in a 7-bit character, if the parity is set to even mode and the character has a odd number of 1-bits it will add 1 as the parity bit to make the transmitted set of bits even. If the 7-bit character is even on it own it will add a 0 as the parity bit. An example of how it works can be seen in Figure A.1.

Transmission using Even parity

A wants to transmitt:	10101
A computes value of the parity bit:	10101 = 1
A adds parity bit and sends:	101011
B receives:	101011
B computes parity :	101011 = 0

B answer that transmission was correct for expected even parity.

Figure A.1 Example of a transmission check using even parity.

Frame checking is different for the respectively ASCII and RTU transmission mode. For ASCII the frame check is a LRC – Longitudinal Redundancy Check, and it is the last field in the character frame that contains a LRC calculation of the message except for the start and end character. In RTU the frame check is a CRC – Cyclic Redundancy Check, which is a specific error-checking field in the Modbus message that contains the CRC calculation of the message.

Modbus TCP

To make the protocol more suitable for modern networks a new version of Modbus was developed 1999 by Modicon/Schneider Electric, Modbus TCP. Modbus TCP is basically a Modbus frame embedded in the TCP frame. This allows sending Modbus messages over an Ethernet network and makes it possible to access the system via the web. Modbus TCP is used for communication on the primary network in a building

automation system. The serial Modbus and Modbus TCP are not natively compatible but they can be integrated by using a gateway to translate between the two protocols.

License and testing

Modbus Organization has since 2004 been handling the Modbus protocol. The protocol is released as open software and all documentation and specifications can be downloaded without any charge. Members of Modbus Organization can also download development tools and samples of implementations.

Modbus Organization does also perform testing and certification of products developed for Modbus ASCII, RTU and TCP. It is not mandatory to apply products for testing and certification, which mean that products can be sold as a Modbus product without following the standard implementation rules.

Appendix B – BACnet

BACnet is an acronym for Building Automation and Control Networks. The BACnet protocol was developed by the American Society of Heating, Refrigerating and Air Conditioning Engineers, ASHRAE. The reason why the protocol was developed was to meet the requirements for communication in building automation, Levermore et al. (2000). The protocol was first released as an ANSI/ASHRAE standard 1995 and since 2003 is BACnet also an international and European standard.

Objects

BACnet is an object-oriented protocol. The entire protocol is designed on objects with different properties. Every product in a BACnet network must have a device object. The device object contains a list of what objects are implemented for that specific product, Siemens Building Technologies, Inc. (2005). To be able to trace devices and objects in a network each device and its objects contain an Object identifier.

The Object identifier contains of 32 bits that are divided in two parts, 10 bits for object type and 22 bits for the entity number.

Manufactures can develop their own objects if that is necessary. There are some required properties that must be included in both manufacture developed and standard objects so the system can adopt them. Some of the required properties are.

- Object identifier
- Object name
- Object type

Services

To enable exchange of information between different BACnet devices services is used. There are five categories of services classes implemented in BACnet; these contain services that can perform different tasks.

Alarm and Event Services

These services take care of changes like change of value of a sensor, an event that indicate something should happen, or an alarm that indicates errors. For example a device can subscribe to a object of a specific device and when there is a change of value, (COV), the subscribing device will be notified.

File Access Services

This service has the ability to read and write to files in a BACnet device.

Object Access Services

These services can access and modify objects in the system. The main functions are to read, write and change the properties of an object but it can also add new or delete old objects that are no longer necessary.

Remote Device Management Services

Services listed in this category are used to access a device remotely and change settings for the device. Included here are also the functions to identify and locate devices in the BACnet network by using the services Who-Is and I-Am. What kind of objects that a device contains, can also be identified with similar services.

Virtual Terminal Services

This service is used to establish a text-based connection to an application on a remote device.

Communication

The protocol is designed for server/client techniques to communicate between nodes in the network. The communication can be initiated as a polling sequence where the server asks the client for the value of an object and the client replies with the object. The communication can also be initiated by an event that indicates that something has changed. If some device is subscribing to changes of that object then the connection will be established. This way of initiating communication can be done without a central server. This is a so-called peer-to-peer communication principle.

Transport

The architecture of the BACnet protocol is layered and based on the OSI-model. It is designed to use the Physical, Data Link, Network and Application layer as can be seen in Figure B.1.

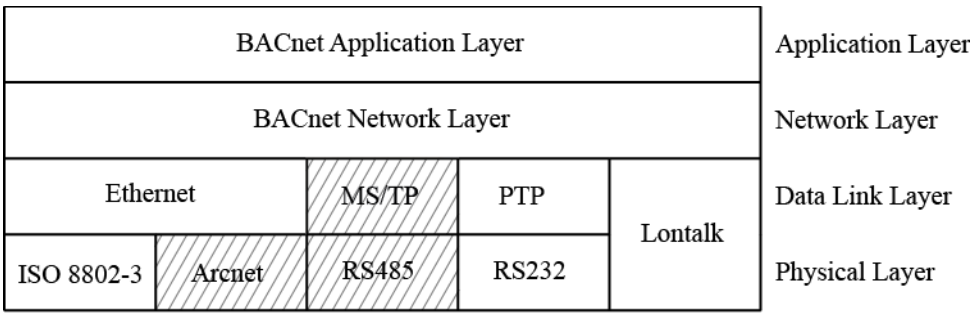

Figure B.1 BACnet layer architecture.

There is five ways to carry the data with BACnet that can be seen in the two lowest layers in Figure B.1. MS/TP, Master Slave/Token Passing, and Arcnet is not included in the European standard but is used in America. The most common of the other transport ways is BACnet/Ethernet that can also be referred to as BACnet/IP.

BACnet is usually used in the Primary network in the topology of a Building Automation System. The different ways of transporting the protocol can be combined by using a router to convert from for example BACnet/LonWorks to

BACnet/Ethernet. It is also possible to use BACnet/Ethernet in the Primary network and connect Secondary network by using a proprietary protocol via Gateway to convert the language.

License and testing

BACnet is released under GPL and has no license. BACnet International is the international organization that looks after the interest of BACnet such as future development, meetings where products are tested in networks. There are sub groups to BACnet International that are located in countries all over the world, like BACnet Interest Group – Sweden (BIG-SE). BACnet International also has an organization for testing and listing of tested products, BACnet Testing Laboratories (BTL).

Appendix C – KNX

KNX is a worldwide standard for communication between building technology systems, KNX Association (2011). It is an OSI-based network communication protocol, which was developed from three previous standard protocols EIB, EHS and BatiBUS.

Communication

The architecture of KNX is based on the OSI-model. It is a simplified version of the reference model, which mean that not all seven layers are included. The KNX protocol is using five of the layers and leaves the Session and Presentation layers empty.

For communication in the Physical layer there are mainly three different medias to choose between.

- Twisted Pair
- Power Line
- Radio Frequency

Both the twisted pair and the power line communication mediums are inherited from the EIB standard. Twisted pair means that data and power is transmitted over one twisted cable. Power line means that data is transmitted over the power line in the building. The communication mode over each media is half duplex, bi-directional. This means that communication direction is one way at the time and the reply is sent back over the same line.

Radio frequency is the solution for wireless communication; it is developed for short-range devices.

Telegram

KNX is using telegrams to send information over the network. The telegram is a sequence of fields containing necessary data to ensure that the telegram is sent to the right device and that all data is reaching the destination. The design of the KNX telegram is varying with the media that transport it, ZVEI (2006).

For twisted pair the telegram looks as in Figure C.1. The telegram for twisted pair is also called KNX core telegram. The control, routing, length and checksum fields purpose is to ensure that the telegram is complete and don't miss any data when the transmission is performed. The source and receiver addresses are the physical address of the device transmitting and receiving the telegram. Data field contains the essential information that should be transmitted for example instruction, temperature or a message.

Control 8 bits	Source address 8 bits	Receiver address 16 + 1 bits	Routing 3 bits	Length 4 bits	Data field 16 x 8 bits	Checksum 8 bits

Figure C.1 KNX telegram for twisted pair, ZVEI (2006).

For communication over power line the twisted pair telegram is embedded in some additional fields, specific for power line networks. It is a synchronization field containing a binary sequence and the two preamble fields are transmitted which indicate the start signal for the receiver. Then the twisted pair telegram follows and it all ends with a system id field. This last field contains information about which devices that can receive the message, only devices with the same system id can communicate with each other. The power line telegram can be seen in Figure C.2.

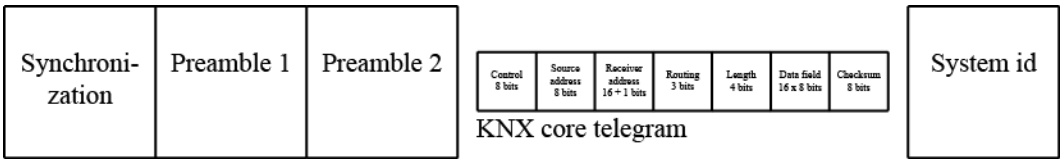

Figure C.2 Power line telegram for KNX.

The telegram is a little bit different when the physical media is radio frequency. It is transmitted in several data packets. The telegram starts and ends with synchronization packets. The data packets are then separated with checksums. The telegram can be seen in Figure C.3. Data packet 1 contains a control field, KNX serial number, and a checksum. Data packet 2 contains a control field, source address, receiver address, the important data and checksum.

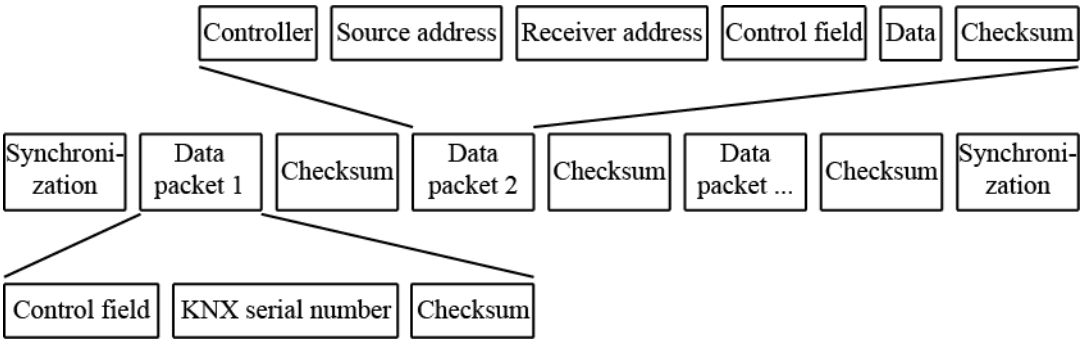

Figure C.3 Radio frequency telegram for KNX.

KNX IP

It is possible to use an IP network as a transport medium for KNX. The architecture of KNX IP is based on the OSI-model and is embedded in the Internet Protocol suit.

Network level

KNX is mainly used in the field network but KNX IP makes it possible to use the protocol in the primary network as well. There are also a lot of routers that can be bought to convert the KNX protocol to other protocols as BACnet and DALI.

License and testing

To be able to get all the documentation and specification of KNX a membership with the KNX Association must be established. This membership works as a payment or a license to use any developed products for KNX. KNX Association provides testing and certification of products developed for KNX. The main reason to certify products is to ensure that the product will be compatible with other third party developed products. Products tested by KNX Association will also be branded with the KNX logotype as a confirmation that the product follows the standard.

Appendix D – The LonWorks protocol

The LonWorks protocol is also known as the LonTalk protocol. The protocol is used in LonWorks networking platform, Levermore et al. (2000). It was developed by Echelon Corporation and was accepted as an ANSI standard in 1999 (ANSI/CEA-709.1-B). The protocol is based on the OSI-model and uses all of the seven layers. The layers have different tasks to perform, Echelon Corporation (1999).

- Layer 7 - Application compatibility
- Layer 6 - Data interpretation
- Layer 5 - Control
- Layer 4 - End-to-end reliability
- Layer 3 - Message delivery
- Layer 2 - Media access and framing
- Layer 1 - Electrical interconnection

Communication

A message with the LonWorks protocol is sent with one or several packets. A packet contains data for each of the seven layers. The data is compressed which makes the packets small and increase the efficiency when transmitting over the network.

There are several physical media to carry the LonWorks protocol. The most common are twisted pair, power line and LonWorks over IP. The communication can also be performed over radio frequency. The differences between the media are mainly the bit rate i.e. the speed of the network, how many devices that can be attached and the maximum distance of cables in the network.

There are different ways of addressing the packets to ensure that they are delivered to the correct address and to a minimum cost of bandwidth.

- *Physical address.* Each device has a physical address. This address is unique and the same from when the device is manufactured to the end of its life cycle.
- *Device address.* Device address is given to a device when it is installed in the network. This is mostly used instead of the physical address because it increases the efficiency of the routing in the network. The Device address has three sub headings that are domain ID, subnet ID and node ID. Domain ID is used to check if two or more devices can communicate, the domain ID must be the same to allow communication. Subnet ID is used to group devices in a sub network. This might be useful in large networks. Node ID is the individual identifier in a sub network.
- *Group address.* Group address is used when a message should be sent to a significant number of devices, more efficient than using broadcasting.
- *Broadcast address.* Broadcast address is a complement to Group addresses.

There are four different types of messages that can be transmitted with the LonWorks protocol.

- *Acknowledged messaging.* Acknowledged messaging requires the receiver to respond to the transmitter to tell that the message was transmitted and received.
- *Repeated messaging.* Repeated messaging sends a message many times to a significant number of devices. It is mainly used when broadcasting because it does not wait to get a confirmation from the devices it transmits to and this will avoid creating collisions in the network.
- *Unacknowledged messaging.* Unacknowledged messaging is transmitting a message to several devices once and does not require a response.
- *Authenticated service.* Authenticated service is similar to an encrypted message checking. The purpose can be to check if a host has the right permission to send a message to a receiver.

Network level

The LonWorks protocol can be used in both the Primary network with LonWorks over IP and in the Field network with the other medium to carry the protocol.

License

The LonWorks protocol itself comes without license requirement and it is possible to implement the protocol to any microprocessor. However Echelon Corporation still sells the Neuron chip, which has the LonWorks protocol implemented. In the past was it required to purchase the Neuron chip to be able to use the protocol.