MSc Thesis

# Integrated Smart Buildings Communication and Networks

Puvishanan S. Naguleswaran (s131250), 26.02.2016

Department of Applied Mathematics and Computer Science

Technical University of Denmark

Technical University of Denmark
Department of Applied Mathematics and Computer Science
Building 324, DK-2800 Kongens Lyngby, Denmark
M.Sc. report, ISSN: 1601-233X
www.compute.dtu.dk

## Abstract

From the moment we wake up, we are surrounded by technology. Many organizations such as educational institutions, hospitals and airports work within strict budgets while also improving services. Schools too, have to provide the best learning environments for children and students while working within limited budgets. However, there is an answer in maintaining exceptional energy efficiency in schools while saving money on energy expenditure and this money can be used to improve schools in ways such as hiring teachers or providing more technology for students and so on. These are big challenges as there are lots of schools with different building types, these buildings, old and new, offer challenges in bringing in old facilities along with new facilities. For these challenges, there are Smartstuxure solutions, enabled by the StruxureWare building operation software. Implanting the Smartstruxure solution into the facilities gives the user handling of the entire buildings and energy. The product will help the user to migrate all the old legacy systems into new generations. Smartstruxure solutions allows the district to monitor and measure energy as a granular level which means it can make decisions on how to manage energy use in real time. As it will be able to see all the connected equipment, the district can implement proactive maintenance to decrease the equipment failure and respond to problems much more quickly. Their users are able to use mobile devices from any location to monitor the schools and make adjustments. Moreover, the user is able to pull in BACnet, LonTalk or Modbus network paths on several different protocols in the system to monitor and control third party systems. These network paths are also able to communicate with each other through a controller and can be accessed through an Internet of Things system. The main benefit through using Smartstruxure is to help provide greener features and save money for further benefits. The project is focused on to create smart algorithm, which will help the user to control and monitor the entire buildings and energy consumptions. Moreover focusing on to have Building automation and control managed network (BACnet), which is designed to have services and data communications protocols used for control and monitor the building systems. These provide BACnet/IP for interfacing it to Internet. To do the interfacing there are BBMD (BACnet Broadcasting Management Device) placed to maintain the communication link between devices inside and outside the buildings. This integration method shows how the BBMD devices can be used to have communication in the BACnet/IP network.

# Acknowledgements

Honestly I would like to thank my supervisor Assoc. Prof. Christian D. Jensen for always be available for feedback and taking interest in this thesis. Especially his patience and interest has motivated me to do my thesis.

I have to give my honor to Mads Skyth Larsen at Technical University of Denmark for his help and time. His insights and ideas were helping me to get well on with my thesis and gave more confident to full fill my work.

In additions I have to thank my family members, who were supporting me to complete this thesis. Especially my wife was giving me the strength and support to finish my thesis. Through the situation I have learned how important my family is for me.

DTU, February 26th, 2016

Puvishanan Sundram Naguleswarn

# Contents

# 1 Introduction

The Building Management System (BMS) or more recent terminology Building Automation System (BAS) focuses on controlling and managing buildings in a computerized ways. Its sensors and software can focus on saving energy and control pollution. The current focus is to develop technologies in a way which is capable of saving energy and giving comfort for the residents. BMS has been created for different kinds of purposes and is still under development [1]. The purposes are to monitor and control the equipment's such lighting, security systems or ventilation etc. Meanwhile the government's focus is to raise environmental protection and to reduce energy consumption.

When we look at previous BMS systems, we can see they were able to cool and heat rooms but didn't have any live control of the rooms or areas. With the improved system, they can now control the cooling and heating in better way with some reduction in energy use. This means the current technology is able to help the user by saving and managing the system efficiently. Security is also one of the main factors in building automation, especially in residential buildings. Moreover, there is flexibility in the design to allow for adaptation for use in older offices and buildings, while making the process easy and comfortable.

There are also more comfortable ways to access the facilities with some specific management tools from workstations. On the other side BMS becoming more complicated as well where lots of devices are deployed into buildings for growing number of control functions (heating, lighting, ventilation etc).

My work can be summarized as follows: There are lots of different hardware and Software available for designing the BMS. It is difficult to look at each individual development. However after research on several technologies, in this work I have chosen to use Schneider Electric Hardware /Software tools which you can read from the following chapters. The intention of the project is to create an algorithm and network architecture for intelligent energy efficient buildings.

Chapter 1: Gives an overview of the BAS where and how it can be used. That means the reader should be able to read about the actual idea of the BAS, such why it is important to use the system and what benefit do we have out of it etc.

Chapter 2: Looks at state of the art more detailed description on what type of technologies are available and how it can be used in our everyday life depends on what technologies are applicable at the present.

Chapter 3: Discussions on how the Struxureware software works with the created algorithms. Three different algorithms presents which has different purposes and uses for the current and feature use on BMS.

Chapter 4: Gives more details description on how the algorithms can be used in a networked architecture structure and for further use and developments.

### *1.1 Advantage on having Building automation system*

It depends on how the system structure are designed and what functionality it has. The buildings structure gives more details on energy savings like newer buildings are structured in a way where they need smaller amount of energy on lighting and heating or cooling of the buildings. In fact the newer buildings have bigger windows which gives more sunlight inside and can be adjusted with energy consumption. Nowadays most of the peoples are working next to each other in the offices which reduce energy on heating and lighting [1]. Earlier, most of the employees do had individual offices for them with separate heating and ventilation systems but now as they are mostly working next to each other some of the heating and ventilation can be reduced or avoided. In this manner they are able to save cost and reduce energy use. When we look at the BMS system is actually an integrated system with Open Platform Communication (OPC) server by controlling HVAC system. That means the OPC server gives the user a complete graphical display interface according to the integrated components. For more details description on OPC servers see chapter 4 on Solution and improvements on BMS architecture. Through the graphical interface the users are able to follow the building indoor energy consumption and indoor climate. Moreover, the graphical interface encourages the user to save energy and maintain the energy efficient behavior. Which motivates people have intention to save energy and water bills.

We have to bear in mind that waste and consumption is a major concern for either small or bigger buildings. We are under pressure to clean our environments as we have polluted our nature. At moment we are able to use smart technologies that do mostly everything for us, but we have to find the right way to utilize the technologies. First, we have to identify the types of Buildings we are going to adapt BAS. If the buildings are not well isolated, they have effect on losing energy, then it is not beneficial to place expensive controllers and sensors in the buildings. Second when it comes to using floor heating system, it has more beneficial profit than keeping the existing radiator heating system. To choose the proper systems for the building is much harder to place them. We have lots of opportunities on technologies and lots of companies are providing smarter and clever way of support. However there are issues as well, in the perspectives of the communication gateways and device supports. As we are in the busy world we are filled with stress and time pressures which make us rely on these technologies. These systems help us to manage and control our buildings in a good manner.

For this point of view, the system should be smart enough to save energy and provide comfort by techniques of remote access the systems via sensors and controllers, and to adjust temperature level and environmental conditions for the user while controls itself without human Interactions. This technology can significantly lower the operating and energy costs over the long term.

The main idea is to make the buildings smarter where the users are able to get benefit out of it. In this case there are lots of companies working on progress to make the BA system more efficient and smart. Most of the controller are designed to work with pneumatics which replacing the electrical and analog electronic circuit. For example, direct digital control (DDC) system is used for buildings to computerize HVAC controllers, so that users are able to control remotely from the automatic controllers on HVAC which will help to improve and maintain the system. In the early 70s the oil price shock was hit the world and consequently started out the development on power saving operation, like start and stop control on light or heating. For this purpose there are some supervisor control system introduced like (SCADA; CCMS). This Supervisory control system gives the user control over the entire building without being on-site. There are lots of options on how the energy can be controlled and saved. For instance, through the supervisory control system the users are able add days (Stop any function for some minutes) where the building or the place is not in use. Users are able to turn off any activities in the room or building (light, heating) which reduce energy consumption. In the 3rd Chapter you can read more about SCADA.

### *1.1.1 Building Management System Communication*

In this paragraph we are going to look at BMS automatic mechanism for the conditions of indoor environment. The main focus for BMS is to improve interactions between devices which are found indoor. This writing focuses on high volume automatic functional buildings such as office, shopping centre and department store. The primary goals for the current researchers are to realize significant savings in energy and cost. All of the building and home automation systems are deviated from each other to get a better interaction between devices. Through the smart algorithm integration all the devices from small to larger buildings will be managed and improve energy efficiency. The shopping centers require huge space and normally have complex structure, it could be designed in different ways compared to smaller or residential buildings [2]. That means there are more controllers and sensors needed to cover the area and appropriate algorithms needed for the BAS. The algorithms should be able to control and maintain the system.

The key point of the building automation market is the management of users' comfort and the reduction on operation cost. In order to achieve this, BAS adopts optimized control schemes for HVAC system. Since energy efficiency plays a big role nowadays most of the peoples would like to be green in a sense to save our planet. It can be achieved by accessing all the building services by centralized control and monitoring central system. By providing these options all the faulty conditions can be detected or corrected in the early stage to reduce or avoid further damages and waste of energy. For instance damaged sensor for heating control can be fixed in advance before wasting the energy.

The premier consideration for the building automation system is the construction cost, the question would be if it is feasible to establish it as it has higher construction cost. It has long term and life cycle return without minimum investment cost. It is best to have long term investments on systems such supervisory control system which can be navigated remotely with the controllers and automation severs. However the construction does have financial risk where the savings will offset the investment within a given period. The construction cost of supervisory control system with security function and fire alarm is higher. In this case, consultants and engineers are forced to work together to handle the system. Moreover different technologies are not capable to speak the same language which makes the user more complicated and expensive to develop the BAS.

While different manufactures are involved and working on different developments, that goal of integration could be out of reach. For example, if DTU decided to develop their building with more advanced technologies which cannot be provided by the current suppliers, DTU has to look for other supplies who can adapt the techniques to the existing system.

### *1.1.2 Energy efficient Building Automation System*

The efficient aspect of BAS is to give the user comfort and cost effectiveness on functional operation such maintenance and management control. The management includes cost allocation, trend logs and global strategies for the access of the controllers and intrusion alarms. This can be managed by verifying the buildings are occupied or not. The maintenance referred to monitoring or fault detection such as alarm safety is much more important. For example, in hotels the alarms are very important as they should be maintained and on wire at all times. These days the intelligent buildings are equipped with advanced infrastructure for data information and communication distribution to promote productivity. Like in an unwanted situation such as weather changes or damages the system can track itself for maintenance. The intelligent buildings are able to adapt to users' changes and achieve the optimization. As an example, the users such as hotel employees can set up the controllers or the sensors for their own purposes, after that they obtain live control of the temperatures or security, this information's can be controlled or maintained in usable manner.

### *1.1.3 Building services*

When we talk about building service that means the help for the user with comfort. In order to do this the system should provide an environment where user can feel comfort inside the building with lighting and adjustment in temperature. There are differences between industrial and residential buildings. For industrial buildings there are demands on machinery process which differs from home comfort. The functions that buildings can support are the safe environment and the necessary infrastructure including data/communication exchange. At present the intelligent buildings should be smart enough to transmit necessary information to the users. The real functionality depends on the design of the building and the technical structure. For using the heating and cooling system in economical way, the devices are eligible to control the environments without handing over the data to the users. Somehow human management is needed for any incidents. But thanks to Web based technology, control system is now mostly used for this kind of situation.

### *1.1.4 Networks on Building Automation*

The possibilities of designing the network are determined by various controllers and servers interconnected with even more devices. To communicate with a network distributed control application is needed for delivery of accurate values that can transfer data between controllers and sensors. Unfortunately control and monitoring system have limited control level from a central location. There are issues for the users when multiple manufactures are involved to develop different interoperability between sensors, controllers and actuators. For instance when we take a look at Schneider, they have designed controllers which cannot communicate with Honeywell automation server as they are developed in diverse ways. Moreover Honeywell motion sensors are not compatible with Schneider automation server as they have different protocol structures. Basically the server should have some extensions file format which then can be used to have communication between these devices. One advantage with the BA applications is that they do not generate high traffic load at the field level because of the absence of high speed control loops.

The safety and dependability of the network rely on the detection of equipment status and failure to meet constraints. Still some certain amount of false tolerance is required on the field and automation level. Single failing unit should not bring down the entire system as long as the layers are remaining operational. When we look at the BAS network it doesn't have any noise in the network and peer-to-peer are well suited to BAS. The industrial automation are mature in high-speed control loop and time-driven master–slave. The focus is to have graceful degradation of functionality as systems need every sensor to be operational to fulfill their purpose. The BA system in higher scale can be achieved if the network protocol supports the address space and the hierarchical subdivision. The network should ~~be~~ have more transparency in order to support wide area network with high volume installation of wider coverage while spanning the nodes.

### *1.1.5 Scalability on Buildings*

Regarding the scalability on building automation system first we should know the requirements for the types of buildings. In closer aspect there are varieties of buildings available such as agricultural, commercial, residential, educational, governmental, and industrial buildings. Moreover each type of buildings should apply with specific type of technology. There are several companies working on specific technologies to resolve the issues given by compatibilities of devices for users. In the following writing we are going to look at the scalability on different types of buildings and their corresponding technologies.

### *1.1.6 Scalability on smaller and larger buildings*

The word “scalability” represents the capability of a system or network to handle a growing amount of work or challenges. As we are living in advanced technology world, different types of needs and expectation on savings energy are required by people [3]. There are less investments on technologies for residential buildings compared to larger buildings. For example there are fewer requirements on installing devices such as sensors or CCTV cameras which are more expensive to invest on companies compared to private homes. There are options on such application, wired and wireless technologies. When we look at wireless technologies like ZigBee standard which gives cheaper way of communication compared to wired technology. At one point hard wired technologies doesn’t have that much expenses in the home environments. For standard house in Denmark it doesn’t exceed more than 200 $m^2$ in space that means there is less material cost. Let us focus on hard wired and wireless security system because most of the users are willing to upgrade their old buildings or systems with the current developments. To look at the facts about the system which communicates between the devices such as alarm or sensors, in the following table you are able to see how the technologies differ from each other.

| **Wireless system** |
| --- |
| **As we know wireless system are less expensive than the hardwire system, wireless system are presently well accepted. There is a significant advantage on using wireless system as they do not require cabling which avoids cutting in the wall to install components, therefore it is preferable for a private person who would like to install the system itself. The wireless system has some issues on security with the devices such as security siren which can be shut off without knowing from the users. When the alarm sensor is turned off the user doesn’t have any clue if the alarm is on or off. The worst case scenario might be hackers are able to hack into the wireless system without being known by the user. Another big issue is the energy efficient wireless devices are often equipped with batteries which have to be replaced when the batteries drain down.** |

| **Hard Wired system** |
| --- |
| **Hard wired system installed during construction or remodeling phases can help to reduce the cost. Hard wired systems are more expensive compared to wireless system when we add each individual system one by one. But the advantages are that once the system is placed you don’t have to replace it again, if the system goes wrong there is no need to replace entire structure only the specific component. Hard wired system has advantage on clear and strong data transfer between networks in signals and links.** |

The automation system is it nearly same as the security system environments. It has rather complex structure with the controllers and devices. Especially for larger buildings compared to smaller buildings. When we take a look at universities or office buildings as there are lots of people involved who need more equipment’s to handle the requirements [4]. There should be some better structured systems to maintain the complicated devices. University accommodates many students who are using the buildings, smarter BMS system is needed as in home environments. In the following chapter we are going to talk about more technical aspects of BMS in details.

### *1.1.7 Scalability on office buildings*

When we look at the scalability on office buildings' environment and technology, there are 3 different key aspects. These are HVAC, lighting and metering system ensuring optimal energy use and working environment for employees. As we know in an office building there is diversity of people working such as men and women. In women's perspective, they are less heat tolerant than men [5]. As a matter of fact that women have thinner skin and less fat compared to male. We should know all human body starting freezing first with legs and hands. Moreover women have less muscles (23%) compared to men (40%) but women do have the biggest muscles as well. Therefore the automation system should be designed to create comfort for everyone in the office. One way to do it is keeping temperature at constant level to provide hot and cool air which can be applied for both genders. The office environment is mostly designed with larger windows which favoring natural light. Open building layout concept is for festering collaboration with plenty of conference rooms and fewer offices. If we consider an office space of total 30 000 sq ft consisting with three HVAC zones, each served with root top unit or Remote Terminal Unit (RTU) of around 15 subzones with Variable volume (VAV) boxes. These could be controlled through NPN UN controllers communicate with wireless ZigBee devices over long distance by passing data via mesh network to all 15 subzones. Furthermore each subzone is equipped with SE8000 room controllers which are the most flexible and commercial controllers at the moment offering scalable solution on immediate energy savings. Also these controllers are reliable, cost-effective and easy to install and scalable for any sized buildings.

On the rooftop there are $CO_2$ sensors attached to the SE8000 controllers to watch $CO_2$ level from each sub zones to enable outdoor ventilation. From the lighting prospective NPN UN controllers are used to control the lighting schedules in the zones. It uses EnOcean technology sending wireless telegram to EnOcean lighting relays to open and close lights (For further details on EnOcean go to chapter 2). Through relays the users are able to save energy and make users more conformable by adopting the daylight harvesting environment which can be pre-scheduled. Also the users are able to access the EnOcean Switch which is a wireless energy harvesting device functioned with batteries to allow light levels in the offices with simple click by on/off the button. There are power metering components to measure main load, HVAC load and lighting load transfer information through ModBus RTU back to the NPN sensor unit. Through this process the data can be transferred to the main network to get actual energy consumption and use.

## *1.2 Motivation and reasons to have smart algorithms*

I have studied most of the building automation systems which are present at the moment. They all have the same motive to control and monitor the rooms or areas. When we look at DTU buildings they are mostly equipped with BMS which are smart but not smart enough. For instance when we take a look at each individual lecture rooms, they are equipped with different sensors which is able to detect people (students and teachers) in the classrooms with timely ventilation and lights. The closer aspect of the current system at the DTU shows that it is not smart enough to handle the situation. If someone enters the room the sensors are able to detect and turn on the light and to measure the temperature in the rooms then provide the heating or cooling in the rooms. But if someone leaves the room the lights and ventilation are still on which is a waste of energy. Also in the evening or on holiday time these devices are still in function which induces more waste of energy. Some of the rooms don't have temperature sensors which makes it difficult to handle the room climate. We have to take into the consideration that some of the network structures of DTU are still with LonWork technologies. The solution capable of adapting the old LonWork and the present BACnet networks is required.

In present days all the organizations are interested in data collection on energy consumption from each individual sensors or controllers. At DTU library most of the students are using the places for study purpose. The HVAC systems at this place are continuously in use or in function compared to other areas at the DTU. If there are any systems able to use or capture these data from each individual sensor or lights devices, it can help the researches to improve the system in the future. DTU BMS are lacking on functionality which cannot save energy with positive effectiveness while no activities in the library the systems are still in function. Even it is in the lecture or study rooms the same system resulted the same effect. For resolving this issue, there should be some updated algorithms placed that are able to avoid these mistakes and turn DTU into an energy efficient university.

Through my research I found out that DTU has issues on device compatibilities and network structure for the old and new buildings. These problems rely on different organizations such as Schneider Electric, Logmatic, Loytec and Honeywell who are supplying devices and controllers with software options. Because these firms have differences on protocols and Integrated Development Environment (IDE) for software application. As DTU is one of the Europe's leading engineering institutions are focusing to make our life to be green in the future. All departments at DTU have thousands of devices running which should be able to be controlled in energy consumption. For example when we take a look at DTU Wind Energy department who are focusing on wind energy using many machines and equipments which consume high capacity of energy which is not be known from the own department. The controlling devices should be placed in order to monitor the department's areas of offices and lab rooms. Through these monitoring they are able to save time and energy in a good manner.

There is a pilot project going on with DTU Smart Campus where they would like to create indoor living lab with several technologies. The principle is collecting data from the individual sensor to carry out qualitative studies for the users (students). All the old lamps in the library will be replaced with new energy efficient LED lights. Various sensors like infrared sensors are also added to collect data about the number of people who are engaged in the area and registering their movements. The actual idea is to collect data from these sensors and pass it to developers who can use it for future developments. Based on these concepts I would like to look at various present technologies and find one appropriate solution for them to measure the devices. As I am involved in this pilot project which motivates me to find smart solution which can be used for DTU.

# 2 State of the Art

In this chapter we are going to take look at different kinds of technologies which are used in the Building automation system. There are different types of protocols available to have an appropriate communication between buildings and devices. These research based architecture should give understanding on how building automation works and what techniques and devices are used to function the BMS system. Moreover these research based writings should help me for further developments on design smart algorithm. In the previous chapter we could read about why we need the BAS but we don't know how we could use it in practical aspect. That means we should know about the available software tools which could applied for the needs. More precise we know why we need the BAS but don't have any software and hardware based knowledge. In this manner the following writings should give us more details descriptions on technologies based understanding.

## *2.1 BACnet Building Automation*

Building Automation and Control Network (BACnet) it is a non-proprietary open protocol communication standard which is created by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRE). The intention for this standard is to have interpretabilities from different kind of vendor's technology such as integrated equipment to the coherent automation. That means different kind of devices can be used in the automation system which will help the user on saving money and energy on devices. In this manner there are big debate going on the protocol elements such as responsibilities and privilege on all network devices. Each network devices are modeled as a collection of "object" and categorized by properties or attributes [6]. That means the standards are mostly extensively applicable object type where user are free to create additional object. Also BACnet can be used from different manufacturers to interoperate with the buildings. In the following writing you are able to know about the data communication protocol for control networks and building automation more in details.

When we look at BA it is a Computer based intelligent buildings which control system products that are frequently made by different manufactures. As the devices are from different manufacture do have issues on information exchange which may critical for building automation. Lots of developers working on the communication part as they are speaking different languages. The BACnet protocols provide a model on building automation system for communication between systems and devices. These specify on flexible and scalable network and internetwork design. The control and data function are structured as object oriented manner. In the following writing you are able to read more about the objects and properties on BACnet.

## *2.2 BACnet objects and properties*

Oriented object of BACnet are used to organizing and accessing information on method for modifying, controlling and examining different types of information in different devices. Every standard objects types are used mostly in many automation system. When we look at Bacnet object closer it is a property collection which representing parameter information. More precise BACnet objects are collection of information within a device. The Bacnet object defines what type behavior and objects are expected from each property. BACnet dose have 18 different types of stand Objects such (Analog input: Sensor input, Binary input: Switch input, Binary output: Real output). Each buildings control system has different

types of objects, such alarm notification, sensors analog input or scheduling [7]. The uses of the object are is to define the devices in to the network. BACnet standard does have 123 different types of Properties objects which are specified for each type of Objects and tree of the object must be present in every object these are object value, type and name.

## *2.3 Network layer on different protocols*

BACnet protocol has different options to provide design flexibility, performance and cost for networking technology. The advantage is particular networking technology can be used in a system or multiple option which share BACnet internetwork. When we look at the network layer protocol it is depends on the message which can be routed from the BACnet network to another BACnet data link technology. When it is comes to functions assigned to the network layer in the OSI model the BACnet doesn't require all of them. For example the device source and destination path can be for one active path on the devices. The BACnet do allow only one most active path eligible between two devices. Moreover there are some limitations on the length of the message which get ahead of a router. The message maximum length shouldn't be exceeded from the source to destination. But there are some exceptions where the messages are longer than expected such they should be segmented and reassembled at the application layer beforehand. When we look at the BACnet network layer portion message has one octet version number and control octet. In order to Control octet it indicates the absence or the presence of the network layer information. But there is one advantage if the device has destination for the message on the same network, no need for any additional network layer information. If the destination is on the remote network there needs to be a client device which should include the MAC address and the destination network number of the device [8]. When we look at the router on the same local network include the addressing information about the local network which helps to return the response. In order to router configuration, the router will look at the network layer protocol service from BACnet and search for the path on the destination network and manage to get temporary connection with the dial up telephone connection. BACnet do have ways where the message can be routed through presented IPX and IP works. These protocols are able to encapsulating and decapitating the message through techniques like tunneling.

BACnet is an open data communication protocol and design to handle Building automation systems. It is design to be cheap and effective on connecting from small buildings to large buildings. The communication LAN is the various interconnections which connects components of a BAS from the maintenance point to controllers. Let us look at the BACnet standard for LANs in details such as (Ethernet, Arcnet, Ms/TP, LonTalk).

MS/TP: Stand for Maser-Slave and Token Passing is used in BACnet devices where manufactures are able to build them in building automation systems and in Industrial automation system. As this network has token passing method it can only communicate if it has the token. Master devices are able to start request but they have to agree for a time slot to make the request.  In this case it can take some memory and processing requirement to the Master device. The slave devices it is mostly design for the low cost implementation but there needed some lack on capability to initiate request such as message can be replied from other devices. The MS/TP Local Area Network is able to help the BSM manufacture to build BACnet devices with low cost. Also it connects supervisory controllers system such as SCADA and field controllers to field point interface. The network controller requirements maximum of 60 nodes per MS/TP network and if the devices are more than 600 meter long in distance need a repeater for strength the signals.

LonTalk:  It is developed as a proprietary Local Area Network and released as an open protocol. LonWorks as the potential needs for the LonTalk and it provides the terms “foreign frame transmission”. In this manner the BACnet standards use the standard for the LonTalk for transporting its “foreign” frames. Also it is a simple mailing system which provided basic mechanisms for transporting message between networks systems. LonTalk use Standard network variables types (SNVT) which is a method to approach to defining data object where sender and receiver uses. Code number identifies these SNVT where the receiving controllers can use for how to interpret the information in each SNVT. LonTalk are developed by Echelon group and implemented in a Neuron 32 bit chip. One issue with LonTalk is less products use the protocol media to transfer BACnet message.

ARCNET: Is a low cost LAN token bus standards which need dedicated communication such as inter grated circuit (IC) which makes it more expensive then BACnet LAN. The more details description specifies it is a communication protocol for local area network and first obtainable networking system for the microcomputer. They are able to run from 150 kbit/s to up to 7.5 Mbit/s and as they are low in speed cant competed with the high speed Ethernet and IP.

MODBUS: It is an application layer protocol messaging for client/server (master/slave) communication. When we look at the messaging process in the MODEBUS network with two different controllers only one controller can be master and the other device will be slave to request data. Moreover it has an easy communication option between different network architecture. There are two different frame types in MODEBUS, which are Protocol Data Unit (PDU) and Application Data Unit (ADU) used to exchange messages between server and client. The PDU frames do have the code for the functions with data to perform action. The ADU frame is bit more complicated and provide error checking. Most of the devices such as Programming Logic Control (PLC), I/O Devices or Human Management Interface (HMI) mostly using the MODBUS protocols for communications. When we look at application data unit part it is managed by client, which imitates the MODEBUS transition.

Ethernet: Is most used and high-speed LAN for many years and the proven worldwide standard. During the following ears it was dropping by its interface but still higher than other BACnet LANs. Moreover it has more varieties of cabling options such as coaxial and fiber or twisted pair cabling and runs from 10 Mbits/s to 10 Gbit/s. The functionality of the Ethernet is to provide standard hardware based on standard switches using standard management tools. From the following Picture 2.1 you are able to see table with BACnet LAN which represents the standard, Data Rate, Packet size and cost for different protocols.

| *BACnet LAN* | *Standard* | *Data Rate* | *Packet size* | *Cost* |
|---|---|---|---|---|
| *LonTalk* | ***n/a*** | ***4.8 to 1250 kbps*** | ***228*** | ***Varied*** |
| *ARCNET* | ***ATA/ASHRAE*** | ***0.15 to 10 Mbps*** | ***501*** | ***Medium*** |
| *MS/TP* | ***ANSI/ASHRAE*** | ***9.6 to 78.4 kbps*** | ***501*** | ***Low*** |
| *Ethernet* | ***ISO/IEC 8802-3*** | ***10 to 100 Mbps*** | ***1515 bytes*** | ***High*** |

**Picture 2.1 Table for BACnet standards**

## *2.4 Standard terms for international Protocols*

Data communication service and protocol for the standard are defied to control and monitor for HVAC buildings. To define object oriented of information communication between equipment and use of applications of digital control technologies in buildings. The protocols do have set of messages for covering encoded analog, binary and alphanumeric between devices. There are no limitations between some hardware binary/analog and output values or text string value [9]. Moreover the standards are defined by draft or international standards for open system interconnection (OSI). The application process is a real open system with element to perform the information processing for specific application. Application refers for users information processing requirements or the service access point provides by an (N) entity to an (N+1).
Now let us look at terms on these standards which have 3 different ways as (right, control, and user). The rights based on the permission of the credential and the control pointing on the network research method for restrictions. The users do have physical access control on the privileges. Alarms are included to the term as well as visual and audible from an operator to an off normal condition which requires action. In order to the acknowledgement of the alarm indicate to human interaction is response for the events notification.

## 2.5 Abbreviation and Acronyms use in this standard

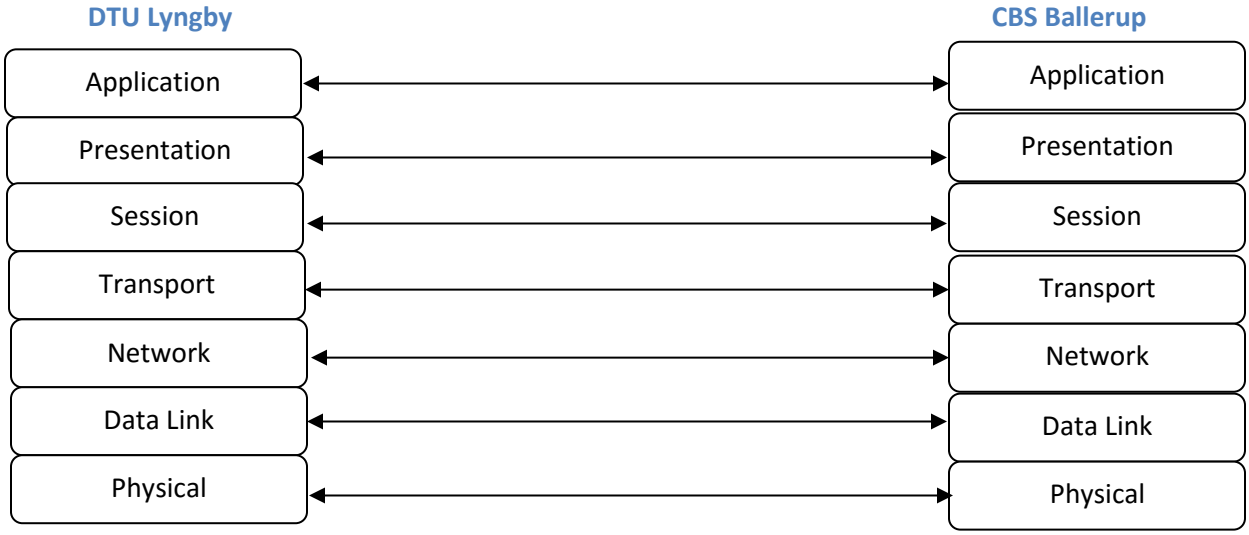
| Abbreviation | Acronyms |
|---|---|
| *ANSI* | *American National Standard Institution* |
| *ARCNET* | *Attached resource computer network* |
| *BAC* | *Building automation and control* |
| *BBMD* | *BACnet/IP broadcast management device* |
| *BDT* | *Broadcast distributed table* |
| *B/IP* | *BACnet/IP* |
| *B/IP-M* | *BACnet/IP multicast* |
| *BVLC* | *BACnet virtual link control* |
| *BVLCI* | *BACnet virtual link control information* |
| *DID* | *ARCNET destination MAC layer address* |
| *IP* | *Internet Protocol – RFC 791* |
| *MAC* | *Medium access control* |
| *MS/TP* | *Master-slave/token-passing* |
| *N* | *Network layer (prefix)* |
| *OSI* | *Open system interconnection* |
| *R* | *The property should be supported and readable using BACnet services* |
| *PTP* | *Point to point* |

**Picture 2.3 Standard table**

## 2.6 Protocol architecture of BACnet and OSI model

Let us look at the architecture of the OSI basic reference model which is an international standard used in model for developing multi vendor's computer communication protocols. More precisely the OSI models are separated in to computer to computer communication and these are broken in to seven different manageable models each with communication function [10]. As can be seen from the Picture 2.4 there are seven different layers arranged in hierarchical manner for providing services. Let use start with physical medium as they are responsible for the connection between two machines. The Physical

layer is selected for several reasons like availability, speed and the chip which supports the protocol depends on the BAS industry. For further details on the network structure see chapter 4 on BACnet network. Application process connects to the OSI application layer and interconnects with second Remote application process. Interconnection takes place between two processes as they are interconnected directly with application interface. Moreover, each lower layer of the protocol provides communication services and virtual peer-to peer transportations with its companion layers on the other side. The purpose of the OSI model address is to communicate computer to computer all around the world in and design to handle complex system. The reference models layers are categorized in different ways: Upper layer Data – (Application, Presentation and Session), Segment – (Transport), Packet – (Network), Frame – (Data Link), Bits – (Physical).




Picture 2.4 Layer architecture of BACnet

Now let us look at the communication level between two different arias (DTU lyngby and DTU ballerup). When we look at the application level between two areas, is there to handle the application program interface between the users. That means it provides commands for accessing and manipulation information between users. There are 35 different application services existing and these can be grouped into six different categories:

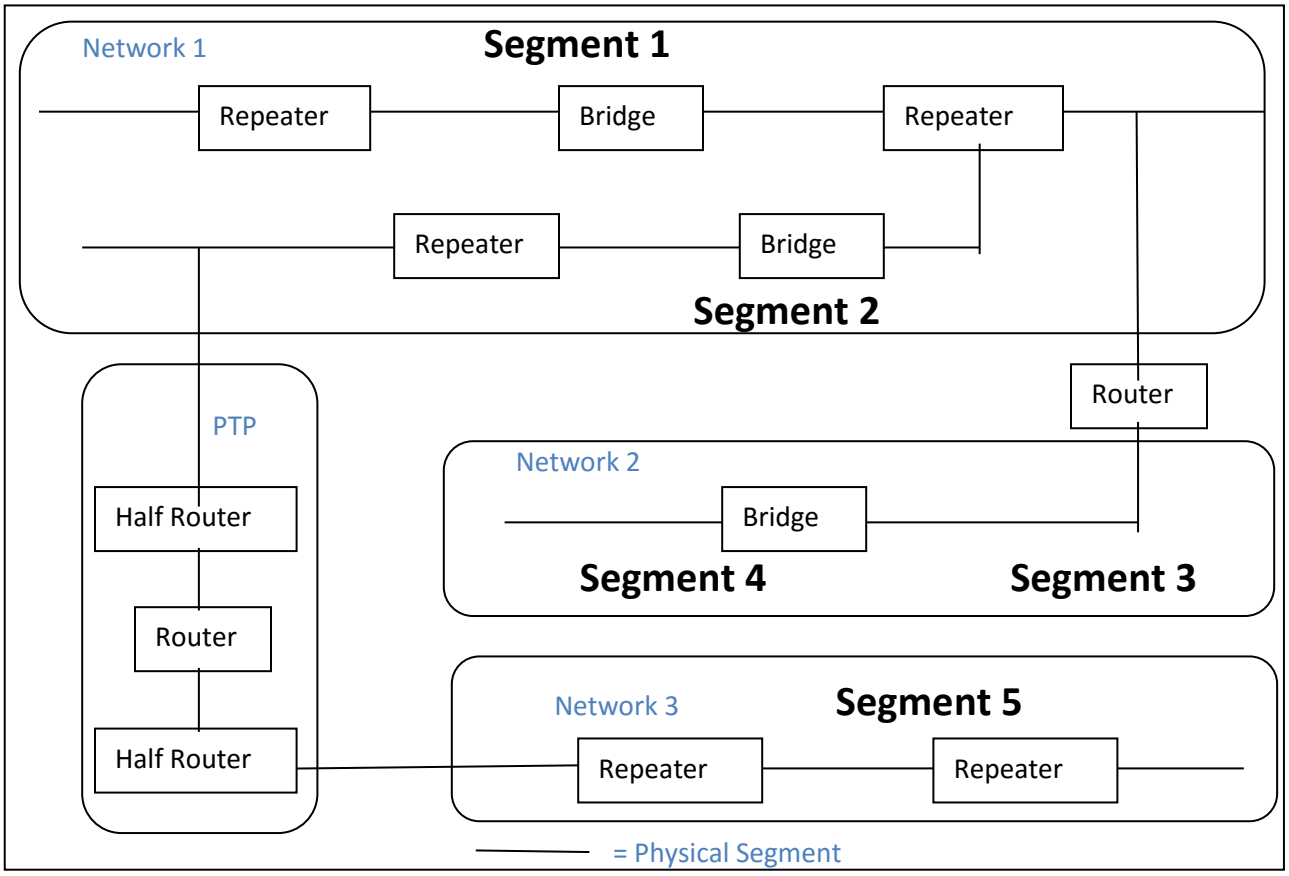
*Alarms and Event Services* – (AcknowledgeAlarm, SubscribCOV, GetAlarmSummary).
*Remote Device Management Service* – (Who-Has, Who – Is, I – am, ConfirmedPrivateTransfer).
*Security Services* – (Authenticate and Request key).
*Virtual Terminal Services* – (VT-Open, Data and Close).
*File Access Services* – (AtomicWriteFile and AtomicReadFile).
*Object Access Services* – (CrateObject, DeleteObject, WriteProperty, ReadProperty).

The presentations are there to converts and recognize data and encrypt/decrypts applications. When we look at the application entry aspect is made with two pats (BACnet application service and user elements). The BACnet user elements have the ability to mapping the devices activities into BACnet object and exchange information between two peer application processes. The BACnet user element it is a set of application or function which support the local Application Program Interface (API). Application Service Element (ASE) task specifies the service procedure portion of each application services and

maintaining generate invokes IDs to application service request. When we look at the session they are based on host layer to manage data transfer with checkpoints etc. In order to Transport layer is responsible for end to end data segments as error checking. Competed to network layer is there to gain routing between machines and establish connection to the logical circuit. The Data Link layer is there to manage access to the physical medium. At Last is the physical layer which works on the physical medium to transmit and revises bits. Moreover the OSI model is used for building automation application as they are giving better connection to the controllers and sensors.

### *2.7 BACnet Network Topology in physical segment*

As can be seen from the Picture 2.2 there are BACnet internetwork illustrated with Repeaters, Physical Segments, Bridges, Half routes and networks. There are BACnet based LAN topology all the devises are placed with physical segment and electrical medium. BACnet based physical segments are attached to physical layer with repeaters to extent the signals strength [11]. More over BACnet segments are interconnected by bridge devices which connects the segments at the data link and physical layers. The bridges are there to connect different segments to be interconnected between the physical segments and link layers. The link layer is there to link different networks together and used for filtering MAC addresses. In chapter 4 there are more detailed description on half routers and network developments.




Picture 2.2 Segmentation on network architecture

## *2.8 Smart Grid*

When we look at the Smart Grid (SG) it is an Electricity delivery system which is capable of distribute and transport power or energy from A to B in the sense from manufacturer to consumer. The main purpose is to develop and manage to balance power consumption. The Demand response (DR) system is there to manage the reduction of the power and the way how to change the electricity consumption patterns. These patterns are used to lower the risk of potential disturbances and the more additional capital cost for the plants. As we talk about cost based on the buildings and industry will have the most consumption. That means in the feature there will be more electricity need compared to present stage. There should be some development and solution required to manages the energy consumption. The researchers believes through the well-designed DR system might have better power use. There are lot of DR algorithms available depends on the user needs and the requirements.

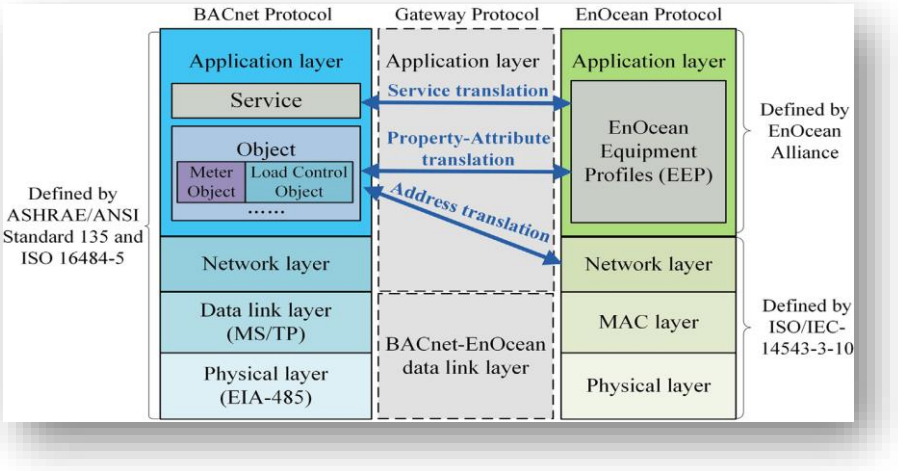
The algorithms should provide and better way of using the devices such as how the power should be used or the activity time such as using fully automated equipment's in reasonable manner. There are some studies going on how to design DR system in the buildings. There was one project based on DR system in Olympic Peninsula suggested to use existing BACnet based building automation system. This cased to not successful suggestion as this was based on complex installation and expensive cabling. This is a big issue as there are different manufactures are working on developing different technologies as they are speaking different languages [12]. I order to installation different cabling there are better way to place with wireless devices as they are less cost efficient and time savings.

These wireless system ideas came to create ZigBee DR system and the Honda et al suggest ZigBee wireless sensors network in to KNIVES, a wired system that allows for demand control. But this system fails as they are not be able to measure they supposed to do. That means it is only able to monitor the component tempter based on the KNIVES system. The kuzlu at al decided to go on with the ZigBee based wireless system to implement in larger arias such as 100,000 ft. but this case them more difficulties in distance as time delay on WAN based system. That means these systems are not eligible to get wider range distance and these case to implement repeater to repeat the signal strength.

In 2013 Hong et al decided to decides to get BACnet- ZigBee DR system which can be used in buildings. These ideas didn't succeed as the ZigBee based devices needed batteries and should be maintains and replaces. For this reason EnOcean was developed to be the first international wireless standard for the energy-harvesting WSNs in buildings. When we look at the EnOcean technology do have benefits such as design for buildings automation system and use the wireless short- packet protocol which use low power consumption and at last able to produce energy from its environment which save the maintenance cost. In this manner the EnOcean might be better choice for the DR application in automation buildings. Also there are some larger buildings such as big organizations which require EnOcean require large bandwidth backbone. In order to bandwidth backbone issue there need to be BACnet as a backbone which holds international building standard and specifications for DR applications.

## 2.9 Architecture of EnOcean-BACnet Building Smart Grid Gateway

In this chapter let looks at the BACnet-EnOcean Building Smart Grid Gateway (BE-GW) development which are based on the OSI model. As can be seen from the Picture 2.5 it is a Protocol architecture of the BE and GW. There are three different protocols (BACnet, Gateway, EnOcean) and when we look at the Gateway protocol application layer it does include the fundamental application function of the gateway and the translation process [13]. The translation process is collected of three types of procedure one the property attributes translation from BACnet objects and EnOcean EEP and in each ways. Second the address translation map between the BACnet and EnOcean and the last is the service translation. The actual idea of the serial communication interface consisted with linked layer where BACnet and EnOcean use to exchange data.




Picture 2.5 Protocol architecture of the BE and GW gateways

## 2.10 EnOcean wireless system for sustainable buildings

Buildings almost use our 40% of total energy requirements. In this manner the EnOcean technology use the unique way to save energy and reducing operating cost. EnOcean is the unique key to intelligent Green Buildings in a way to overcome the wiring and no limits. Wireless sensors (Switch, Room Temperatures Sensors) are connected via wirelessly to the Actuator/Gateway through LON,KNX,BACnet,TCP/TP protocals. EnOcean intelligent self-powered wireless switches and sensors are powered by energy drown from movements light or even changes in Temperature. This harvested energy is used to transmitting censored data in a building to control lighting, heating or air-conditioning whiteout any cabling. Adding energy system in offices, schools, industrial buildings or airports etc has become strayed forward. EnOcean has some solution for energy savings in a way to place the wireless sensors and controllers to get energy efficient functions.

## 2.11 IPv4 vs IPv6

Before looking at these IPv4 and IPv6 we have to know what an IP address is and why they are used for. IP is an Internet Protocol has set of rules governing the format of data sent over the Internet and other network. IP address is a numeric label assigned to devices in networks enables communication [14]. Every IP address is unique much like our fingerprints every person has unique fingerprints even twins. Is same as Just how the fingerprints identify people the IP address also used to identify devices in a network.

IPv4 is the forth revision of the Internet protocol and at the present is the most commonly used method. It uses the 32 bit address for a total on 4 billion possible addresses. The 32 bit addresses looks like (IPv4 address 192.168.1.1) every segment is 1 byte of information such 192 is 1 byte and 168 is another byte so there are altogether 4 bytes (4x8) in IPv4 address. Every byte in IPv4 can have the value from 0 to 255 and every byte in IP address can be expressed in binary. There are two possible values in binary which are 1s and 0s and there are 32 bit address scheme total of 4 billion possibilities on unique address. As we are running out of address we consider to having IPv6 which is able to fulfill the feature requiems. Most of the people don't need the IPv6 as they are satisfied with the current IPv4. When we look at the BMS system in DTU, doesn't need IPV6 as they are only using automation system in the Campus. They have enough of IP address left over for more devices to be added or connected to the network.

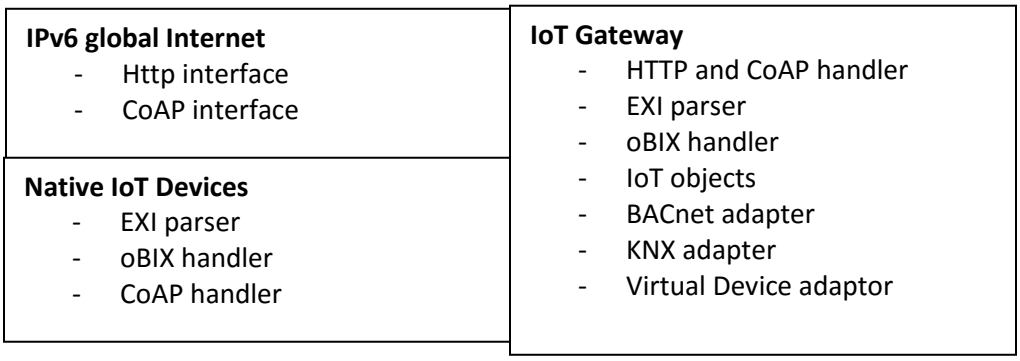
IPv6 will replace the IPv4 address from 32 bit to 128 bit which has more capabilities on control and convenient on devices and network communication. Also there are more benefits on IPv6:

- Quality of service (QoS).
- Extension flexibilities.
- Do have efficient routing.
- Improved multicasting routing and simple header format.
- No need on Dynamic Host Configuration Protocol (DHCP) administration.
- Avoidance on Network Address Translation (NAT).

## 2.12 IPv6 multi-protocol gateway

The main idea to develop IPv6 is to enable machine to machine interaction without domains and deploy IP directly on the devices. In this manner there are different types of research going on to get better and easy of interaction. That means (OASIS open Building Information exchange Technical Committee) to define Web services and Extensible Markup Language (XML) mechanisms for BAS control systems. The actual idea is to manage web service communication between building electrical systems such as controllers and sensors. Also the Open Building Information Xchange (oBIX) public web services technology gives the possibilities to get data communication between enterprise application and facility systems. As we talk about web service it has a big role for constrained node and network in the IoT which is the constrained application protocol (CoAP). This technology is useful for the future increasing devices and last for decades. This idea will be one of the solutions for the different type of people who are dealing with the BMS system [15]. There are possibilities where two legacies devise communicate each other with IoT API. In the following picture you are able to see IPv6 multi-protocol gateway for the (Smartphone apps, web portals or enterprise information systems). There are adapters such KNX, BACnet which are the key component of the gateway architecture. This provided interface to the BAS application protocol layer. As can be seen in IoT gateway the oBIX headers are responsible for the read,

invoke and write request to open Building Information Exchange (oBIX) objects to interact with the objects. Moreover the oBIX handler publishes the devices to be known or mapped from the CoAP. That means the oBIX hander publish the devices which are using HTTP and CoAP hander to the IPv6 address through this purposes there are possibilities per device and centralized access in parallel.



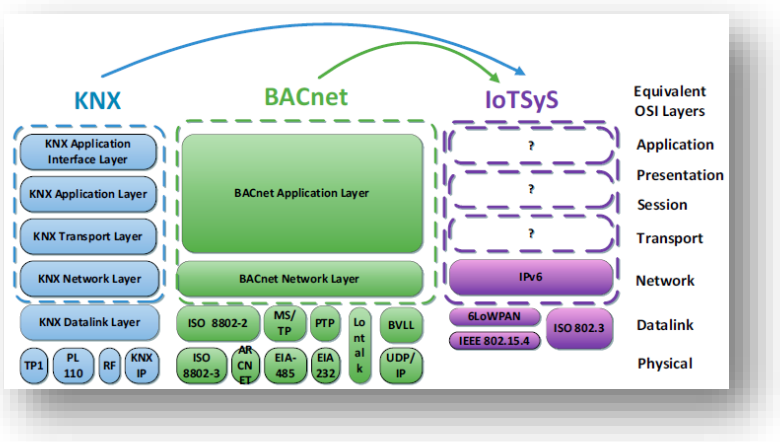

The Internet of Thing (IoT) is a technology which enables and connects billions of devices each other on different supply chain, building automation, homes etc. Also the current companies interconnection focusing on developing smart grid and smart metering infrastructure. The feature development does have the Web based communication option such as HyperText Markup Language (HTML) and XML. This gives the end user much more control and efficiency management on technologies, which mean there are less investment and maintenance required. In this method the integration of enterprise IT system over SOAP based are better suited. The interconnection of the building services do have different type of technologies and standards present like LonWarks, EnOcean, ZigBee and BACnet focusing on very specific building services and building automation. These might case to replacement with the new system based on an IoT protocol stack with IPv6 at network layer. The current building automation technologies such as BACnet/WS and OPC UA do have the BMS technologies to web based protocols that means the user are able to access the software remotely and do have all the required access and features.

There are lots of researches going on developing IoT as they should be able to handle billions of devices or objects through the internet. There is a basic model with 3 different layers consisting with Application, network and Perception layers. When we look at the application layer it is there to provide the service for the user request. In deeper understanding the application layer provides data (air humidity, sensor measurement) for the user [16]. That means the IoT is able to deliver high quality of data to the user and do have possibilities on billions of devices. Not only to deliver data for the user also connection between the layers on smart homes, transportation and industrial automation. The service management layer is there to manage the paring a services on names and address. That means the layer should be able to enable the IoT application to work with object without any hardware platforms consideration. The object layer is the first layer which focuses on devices to process and collect information.

This layer has the controllers or actuators to have functionalities such measure humidity, vibration or temperature. For brain of IoT there are different microcontrollers or microprocessor Software's available which can be programmed on hardware such Arduino or RasberryPi. Some Gateway controllers are available to have less expensive alternatives which can collect data from the placed sensors or controllers. The Elitegroup Computer System GWS/QX it is an intelligent host which is used in the smart energy framework to control remotely the devices in meeting rooms or lecture rooms. That means the users are able to remotely pre-configure the rooms like if the user arrives in to the room the lights, heating or projectors should work on its own. Also there are one Real time location system (RTLS) solutions tracks peoples, objects and workflows to help the user to make better decisions for the user. An active RFID tags can be placed on all the controllers in the BMS through 802.11 wi-fi networks provide advanced location analytics and cost effectively deliver Room-level real time location accuracy.

## *2.14 Integration on protocol alternatives on Internet of Things*

For the building automation system there are different ways and possibilities with the OSI reference model. The application layer has the express on input and output data points and as function blocks to define the behavior. The network and data link layer in the building automation system define the interaction style such as server/client or Manufacture/consumer communication. The main point of the technology is to keep simple as possible such as the point to point or multicast communication supported. The gateway has possibilities on N-to-N protocol mapping but for the IoT system there should be N-to-1 approach. Neither means nor 1 stands for the new IoT protocol stack which have the communication interaction between devices in the LoT. Communication between two BAS referrer on N-to-N interaction are based on the gateway featuring and the network options. In this manner the N-to-1 integration refer for two way communication between two BAS system and do have the compatibility through gateway featuring option. The implantation of the N-to-1 can be seen from the Picture 2.6 there are mapping from KNX and BACnet to IoTsys [17]. In this mapping between the two BAS to the IoTsys the IPv6 involved as a comment IoT network layer. But the upper layers as Application to transport are question how it can be implement. There are some alternatives for IPv6 on the transport layer is the TCP and UDP. As UDP have the best communication option compared to TCP. There are some issues on TCP such low/power and lossy wireless networks that means it does not fit well as transport layer. For that purpose UDP is the suitable transport layer for IPv6 communication stack as it is able to support several protocols (Constrained Application Protocol (CAP), real time Protocol (RTP), simple network management protocols (SNMP) and NanoWS. Compared to TCP it has only session initiation protocol (SIP), HTTP and file transport protocol (FTP). The solution will be rather to use protocol such as BACnet and KNX on building automation is better to combine oBIX together with UDPIP binding. The oBIX are used as application layer protocol for the design of the IoT6 stack and providing protocol binding to UDP/IP.




Picture 2.6 Mapping BCAnet and KNX in to IoTSyS

BACnet and KNX web service can be used to integrate to IoTsys and it depends on which point the integration happen. That means there is two possibilities such providing the device with Web services interface or provide with centralized interface types. When we look at the centralized server do have the possibility on providing computational resource for a Web service interface for each individual device. A decentralized method has more computational possessions on field devices such as actuators and sensors. Interaction might be a centralized server on the IP backbone of the BAS which allows the interaction into remote access. Another interaction will be IP field devices which data link and network layer protocol can be prepared with Web services.

As we talk about small devices such sensor or switches can be handled with the Constrained Application Protocol (CoAP). That means CoAP is a software protocol which is used in electronic devices that works on protocol stack based on IPV6 and UDP. In this manner it interacts with the devices (sensors, switches). All the current buildings are based on the Ipv4 with has an address space of 32 Bit capable of handle small buildings. That means Ipv4 is capable of providing limited unique address for the devices in the buildings. For the IoT technology Ipv6 is suitable as it has 132 Bit address space which is able to handle billion of devices.

## *2.15 Intelligent buildings with smart system*

As we are living in fast growing world there are needs on intelligent and sustainable building. The buildings are around 40 % of global annual energy consumption. Is not only on energy including water and waste we are using every day. The “intelligent building” impressions has been for numbers of years and focused on developing different type of technologies, which can help us to reduce energy bills. But there are still some issues occurring in the intelligent buildings such as compatibilities issues with devices in the buildings.

The communication requirement on HVAC system specify on control in the mechanical way but lack on intelligent. That means the current HVAC system is able to control each individual controllers and sensors but not be able to maintain it in efficient manner. Also these depends on the user how they are going to use and manage the devices. Such as school they are looking for systems which are smart and fast enough to adopt the use on their environments. The School might look for Access control system which will focus on HVAC, alarm and lightings where the users are able to manage and control it. In order

to access system will allow students to get information where they have permission to control with number of independent systems. There are different types of supervisory control system available such as SCADA or Strucxware let the user to manage and control each individual devices.

The idea behind the system is to manage the room in efficient way such when the room is not occupied the lights and ventilation should be shut down or be in standby mode. Through this function the user are able to save money and energy and do not harm the environment. These include for the universities and offices where lot of peoples are in. Furthermore alarm system play big role such an unauthorized person enter the control zone which do remote magnetic log to prevent against serious damage. In the feature the system shout be able to control all the required control at one point where human interaction not required.

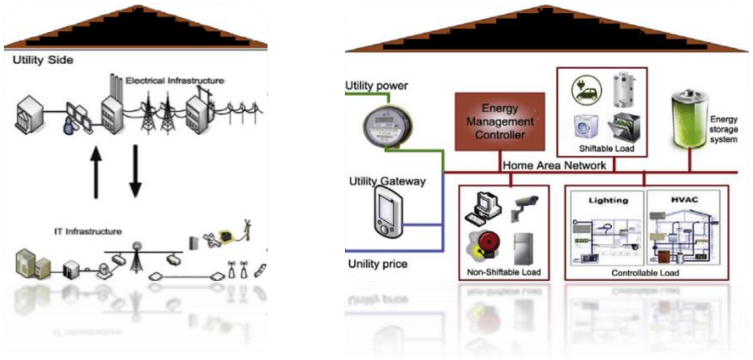
## *2.16 Algorithm on price based smart grid*

In this chapter we are going to talk about the algorithm which is able to cut peak use and renewable energy source. When we look the smart grid scenarios is the most usable and increasing widespread technique. This system focuses on the home to grid demand response algorithm present as pointer for domestic electricity tariff and modern smart grid.
The smart grid is current technology used for the transmission, power system technology and uniting power-generation. In this manner smart grid using advanced sensing and control communication technologies to improve the use of the energy and the consumptions in the feature world. When we look at the smart grid key feature is based on DR (demand response) algorithm [18]. The DR algorithm feature is able to consummate the electricity in a smart way and controlling the power usage in the peak periods. That means it is able to control and manage the power on price usage during the peak time. Most of the electricity consumptions are based on the Weather extremes of heat and cold demand for electricity growths. Special in Demark we have to face lot of heating expenses compared to Mideast countries. That means we have more than 6 month colder wheatear condition as hot weather in a year. In this manner we have the opportunity to get place the algorithm to the generator which can be mange to work only for sensible days such when the weather getting more warmer the grantors should go down to energy saving mode. This should be very used full for the public places such as conference buildings or offices. Which means when the building or premises are empty the power generator should be in save mode.

DR algorithm is the most usable system which can be used in the residential areas such as use of dryers or dishwashers which can be setup for off peak and peak time to save energy. By saving energy on each individual residential devices dose have effect on the world in positive manner. When we look at the home-to-grid system do have the capability to provide the user with more information to allow them to control the system operation.  In the following Picture 2.7 you are able to see two different figures which represent the home to grid demand response model. Compared to early life we are much loaded with technologies such as mobile phones, User interfaces and electric car which are heavy loaded in energy consume in the home. However this should be managed through the addition savings mechanism where it can be reduced. When we take the HVAC system in the house it can be managed to work automatically. Through this progress the user are able to save energy and utilize the peak and off peak time.

There are possibilities where user are able to use the high-end devices such as (utility gate way, smart meter, web based control) to control and limit budget of energy consume. Example when we take the utility gateway devices which receive price ranges from the utility company sends the data electronically to the house in real time and these can be handled from the in house utility device. These devices can use the DR algorithm to handle the prices where the users have benefit out of it. The combination progress the data are sending through telecommunication infrastructure to the utility gateway which provides and infrastructure between the company and user.

The gateway devices as been shown in the figure 2.7 could be integrated with other controllers or gateway devices depend on the home technical structure. In this manner the devices should be able to manage the energy use in the house. Also there is some residential load appliance such as non-shift able load which looks at the uninterruptible power supply such as television or refrigerators. These should be on all the time as they are in continues use. When we look at the controllable load appliances such as HVAC system can be applied with algorithms which are capable to work on their own and make usable energy savings. When we look at the shift load it is there to shift off peak and peak times to save energy. Example plug-in hybrid electric cars or washing machine can be used on off peak time. There are some similar systems existing already in the flats like people who are living in collegiums. They could save energy on laundry machines such to setup times when it should be function or not. That means the laundry machines are usable from 7am to 9pm but after 9 pm the machines will be shut down until tomorrow which rest for 10 hrs.




Picture 2.7 Smart grid demand response model

# 3 Design of smart algorithms

In this chapter you are able to read about different type of technologies which could be adopted in the BMS system. Also there are some smarter solutions available which are applied to the Building automation. As described in the previous chapter about the smart grid demand response model is still under construction and needs some further developments to full fill the user's needs. From the following writing you are able to see Designs, which focuses on the operation software for building automation and how to understand different types of software functions. There are different devices available such as controller and sensors which have appropriate tasks and provided functions. That means these devices are able to provide smarter solutions for the end user in buildings. The first part will explain how these software and hardware functions, and the second part will provide actual solutions for smarter use in the Function block diagram (FBD)HVAC systems in DTU buildings. There are three different algorithms available one is focusing on to work with the HVAC systems one for the weather system and the last

algorithm specify to control under floor heating system. Before to read the following chapter we should consider why we need the algorithm? From chapter 2 we could read about different protocols and algorithms which give us more details understanding about the availabilities on system which presents at the moments like the algorithm on price based smart grid. These price based algorithm can be used in different ways to the BAS where it could have a smarter way of energy use. Also the integration with different protocols dose has effect on the smart algorithm, such how it can be applied to the buildings. The actual idea is to build smart FB algorithms for HVAC system, which should help the DTU campus net CTS Engineers. That means these algorithms should provide the CTS Engineers with easy of use, fast action and savings on energy. There are different types of software systems available which dose has similar function to the system, which I have been providing. The provided system are much smarter and does have features which can adapted DTU buildings. In the following writing you are able to read more about the software system more in details.

## *3.1 StruxuWare software solution*

The StruxuWare software has a useful interface which delivers information when and where the user such (DTU campus CTS engineers) wants it. There are day to day operations with drag/drop schedules and trending, with easy access to the work. Open protocols gives the user freedom to choose the right equipment for the application. In this manner, there are more options with which to choose a wide variety of devices, which makes the user more comfortable and has greater ease of use. Moreover there are options on day to day handling of alarms, schedules and reporting etc.

That means the user has 24/7 live information on their active devices. When we look at the application point, there are controls on HVAC and Lighting systems and integration platforms for design. On the solutions side of SmartStruxure, there are options on Engineering, Software, Hardware, services and installation to make buildings smarter, more sustainable and efficient. When we look at the software operation perspective, it has integrated management, monitoring, and control of Fire Safety, HVAC, Lighting and Energy systems. It is a powerful application which is easy to handle. Also it is able to reduce the energy expenses approximately 56-81% more specific (HVAC 32-50%, Lighting 20-25%).

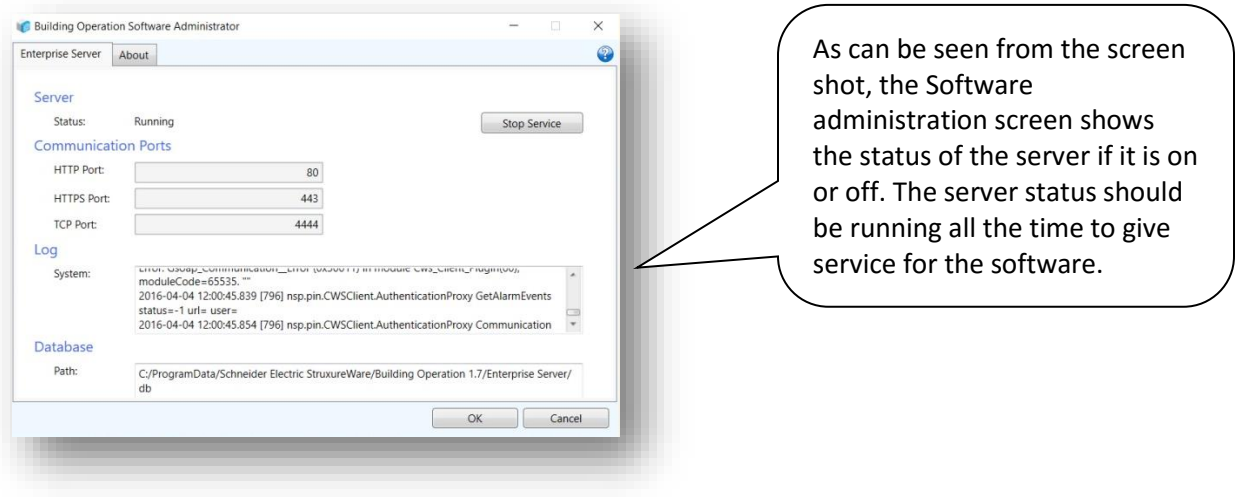
The web based graphical design as can be seen from the picture 3.22 gives the users a site map of their own system facilities. That means the user (DTU CTS Eng) has different kind of readings on temperatures or wind speed around DTU aria. Similar example can be applied to DTU University as it has several buildings each with individual building numbers: through the graphics the user is able to identify a specific building to work on. Moreover the buildings graphs each have individual floor functions with HVAC floor plans separated by temperature zones. Zones are colored so you can quickly see if anything is out of range; hovering over the thermostat will enlarge it to give a better overview and see even more data. The software is flexible and presents tools in many forms, including collapsible table and graphics. From a scheduling point of view, the user is able to create user schedules and calendars to manage when and what time the system should be active and put it in energy saving mode. Energy efficiency is everyone’s top priority: StruxureWare building operations is engineered to monitor, measure, and control energy usage through real time power consumption, and also monitor active and prior energy use to increase energy awareness [19]. Overall it is a smart tool which is used for Building Management tools for increased benefits.

## 3.2 Installation part

There are user rights needed for the software installation – a user license from Schneider Electric is required. To install the software there are possibilities to look at Schneider Electric's home page where they give further guidance. Make sure to install all the packages with the upgrade, server, repair, and reinstall Building operation products, as this is very beneficial. Regarding installation packages, there are different types of programs available which are based on your own usage habits; for instance a program such as Workstation has a graphic editor which helps to design a Function block diagram. Importantly, you have to make sure to install the license server for development of Hardware controllers and sensors. The following sections will demonstrate how best to work with the enterprise server.

## 3.3 Enterprise Server

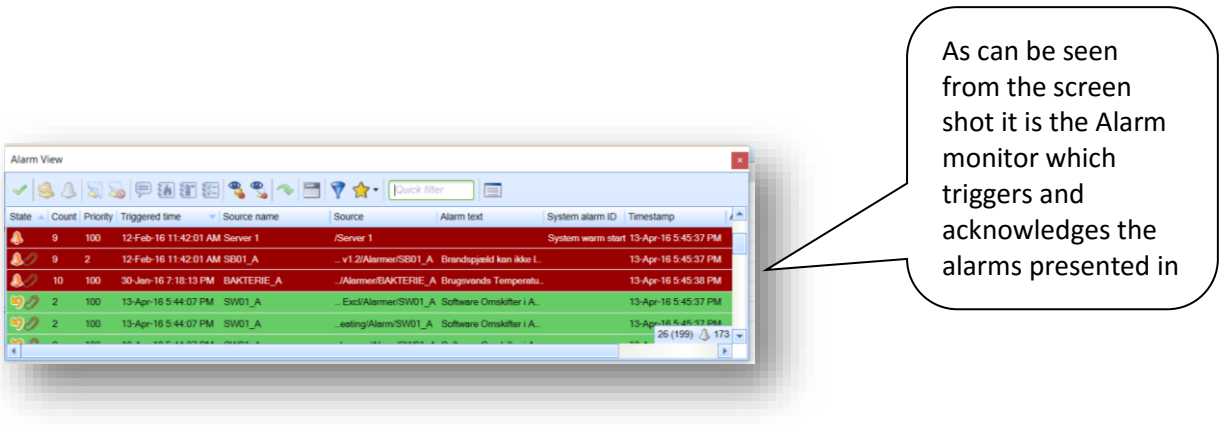
The enterprise server should run on the workstation that you are working on - without the enterprise server you will not be able to run the StruxureWare software. To activate the software administrator, click on the windows toolbar, under start and all programs, to look for the 'Building operation software administrator'. At the end, accept the software administrator to run the StruxureWare software.




Picture 3.1 Software Administrator for server set up

## 3.4 Understanding on how Alarm works

The Alarm monitor should be utilized when using this software as it indicates whether the monitor variables are matches. This gives the option to configure and send messages to a specified user when the alarm is triggered or acknowledged. When you want to monitor a sensor, you can create an alarm that triggers if the sensor is active or not. For example, you can place the Alarm on a floor heating algorithm. If the temperature drops, it should trigger the alarm. That means the user will be warned if the temperature drops, or in the worst case breaks down. The idea is that if anything like this happens, the message will be sent to an operator who is in charge to fix the problem.




Picture 3.2 Alarm view screen

Alarms are always in a fixed alarm state and are present in the alarm properties window. The state differs from the alarms; it is the normal represented state that the alarm monitors the variable. The Reset state has to be acknowledged by the user before returning to a normal state. A Fault state means the device reports the values which it knows not to be trustworthy, so the fault state will be activated until it is cleared. The Disable state should be known to the user as it can be used if any fault sensors trigger the alarm. As the word says, the system will show if any alarms are disabled.

The alarms can be placed to monitor from different sources, like BACnet devices or from LonWorks. They're also able to collect values from Enterprise and Automation servers. There are differences between the alarms; for instance there is an 'out of range' alarm which monitors the tolerance between the upper range and lower range limit.

## *3.5 Notification*

The actual idea on notification is to notify the user that a certain alarm event has placed in the system like if the motors stopped working. This notification message can be send either through E-mail or text file. The E-mail notification will be send through SMTP server protocol if any alarm occurs to the user. That means the user has to verify the notification which was send from the Struxuware software and they have the option to handle the alarm. There is also another way for the notification, where user doesn't have actual access to the StruxuWare software but wants to collect alarms. Where you are able to use the Simple Management Protocol (SNMP) which can manage devices attached to a TCP/IP network. Also the SNMP Protocol is privacy encrypted for the user which has strong security level as well. More over the Authentication protocol settings gives more selectable level on trustworthy information accessible through the network to keep away unauthorized person from damaging the notification.

## *3.6 Understanding how Trend Charts works*

Trend charts are able to display live updates of the trend log. Depending on the location time, the logs are able to record live updates automatically from any devices. For example I have been using sensors and dampers in my project which are recorded in the trend charts, such that if any actions were to occur the damper charts are able to display the correct time and date of the action. These details can be used for further developments, such as how many times did the damper activate, how much energy has been used etc.

## *3.7 Trend Log introduction*

Trend logs are used to log variables to that which they are connected to, and store records (such as logging the temperature motor to see how much energy it has used). Trend logs can also be shown numerically or graphically for further developments or improvements. Moreover, the trend logs are able to log digital or analog variables. One issue is if the sensor which is logged goes offline, meaning that the trend log will be affected. Therefore, it is better to place the log to the logged variable. More precisely, it is better to place the log where the controller is connected to an automation Server. The extended log is there to structure the log to a place where it has more capacity for storage.

There are different types of trend logs which can be used for different purposes. The Meter trend logs are capable of calculation of meter exchanges and meter rollover. This means if you place the Meter trend logs on any kind of metering device, it is able to calculate all the readings – for instance if the log is activated or created from January, the meter reading will be 00000. Once it passes over to the end of January it will show how much energy or water has been used, for instance 52778. It is exactly how our energy meter readings works. There are differences on how the charts are displayed in a Variable, Trend Chart or Trend log. Furthermore, there are options on replacing the old meter with new meter - there should be some changes made to the system. In the management options, the changes should be applied to have new meter readings.

Manual trend logs are able to record manually entered data. This is used for devices which are unreachable or connected to the building operation. For example, if we were to take metering devices not in the building, they can be manually entered to get a reading from them. Implicit trend logs focus on changes in value to monitor the IO variable and new value record. The log can be placed for all kinds of devices with IO ports and can store approximately 500 records (voltage, temp, current, resistance) automatically by the buildings operation.

The interval trend log is there to catch up on or collect data at a specific time interval to have a collation of data. The idea is have certain times to stop the recording which can be used if you don’t wish to record the same data again, or if a device is replaced for maintenance purpose.

## *3.8 Command Property Process and levels on BACnet*

To assign different levels of priorities to command property in to BACnet it used the struxuWare software. There are 16 different priories available in the BACnet which are known as commendable properties and controlled by the process. When we look at it close it has 11 available levels and two top priority levels are used for personal safety. From the following list you are able to see the list of priority levels:

1. Manual Life Safety
2. Automatic Life Safety
3. Priority 3, available
4. Priority 4, available
5. Critical Equipment Control
6. Minimum On Off
7. Priority 7, available
8. Manual Operator
9. Priority 9, Available
   These priority are followed until 16.

## *3.9 Project overview and planning*

I have used an FB diagram to create a smart algorithm which is able to control indoor temperature, outdoor weather and floor heating. Before creating the algorithm, I looked at different options and analyzed how it can be done in better way. There are different software tools available but in my case I have used StruxureWare software to create the algorithms. This software tool is a smart tool which can be used for future developments. I could create a smarter algorithm with the software tool, which is smart enough to save energy by up to 30%. In the following sections you will be able to understand more about the algorithm and the controller's functions.

### *3.10 Network Architecture*

There are several devices interconnected to each other as can be seen from the following figure. This is my own network architecture which I have created to do my project. There are several devices interconnected to be smart and energy efficient:

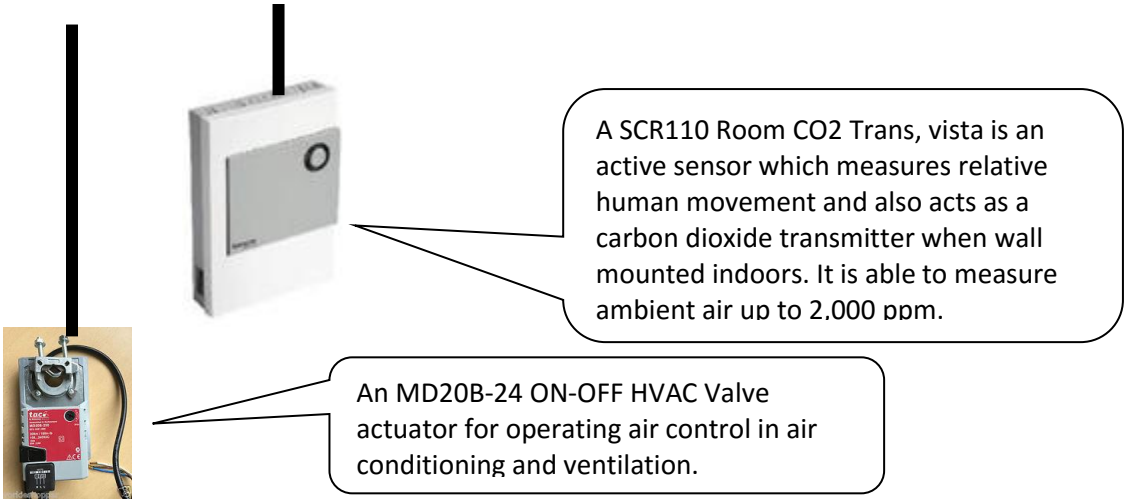
The Main **Server Workstation** is where the software (StruxureWare) functions. The Server is the core of the system and provides the core functionality, such as trend logging, alarm supervision etc. The Enterprise server is the core system to run stand-alone applications

The PoE + Switch 24 port HP is for connecting the Workstation with the automation servers. This is the network connection for the system.

Ethernet TCP/IP /BACnet IP

The Automation Server connects to the switch which can be accessed from the user through the workstation. It also connects to the individual sensors, motors, lights through I/O Models.

A Servodan PIR sensor detects activity in the designated area such as humans, levels of movement etc. It has a lux function which can be used to control lighting level.




Picture 3.3 Struxuware software network architecture

### *3.10.1 Automation server I/O module*

There are different kinds of automation server available for different kind of actions. An automation server can have around 32 modules attached to the module and one power supply with connected I/O modules. There are differences in I/O devices, such that they can only support a fixed number of inputs and outputs. Others are capable of different electrical types such as universal inputs and digital outputs. From a memory perspective, if there is a power failure all the important variables are kept saved as they have flash memory. This means the flash memory is able to keep the data safe when a power cut occurs.

There are advantages in supporting building standards such as BACnet, Modebus and LonWorks. The built-in FTT-10 port is capable of getting access to the LonWork and Xenta devices. The automation sever supports LonWork as it has its own binding tool to get communication on a LonWorks network.
Modebus: Modbus RS-485 master and slaves configuration and integrated IP client and server use for devices which supports modebus protocols Controllers (lighting, meters).
BACnet: Communication on BACnet MS/TP and BACnet/IP network to get access to BACnet and b3 devices.

The Automation server communication ports:

- An Ethernet 10/100 megabit port. It is dependent on the switch which is attached to the server, and there are different types of server which are better at communicating to different specific devices. For more and larger file transferring, it is better to have high quality of communication ports which can be gained from the Automation server.

- Two RS-485 ports also known as TIA/EIA-485 which is an electrical characteristic used in digital systems. This is used for long distance (1,200m) and in particularly noisy distances and environments such as industrial areas.

- The LonWork (TP/TFT) local operating network's purpose is to address the control applications.

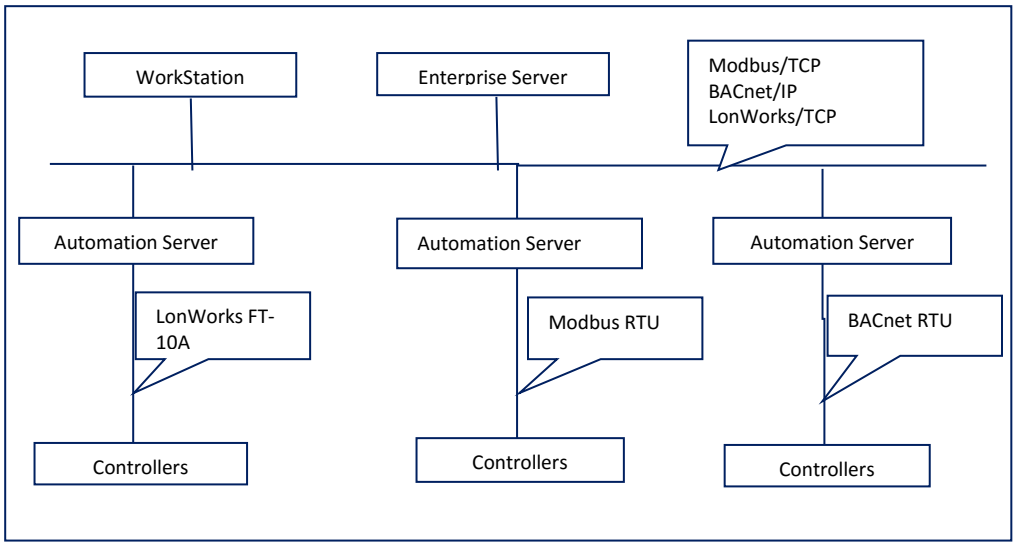
Automation server operation:

- Systemic operation for local control.
- Able to inter operate with third-party control devices.
- Support various protocols (BACnet, LON, Modebus).
- Integration support on security, HVAC or lighting system.

From the following table and drawings you are able to see all the communication ports which are in the automation server.

| Automation communication port | Connection |
|---|---|
| *USB devices* | *Device Administrator* |
| *Ethernet 10/100* | *LAN/WLAN, BACnet, Modbus and IP* |
| *RS-485 COM A* | *Modebus and BACnet* |
| *RS-485 COM B* | *Modebus and BACnet* |
| *Backplane Input/output bus* | *Internal power supply and I/O addressing* |
| *LonWorks (FT and RS-485)* | *LonWorks* |

3.4 Table: Automation sever options




3.5 Picture: Automation Server protocol options

### *3.10.2 Sensors*

I have used the PIR Sensor 41-271, which can be used for areas such as corridors, offices, school permissions, canteen, sports halls, lounge, and warehouses. It also has the function to adjust the lighting in a hallway to be dimmed or brightened. This means the sensor is smart enough to find out if the room or the area is brighter or darker to turn on/off depending on the levels of humans. The Presence sensor type 41-340 is able to detect 360 degrees for small movements such as in offices. That means they have the optical function with two detection ranges to detect small movements.The new energy-autonomous PIR-sensor can be used for the intelligent lighting control system. That means the movements PIR sensor can be connected wirelessly and has a solar function to avoid battery function. The very sensitive inferred sensors receive and measure the general temperature of the room around it, depending on movement the sensors changes the temperatures. It is precise enough that it can actually identify, by movements, the change required for the detection.

There are lots of sensors available in the market for people's own system needs and we have to make sure what type of sensor we are going to use. Also we have to make sure what sensor is used in the system, such as what gateway the sensor supports. Most wireless sensors are much smarter and can be used on most every system. The PIR sensor does have the functionality on dimming the lights which maximize the energy saving of the lighting by dropping down the light level to most efficient stage. In this case new LED lighting technology can be applied to the sensors and provide less energy and comfort by best suits the lighting level in the room or aria.

### *3.10.3 CO2 sensors*

SCR series from the Schneider Electronics living spaces sensor CO2 measurement levels. This sensor is placed in the area where it can capture the temperature and air level. The purpose of the sensor is to collect the temperature and air level inside a room and send the information to the algorithm which I have created. Then the algorithm is able to collect the data and have an energy efficient function. That means through this data the algorithm can manage the heating or cooling system.

### *3.10.4 Humidity sensor*

There are different types of sensors available in the market. Most devices are smart enough to detect humidity and temperature levels in the room. Humidity is the level of water in the air, which can affect human comfort and the room climate. To measure and control the humidity is very important in some industries as they have sensitive products or equipment which has to be maintained. When we look at living environments in the building, humidity sensors are important to have. Some sensors do have wireless options: one of them is the Vaisala Wi-Fi data logger.  It is a humidity and temperature sensor that can be used in laboratories or in larger rooms, as it has a resistance to dust and chemicals. It is able to connect to most wireless access points and does need battery changing. But there are backup opportunities on external power sources which can be used.

### *3.10.5 Sound Detector*

There are different kind of sound detector Circuits available such as Arduino or RaspberryPI. These are single board computers that are the size of a small visiting card. Moreover there are different types of generation available for different kinds of purposes. This means these chips are small computers, where the user is able to program for their own purposes. In this sense the programming languages used are Python, C, C++ or Java, etc.

When we look at Arduino microcontroller chip, it is similar to the RaspberryPI microcontroller and does similar tasks as well. Arduino can be used for interactive objects with open software design for development, such as working with several devices. This means they can be used for design with a group of devices, and multiple shielded together to get better qualitative achievements.

The reason why I have mentioned these chips is because they can be used for replacing the PIR sensors. As we know, these sensors are able to detect any movements if a person accesses the area. Compared to an Arduino chip, it can be used to detect noise around it, meaning some unwanted noises can still be detected. However, the PIR sensors, whilst improving with diction, still have some issues. For example, in a lecture room there are lots of students listening to the lecturer who is performing the presentation. But these students, as they are listening to the lecture, don't perform any movements and thus cannot be detected by the PIR sensor. For that reason sound detection sensors can be replaced or added to solve the problems.

There are some sound detection sensors available to provoke lighting systems: for instance by clapping your hands or playing music the light will turn on or off. My idea is to place a sound detector Circuit with a PIR sensor to improve its functionality. In this way, if the PIR sensor is not able to detect anything, the sound sensor should do the task. There are some issues with placement of these sensors: when we place the sensors outside, there are different decibel (dB) levels than when we place it in the buildings. From the following table 10.6 you are able to see the difference decibels (dB) readings. That means the sensors should be programmed differently for the environments as they have different noise values.

| Environments | Decibel Scale (dBA) |
|---|---|
| *Chainsaw* | *160* |
| *Jet Takeoff* | *140* |
| *Lawn Mower* | *90* |
| *Motorcycle* | *100* |
| *Vacuum Cleaner* | *80* |
| *Hammer Drill* | *114* |
| *Hand Drill* | *97* |
| *Air conditioning unit* | *60* |
| *Conversation* | *65* |
| *Tree leaves* | *40* |
| *Floor fan* | *50* |
| *Refrigerator* | *40* |
| *Pin falling* | *15* |

3.6 Table: DB readings on different devices and places

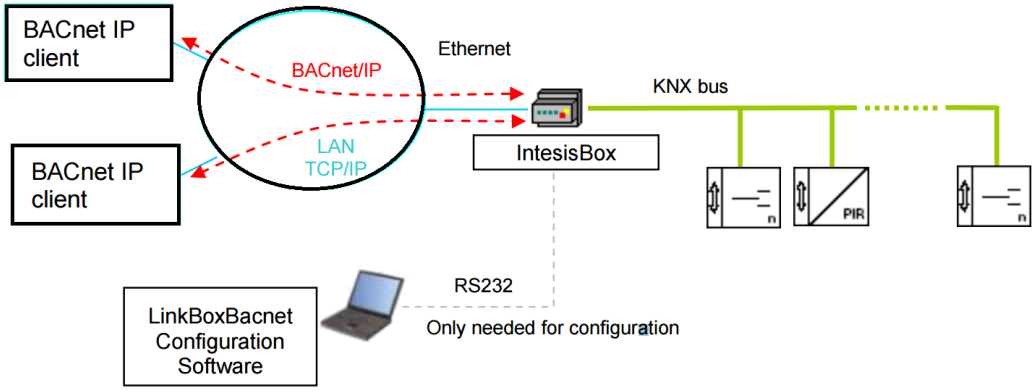
## *3.11 Examples on different Controllers and Sensors*

As we have seen on pervious writing I have stated what kind of dives I have used to design. From the following Picture you are able to see different Kinds of sensors, controllers and bridges presents which can be used for further developments.

3.7 Picture: Controllers, Sensors and multi propose Managers

## *3.12 How to use EIB/KNX with BACnet*

This writing gives us the details description how we can apply our design to different European Installation Bus (EIB) Function Block describes the semantics how it can be access the function with associated service. That mean there are needed “Datapoints” which are divided in two different categories as input and output. Furthermore the function blocks do have non-empty collection of one or several input and output data points at least with one data points. In the following Picture 3.7 you are able to see an example which gives closer understanding on how KNX integrate (EIB) system into BACnet controller system. That means there are some kinds of IntesisBox available which is able to act like BACnet/IP Server to allow communication with BACnetIP client devices to other network. Let us look at KNX side architecture intesisBox acts as the main devices which are able to control all the services in the KNX devices. The IntesisBox get connection to the individual devices in the KNX system through EIB bus technology. These can be used to transport information (read and write) through Internet to the other side of the network system such BACnet and LAN TCP/IP. There are some software’s which is able to configure LinkBoxBACnet to have these kinds of communication possibilities.




Picture 3.7 IntesisBox allows different gateway options

From the below list you are able to see the BACnet IP Server to KNX gateway using IntensisBox. For further BACnet gateway configuration see the link [21].

| KnX (EIB) devices | BACnet control system |
|---|---|
| **Management Automation devices** | **SCADA system** |
| **Home Automation devices** | **Building Management Systems (BMS)** |
| **Pump control system** | **Human Machine Interfaces (HMI)** |
| **Lighting controller** | **Direct Digital Controllers (PLC)** |

As I have talked in the previous writing on how to use EIB/KNX with BACnet, so the IntesisBOX can be used to interconnect directly with the internal systems, such as Industrial and building automation, LonWorks, KNX, BACnet and Modebus etc, with external system HVAC, lighting or alarm control and so on. There are possibilities where the users are able to use the IntesisBOX with console RS232 port via a PC to program or monitor the network. There are more possibilities in getting connection through Ethernet/LAN/WAN networks to expanding with Ethernet/IP based protocol system (Alarm monitoring, web server, e-mail alarm sending).
Gateway possibilities:

- ASCII Server – BACnet/IP Client (enables connection on read and writes between these two technologies).
- ASCII Server (connection on RS232/TCP/IP) – KNX (EIB Bus).
- ASCII Server (connection on RS232/TCP/IP) – LON (TP-FT/10).

Using IntesisBOX as BACnet/IP Server to talk to another protocol.

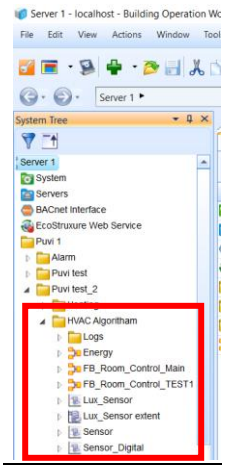
- BACnet/IP Server (BACnet/IP and LAN TCP/IP) – KNX bus.
- BACnet/IP Server (BACnet/IP and LAN TCP/IP) – LON (TP/FT – 10 network).
- BACnet/IP Server (BACnet/IP and LAN TCP/IP) - M-BUS (RS232/RS485).

## *3.13 Function Block Diagram (FBD)*

There are different types of function block diagram which perform different functions. These algorithms are able to do different types of functions which you are able see in the following diagrams (Picture 3.8). FBD is the graphical representation of the application which has different function blocks and connections between the blocks. Starting with the HVAC algorithms, as can be seen from the diagram this is able to control in/outside temperature and any activity in the rooms. That means it is able to detect human activity and temperature level in the room. If someone is in the room it is able to keep the temperature at 20°C; if the room is empty the algorithm is able to save energy by turning off the devices which are not relevant and keep the temperature constant. Moreover there are no need for human action which means the algorithm is able to automatically adopt the climate level with in and outdoor temperature. Also The StruxuWare software do provide supervisory control function on the algorithm where the user such DTU campus net CTS engineers are able to change any activities or mange the HVAC system.

**HVAC Function Block diagram**

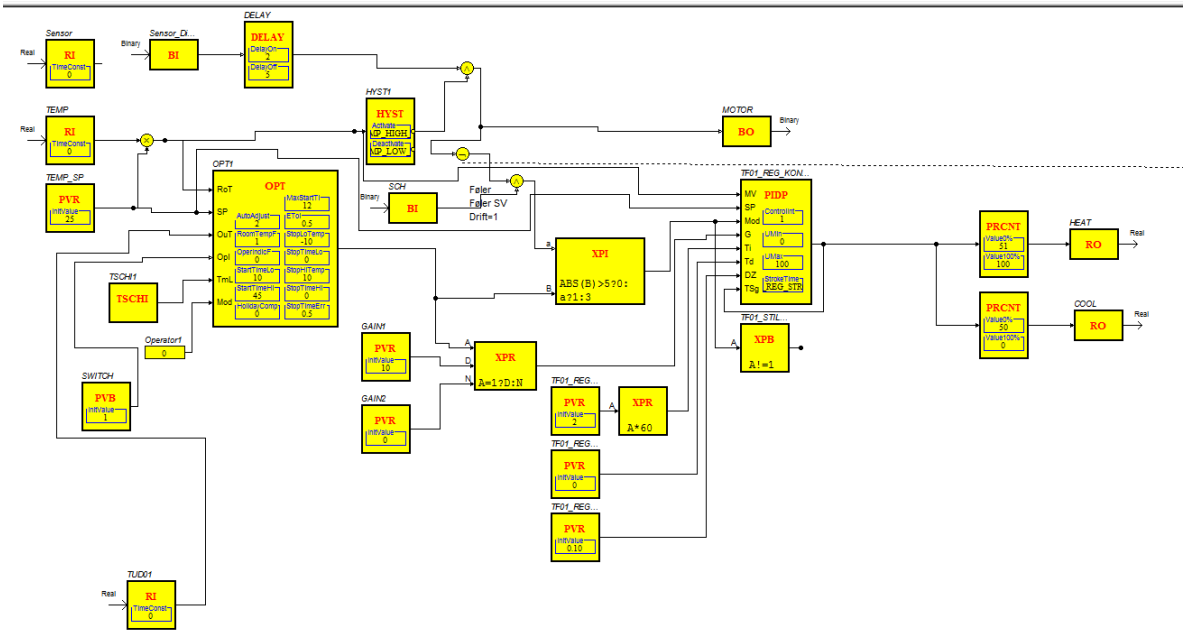
1. File structure of the HVAC algorithm




File structure of the HVAC Function Block Diagram. As can be seen from the figure there are files with logs and FB.

2. Drawing a Function Block Diagram

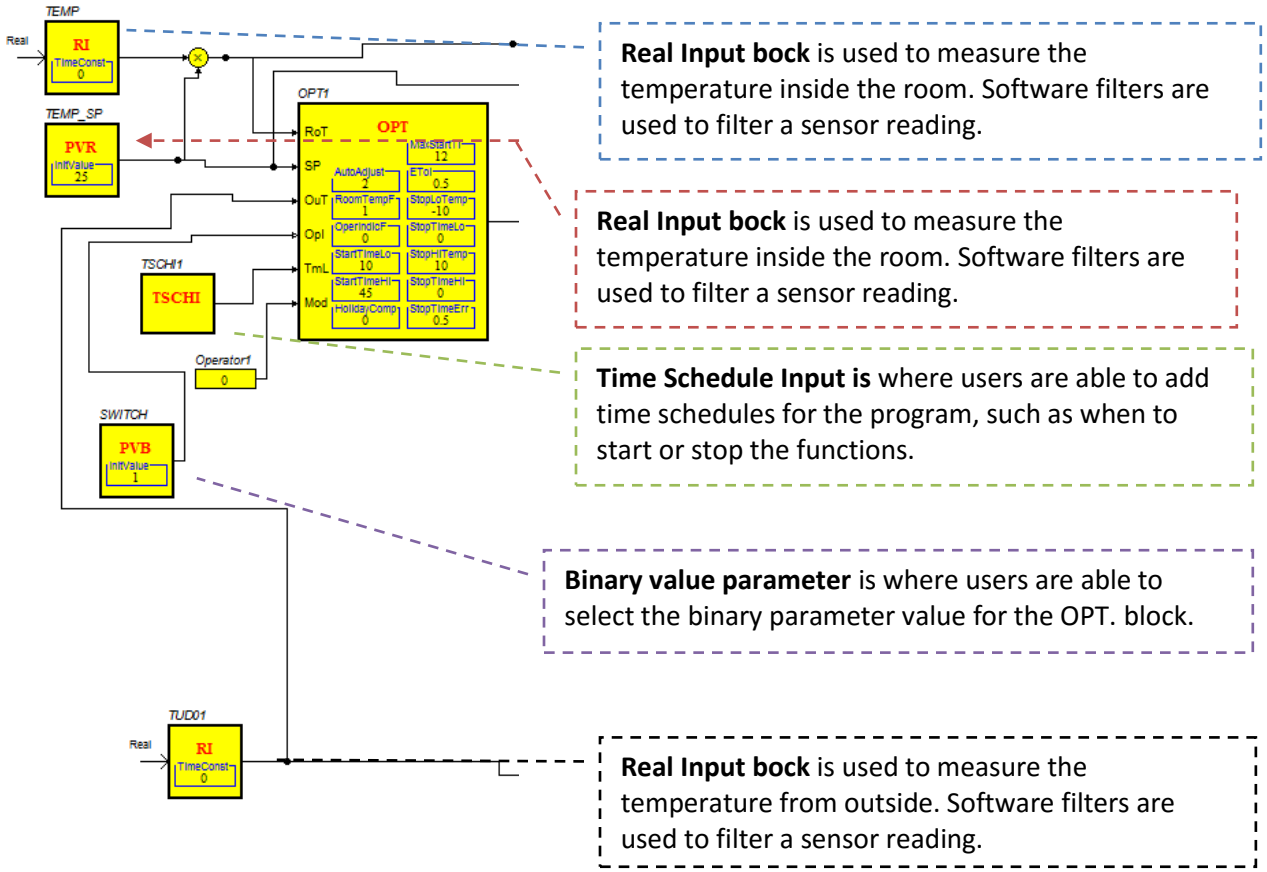
It is a graphical representation of the application and shows the connection between function blocks. Before starting to talk about the algorithms, we should know the fundamentals on programming the TAC Menta. Each individual programming devices can be categorized in three different phased:
Design phases: Dependents on the software application have menus for an optional operator panel for design and appliance.
Functional phases: There are different types of functional analysis which specifies function on needs.
Test phases: During development each individual function can be testes and used for further developments.
For further information on FBD do have read the paper which gives more specified and details information on the products.
From the following figure 3.8 you are able to see the entire HVAC control algorithms.




Picture3.8 FBD HVAC control algorithm

3. Description of HVAC FBD first part

We will focus on the first part of the function block diagram:




Picture 3.9 FBD HVAC control algorithm part 1

4. OPT – Optimization

As can be seen from the figure 3.9 OPT function: The OPT function is used for cooling or heating applications, and the algorithm is able to execute once every few minutes. For instance, starting the heating/cooling system in advance gets the correct temperature during a normal operation. It can also automatically stop the heating/cooling system before the normal operation. That means with this operation it can manage to keep the temperature constant even if the outdoor temperature falls below zero.

When we look at the Start time optimization the start time is calculated every minute depends on the TmL > 0. In order for it to be optimized, it is best to set the start time to be longer then the time in normal operation. From the curve we are able to define the start time between the outdoor temperatures (OuT). If the room temperature is not in use, the start time will be calculated from the curve with possible holiday options. When a room sensor is connected, the curve instead yields the start-time per °C deviation between the room temperature (RoT) and its

set point (SP). For instance, the start-time will be 80 min if the curve yields the value 60 min at the outdoor temperature, and the room temperature is 3 °C too low.

There are possibilities to have holiday compensation, which means if the building's heating systems were shut down for longer periods of time. Longer heating time and energy is required to reach the desired temperature, due to the fact the buildings are cooled down more effectively. For this reason there could be an extra percentage of the starting time to be added. For instance, if the outdoor temperature is less then -5 °C the heating time should be adjusted to the indoor temperature. That means the heating system should keep a constant temperature, but if the outdoor temperature is more than + 20°C the heating system shouldn't perform any more actions.

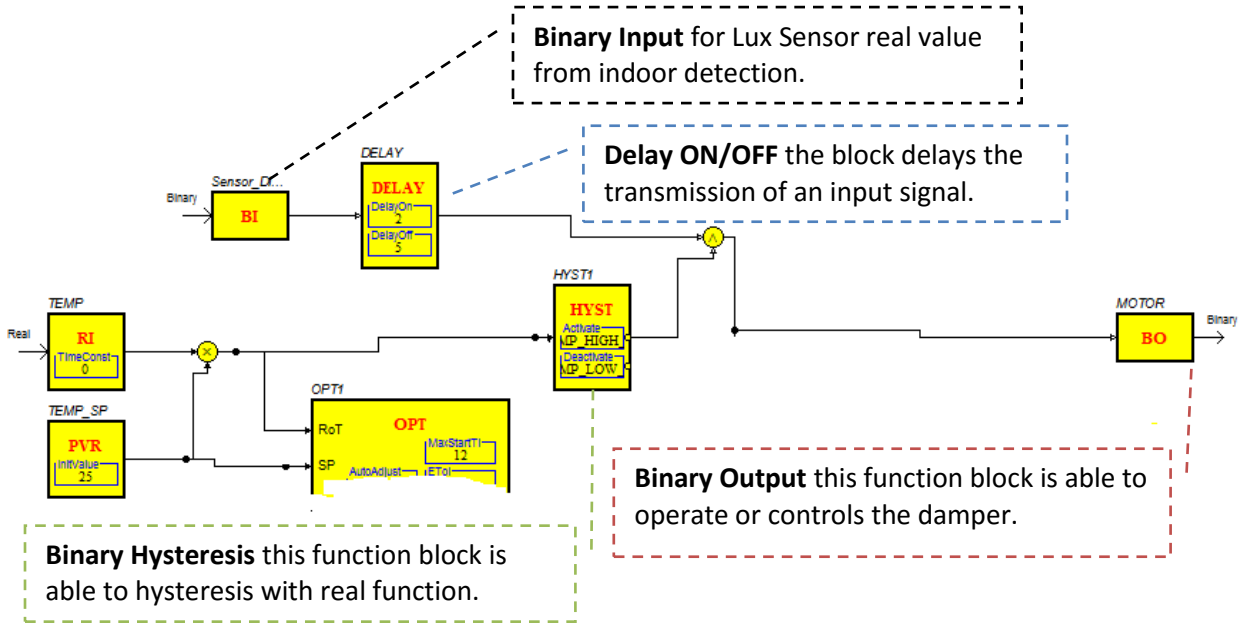
| | | |
|---|---|---|
| RoT | REAL | Room temperature. |
| SP | REAL | Room temperature set point during day time. |
| OuT | REAL | Outdoor temperature. |
| OpI | BINARY | Operation indicating if the controlled equipment is in operation.<br>OpI = 0=> not is use.<br>OpI = 1=> in use. |
| Tml | INTEGER | If the time left until the plant should be in operation. If negative, OPT interprets the size of TmL as the time until the plant should shut down. |
| Mode | INTEGER | Switch for disabling optimizer.<br>Mode = 0=> heating.Default = 0, i.e heating.<br>Mode =1=> cooling.<br>Mode =-1=> no optimization. |
| AutoAdjust | INTEGER | Automatic control on Switch.<br>AutoAdjust = 0=> no adjustment.<br>AutoAdjust =1=> adjustment of curve points.<br>AutoAdjust =2=> adjustment of curve points and holiday compensation. |
| RoomTempF | BINARY | Room sensor flag. If 0 the sensor is not present; if 1 the sensor is present. |
| OperIndicF | BINARY | Flag for selecting operation indication, such as if 0 is not present or 1 present. |
| StartTimeLO | REAL | Start time in minutes at low outdoor temperature -10 to any. Default =105. |
| StartTimeHI | REAL | Start time in minutes at high outdoor temperature 10 to any. Deafult =45. |
| HolidayComp | REAL | Holiday compensations it the system has been shout down >45h. Default =0. |
| MaxStartTi | REAL | Max start time in hourses default 12 |
| ETol | REAL | Temerature error when switching from optimization to normal operation efault =0.5. |

| | | |
|---|---|---|
| StopLoTemp | REAL | Low outdoor temerature piont in stop time optimization °C (F°). Default -10. |
| StopHiTemp | REAL | High outdoor temperature piont in stop time optimization C (F°). Default=10. |
| StopTimerHi | REAL | Stop time when outdoor temerature = StopHiTemp. Default =0. |
| OUTPUT | INTEGER | Read and Write. |

Picture 3.10 FBD the OPT function

5. Description of HVAC FBD second part

As can be seen from the figure 3.11 there are 3 different sensor inputs which have different functions. These are connected to the motor (damper) which is used for the cooling system or for windows. When we look at the delay on and off function block diagram, it is there to transmit the signal by the specified delay. The If Delay on the signal must be true to generate a pulse on the block output and, if off, reset the output to false. The Binary Hysteresis (HYST) function block has a real input signal and binary output signal.



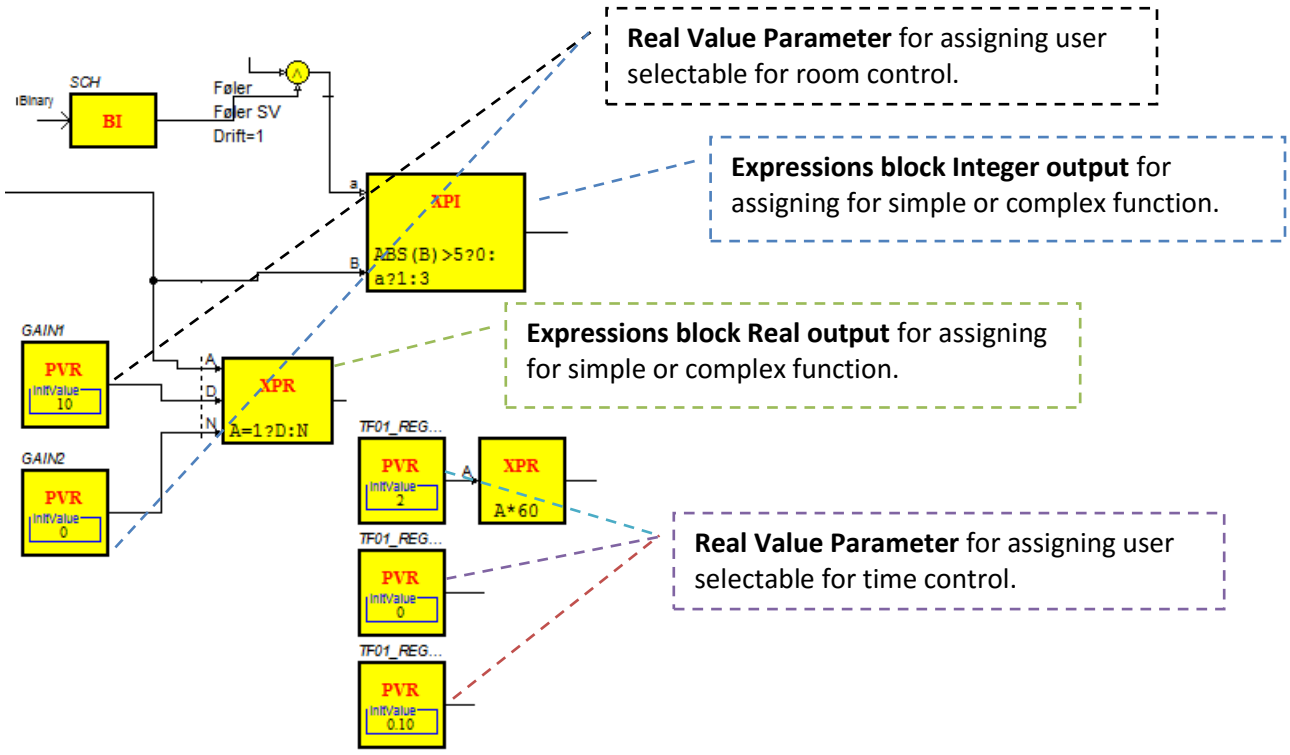

Picture 3.11 FBD HVAC control algorithm second part

6. Description of HVAC FBD third part

There are real value parameters assigned to the expression block where users are able to place some value.

The algorithm on the real output expression block represents (A=1?D:N). The capital letters represent analog input and in this algorithm the expression block is able to calculate: If analog input A equal to 1 IF-THEN-ELSE D included N.

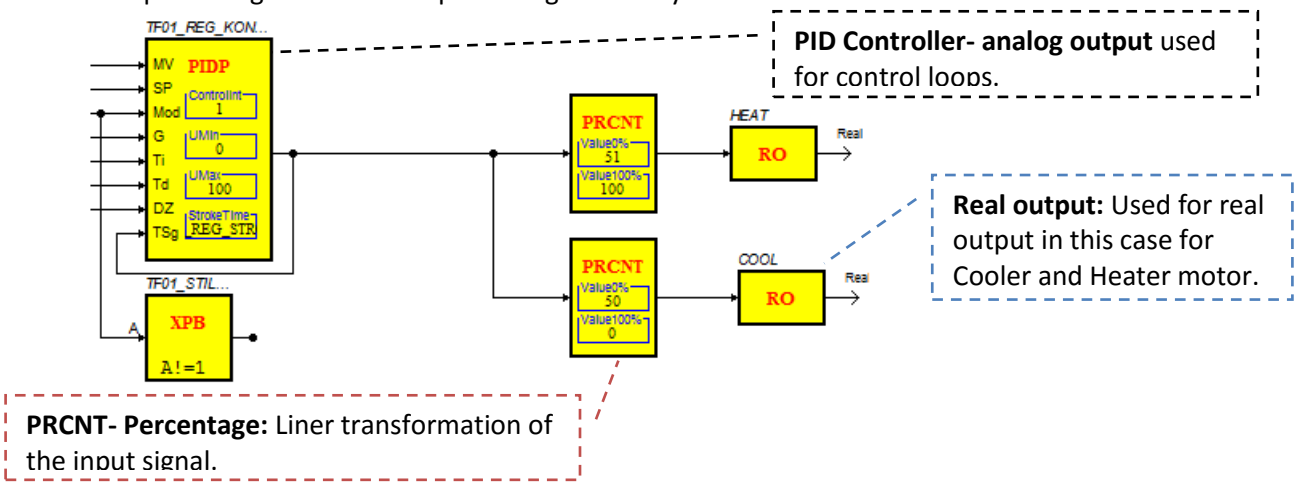
The algorithm on the Integer output expression block represents: Analog input ABS followed by B greater than 5 IF-THEN-ELSE 0 or binary inputs IF-THEN-ELSE 1 to 3.




Picture 3.12 FBD HVAC control algorithm third part

7. Description of HVAC FBD fourth part

The PID controller is designed to control the heating and cooling function, before it is connected to the percentage block to add percentage to the system.




Picture 3.13 FBD HVAC control algorithm forth part

8. Test on HVAC FBD

From the previous writing you could read about how HVAC FBD made and function. Now you are going to see tests on each individual components and devices from crated algorithm.

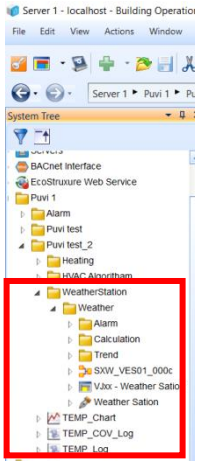
| Test on individual components or designs | Test result |
|---|---|
| Binary input from the sensors (PIP lux and CO2 sensors) | They work as they supposed to do and get real temperature around the sensor aria which is accurate. The both sensors works well to the damper. Also the PIP lux sensor is able to measure the light level around the aria. |
| If someone is in the room how dose these sensor and controllers react? | The PIP sensor detect the persons every movements and send it to the delay adder which is able to delay (light or heating) for some minutes. The outdoor and indoor sensors are able to measure temperature and send it to optimizer adder, which is able to keep the place in optimal or controllable temperature level. |
| Where can we use this FBD algorithm? | It is a smart algorithm which could be places mostly in all small and lager rooms and for own purpose it can be adjusted in temperature level. The smart algorithm provides outdoor temperature level which is used for the temperature level in the building. Like if the outdoor temperature drops the indoor temperature will be warmer. |
| Are there any possibilities to adjust the operation time on the systems? | Time schedule information block is able to schedule the building operation. That means the users are able to program the block to turn |

| | |
|---|---|
| | on/off the functions on the devices from some period of time. Like set up time from 7am to 7pm the system should be turned on but rest of the time it can me in save mode. |
| If the indoor Temperature more then set up temperature what will happen? | The eating function will be activated and the windows will open. |
| If the indoor Temperature less then set up temperature what will happen? | The cooling function will be activated. |
| How does the window algorithm work? | The windows will only open if the temperatures are high and if someone is in the room. Also it can be set up when the function shouldn't work like in the night time. |
| Dose the window open if the room temperature is cold? | No it doesn't open the window. |

## DTU Weather station FBD

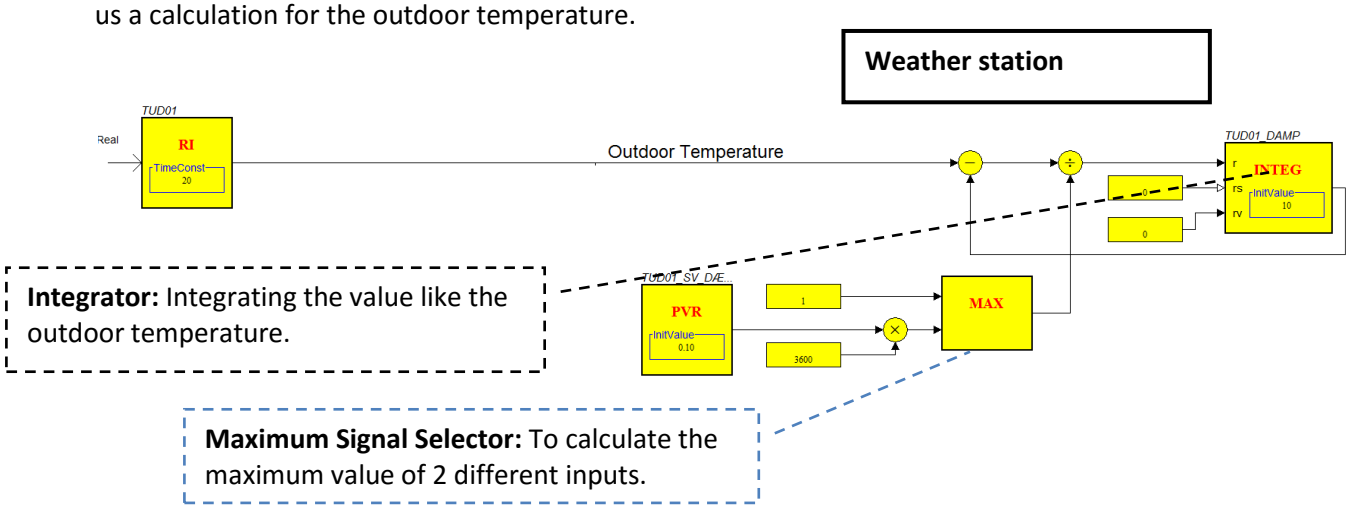
1. File structure of the Weather station from DTU

   This function block diagram represents the real weather station from DTU through a measurement device. This shows there is also another way to work with the software.



2. Structure of the Weather station from DTU step one

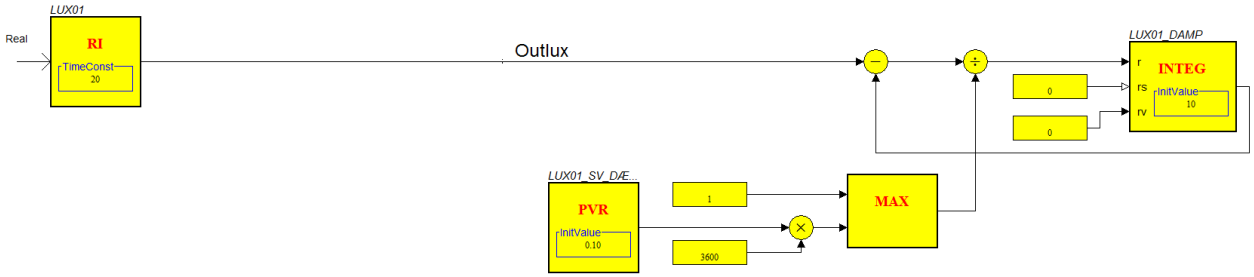
Before starting with the program we have to understand why we need the weather station. In the previous function block diagram you could see how the indoor algorithms work, but there was a lack of outdoor temperature. This weather station will help us to get outdoor temperature. Also provides data on weathers which were three days back. That means if someone would like to see how the weather was last three days or later month. As the FBD is big it needs to be broken into different parts in order to write about the functionality. We will look at the first part which calculates the outdoor temperatures. As can be seen from the figure, there is a real input FBD connected to the Integrator block, which allows the integration of the temperature flow over time. There are also values from the Real value parameter block to give us a calculation for the outdoor temperature.




Picture 3.14 FBD Algorithm for weather station part one

3. Structure of the Weather station from DTU step two

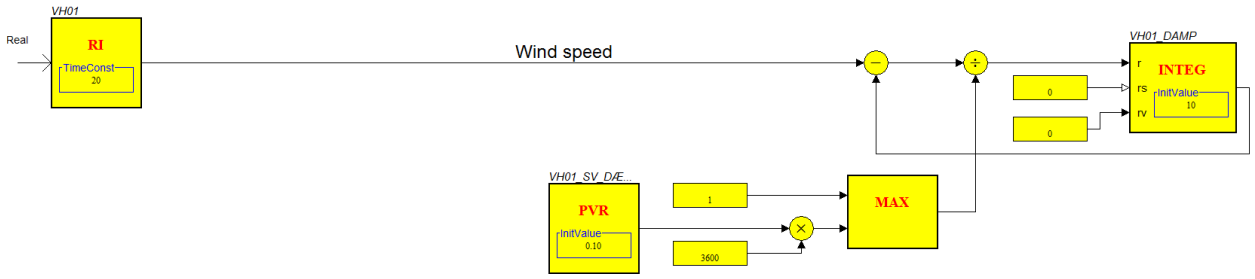
In the second step you are able to see similar drawings, but they are used for different functions. This is for calculating the Outlux: this is the means from the DTU sensor by which we are getting outside sunlight level. It tells us how dark or bright it is outside and it is only from around DTU.




Picture 3.15 FBD Algorithm for weather station part two

4. File structure of the Weather station from DTU step three

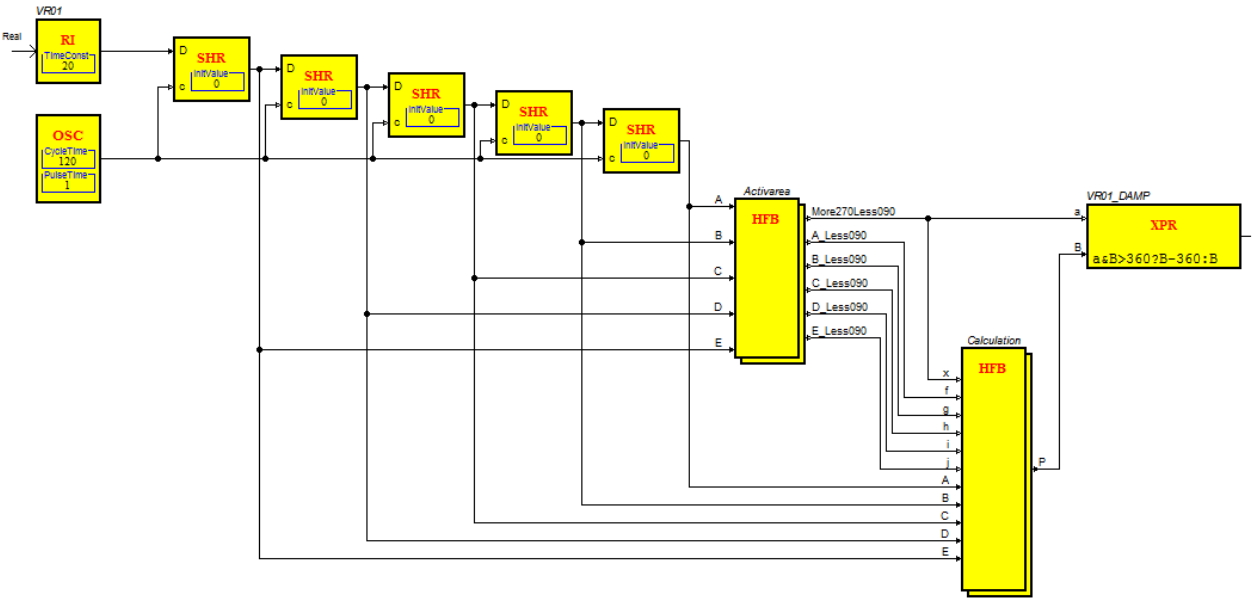
In the third step we are able to see how to calculate the wind speed.




Picture 3.16 FBD Algorithm for weather station part three

5. File structure of the Weather station from DTU step four

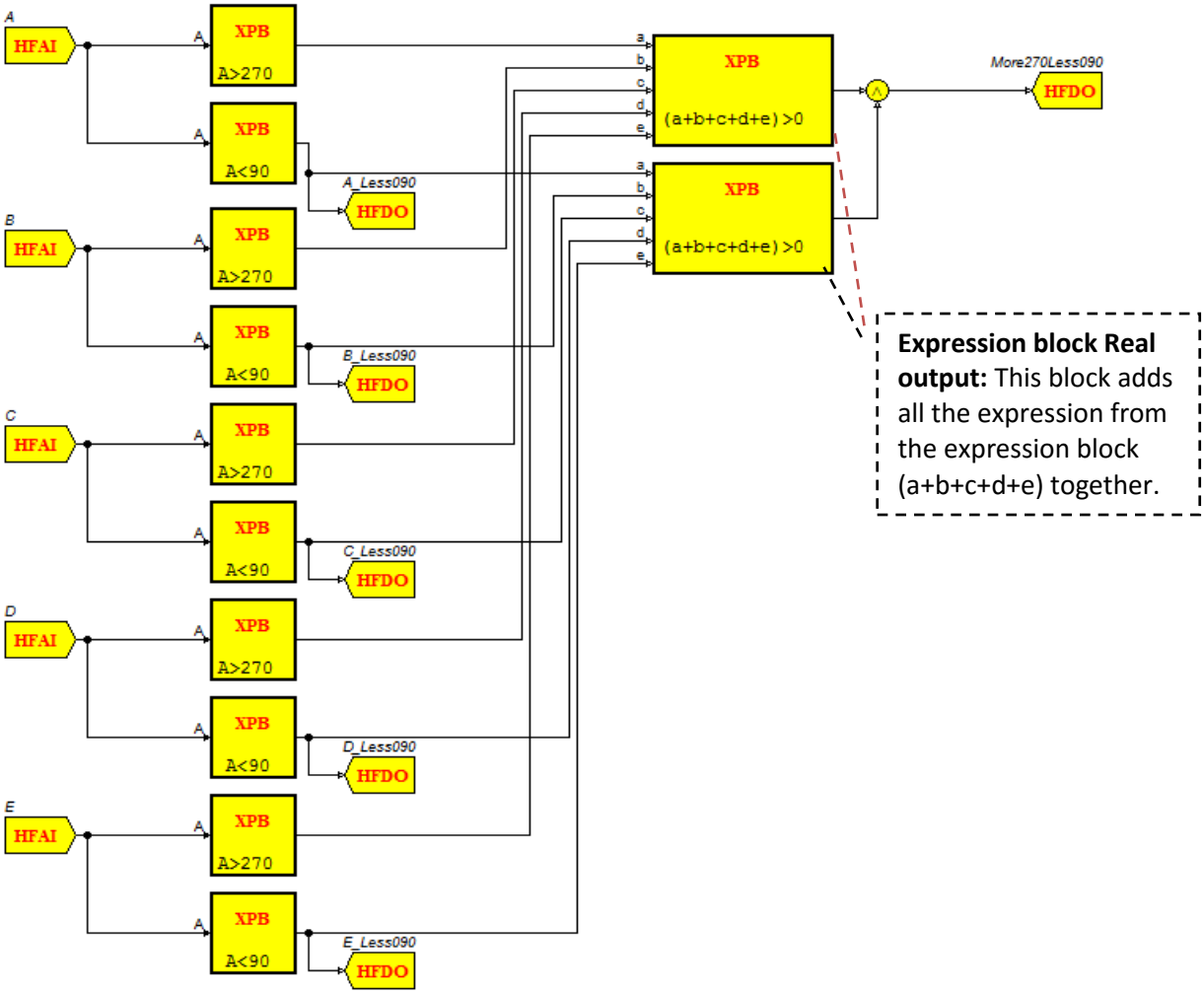
As can be seen from the function FBD there are calculations and activations for the Weather station. There are real inputs for day wind direction which is connected to the 5 individual samples and hold real value: that means the user is able to manually input. Also an Oscillator is added to the 5 different samples and hold real value, which is able to generate a train of pluses with a period of cycle Time and duration pulse Time. In the next drawing you are able to see more about the other FBD.




Picture 3.17 FBD Algorithm for weather station part four

6. Structure of the Weather station from DTU step five

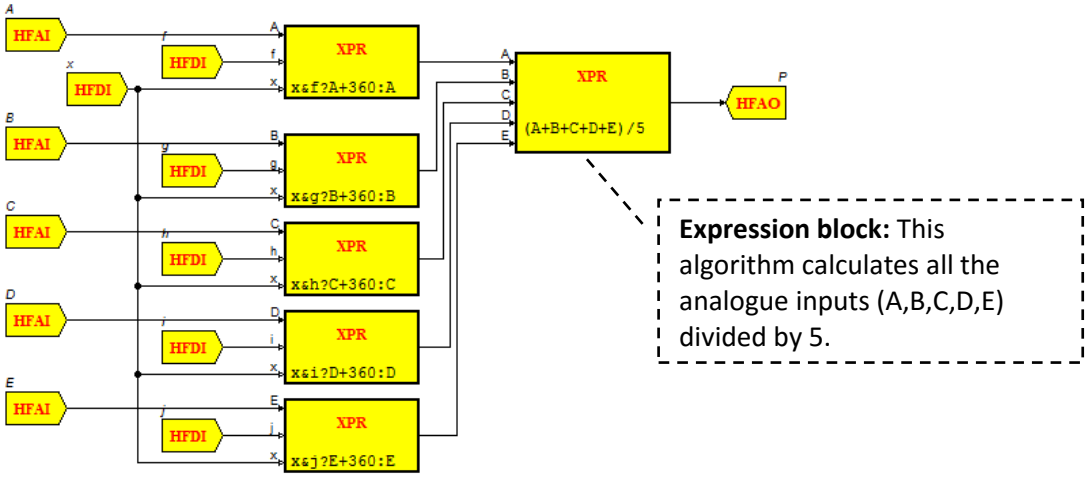
Hierarchical Function block can be used for grouping blocks and can contain other compressed function blocks and connections. In our case we have 5 different analog inputs (A,B,C,D,E) which are connected to the expression block (binary output). For each analog input there are two different expression blocks. One is designed to calculate if A is more than 270, the other designed to send a calculation of whether A is less than 90. These expression blocks are connected to the other expression block (binary output) which calculates all the analog input from the 5 different analog inputs.




Picture 3.18 FBD Algorithm for weather station part five

7. Structure of the Weather station from DTU step six

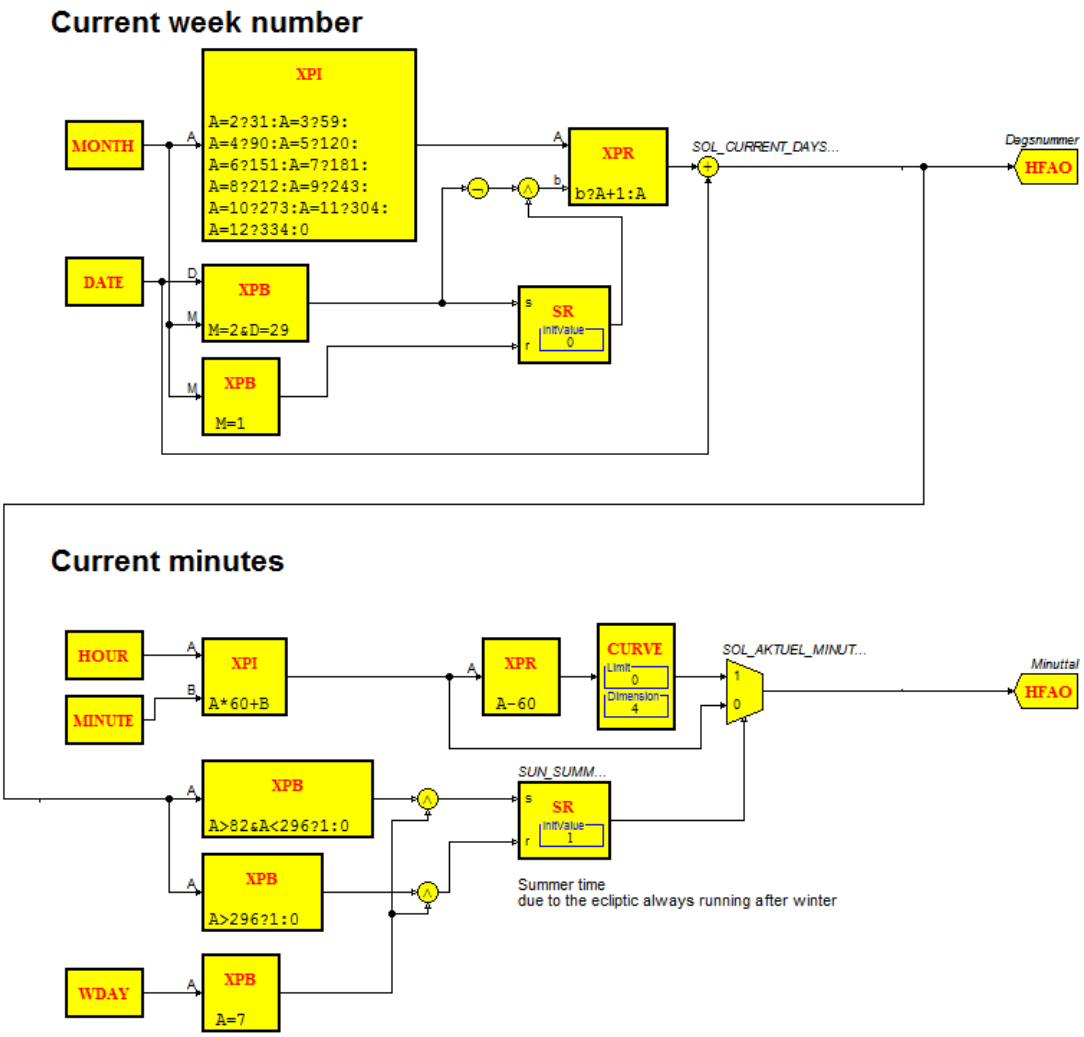
This FBD is similar to the previous FBD, but here calculations are on 5 different analog inputs and 5 different binary inputs. These inputs are calculated from different expression blocks.




Picture 3.19 FBD Algorithm for weather station part six

8. Structure of the Weather station from DTU step seven

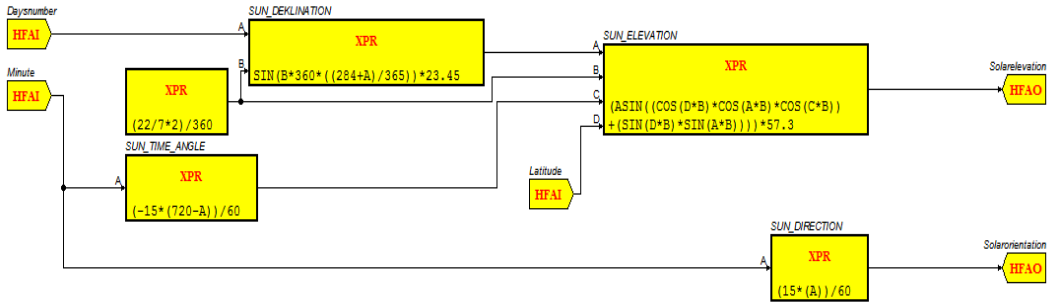
There are different calculations on current week numbers and current minutes. The current week calculation is calculated based on months and date such that month A is equal to 2 then 31 else A equal to 3 then 59 else. There are also calculations on 90, 151 etc. When we look at the expression block binary output, it calculates the month and date (M equal to 2 then D equal to 29). These are calculated from different expression block real output block (B then A addition to 1 else A). These are likened to current munities calculation blocks and for output for day number calculation.




Picture 3.20 FBD Algorithm for weather station part seven

9. Structure of the Weather station from DTU step eight

In this FBD, the angle of the sun with respect to the equator and altitude in the sky is calculated. That means it able to calculate the current height of the sun solar orientation with the arithmetical functions.

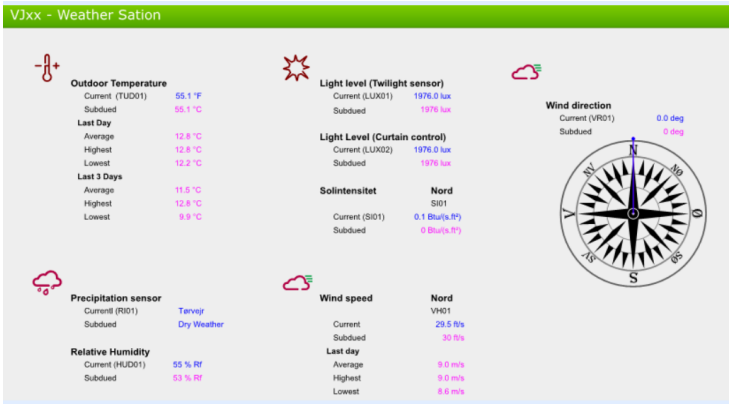



Picture 3.21 FBD Algorithm for weather station part eight

10. Structure of the Weather station from DTU step nine

This is the graphical design of the Weather station where the users are able to see real time weather reading IDE. This graphic is for web application for the user to use with remote access to the weather station. As can be seen from the figure there is the current Fahrenheit from the DTU and:

- Outdoor Temperature: This gives current temperature level in Fahrenheit and Celsius.
- Perception sensor: lets us know the location of the sensor.
- Relative humanity: The rain level in percentage which is accurate such as how heavy the rain is.
- Light level Twilight sensor: This sensor is able to detect outside humidity such as if it is dark or light outside.
- Light level curtain control: This is the same as the twilight sensor but it is able to look at the indoor humidity, for instance if it is getting dark outside the indoor lighting level is different.
- Wind speed: Calculate the wind speed in around DTU.
- Wind direction: looks at wind directions.




Picture 3.22 FB Weather station user interface part nine

11. Plain English for Weather station for DTU step ten

There are two programming options possible on Smartstruxure solution: Script and function block. This gives the user a good programming method for the applications. The main focus for the script programs are to give the server easy commands, such as turn on/off the fans, or if the temperature is high or low to turn on/off etc. Moreover, the Script programs are easy to understand and follow logic. The advantage is you are able to store common documents of the script programs for later use or for other projects. It is also able to write programs which can be used for very complex control systems like control motion sensors. To run the Script programming there should be a connection to the task to which the property objects can be used for the program cycle.

As I have mentioned earlier, there are differences between script and plain English. When we look at the binding variables on object properties, there needs to be a declaration for the scripting program to access. But compared to plain English, the path and property names are used in this case. To declare a binding variable in my project I have chosen the FBD files and chosen the specific bock and used script editor.

There are also differences between the Priority level accesses for configuring BACnet. As I am working with BACnet priority level access and need to look at the path level, I have to make sure not to use the full path level access for the BACnet. That means I have to bind the variable to a specific property priority level. As you can see from Picture 10.21 there are scripting (plain English) programming languages which are calculated for the Weather station. There are different calculations which are based on specific days, such for the current and previous day's weather measurement. These are the reasons for this further development, for saving energy and make the future system smarter and usable.

**Weather calculation**

```
Numeric Input VALxx_DAMP     'Valxx_Damp is bound to a
Damp object
Numeric Output VALxx_GSNIT
Numeric Public VALxx_MAX
Numeric Public VALxx_MIN
Numeric VALxxArray[288]       '1Day of 24Timer of 12*5Min
  24*12 = 288
Numeric tempArray[288]

Numeric i,j,k, Dag
String Input VALxx_Gsnit_IN  'Data type
String Output VALxx_Gsnit_OUT 'Data type
String tempIN

Init:
 'Here must be corrected if cuts <> 1 day that means is
calculated
'with days.
  Dag = 288

  i = 1

  tempIN = VALxx_Gsnit_IN 'Function call
  j = search(tempIN, ";")
  while (j>0 and i <= Dag)
    tempArray[i] = strtonum(mid(tempIN, 1, j-1))
    tempIN = mid(tempIN, j+1, 10000)
    j = search(tempIN, ";")
    i = i + 1
  EndWhile

 if i > 1 then
  i = i - 1
 Endif

 'Find start index
 k = Dag -i
  'Move the stored data end of Array
  for i = k+1 to Dag
    VALxxArray[i] = tempArray[i-k]
  next i

 'Complete Array with actual outdoor temperature
  for i = 1 to k+1
    VALxxArray[i] = VALxx_DAMP
  next i

 goto Calc

'Calculation on average, Maximum and Minimum for the

Calc:
 VALxx_Gsnit_OUT = ""
 for i = (Dag-1) to 1
   VALxxArray[i+1] = VALxxArray[i]
 next i
 VALxxArray[1] = VALxx_DAMP
 VALxx_GSNIT = average(VALxxArray)
 VALxx_MAX = Maximum(VALxxArray)
 VALxx_MIN = Minimum(VALxxArray)
 for i = Dag to 1
   VALxx_Gsnit_OUT = VALxxArray[i]; ";"; VALxx_Gsnit_OUT
 next i


goto pause

pause:
 if TS > 299 then goto Calc 'every 5. minutes (TS)Total
Seconds
```

This field shows the declaration of the binding variables where the path names and properties are used.

This field shows the calculations on the days for the weather station (last day and for last three days).

This field shows the calculations on Average, maximum and minimum.

Picture 3.23 Weather station scripting calculation part

12. Testing on Weather station for DTU

| Test on individual components or designs | Test result |
|---|---|
| Dose all the sensor work properly? | All the Sensors (Outdoor, Precipitations, humidity, light level, wind speed) sensors are working in order. The sensors are able to collect data from the DTU weather station and provide as diagram on pervious measurement data. These data can be collected from the user for further developments. |
| How smart are these weather station algorithm? | These sensors can be used to connect with indoor temperature algorithms and can be used for data collection on Weather changes. |
| Dose the weather station applied for whole Denmark? | No actually the idea is to take the weather reading around DTU universities. This algorithm can be used for different weather readings sensors. |

13. Data collection Weather station

There are some options in the software where user are able to collect data from the Weather station readings. That means the user are able to collect data from the sensors like temperature. Which will be showed as a function diagram from all the reading from the weather station to current temperature level to previous temperature level. From the Picture 3.24 you are able to see different readings diagrams shows the weather activities. From the chapter 4 you are able to read how you could collect the weather reading data with some web application.

Picture 3.24 Weather station data collection

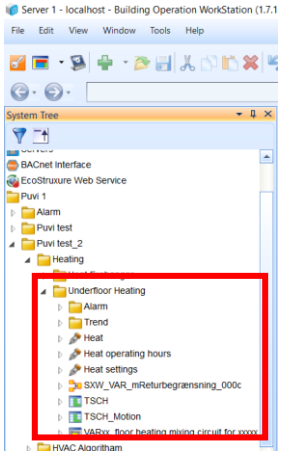
There are different kind of solution where the data from the weather station can be stored or maintained. One solution might be to use Structure Query Language (SQL) data base which is designed for managing data from some programing languages. There are option to use Microsoft Access with visual studio to pull Weather reading data from the StruxureWare software to Microsoft Access. These data can be managed or developed in the Microsoft Access for further developments.

The second option might be to use Data center infrastructure management (DCIM) where the data can be stored and managed. These data reading from the weather station can be stored on the server for further use or keep safe from being anciently deleted. Schneider electric StruxreWare do provide data centers software which can be used for this purpose.

1. File structure of the Underfloor heating

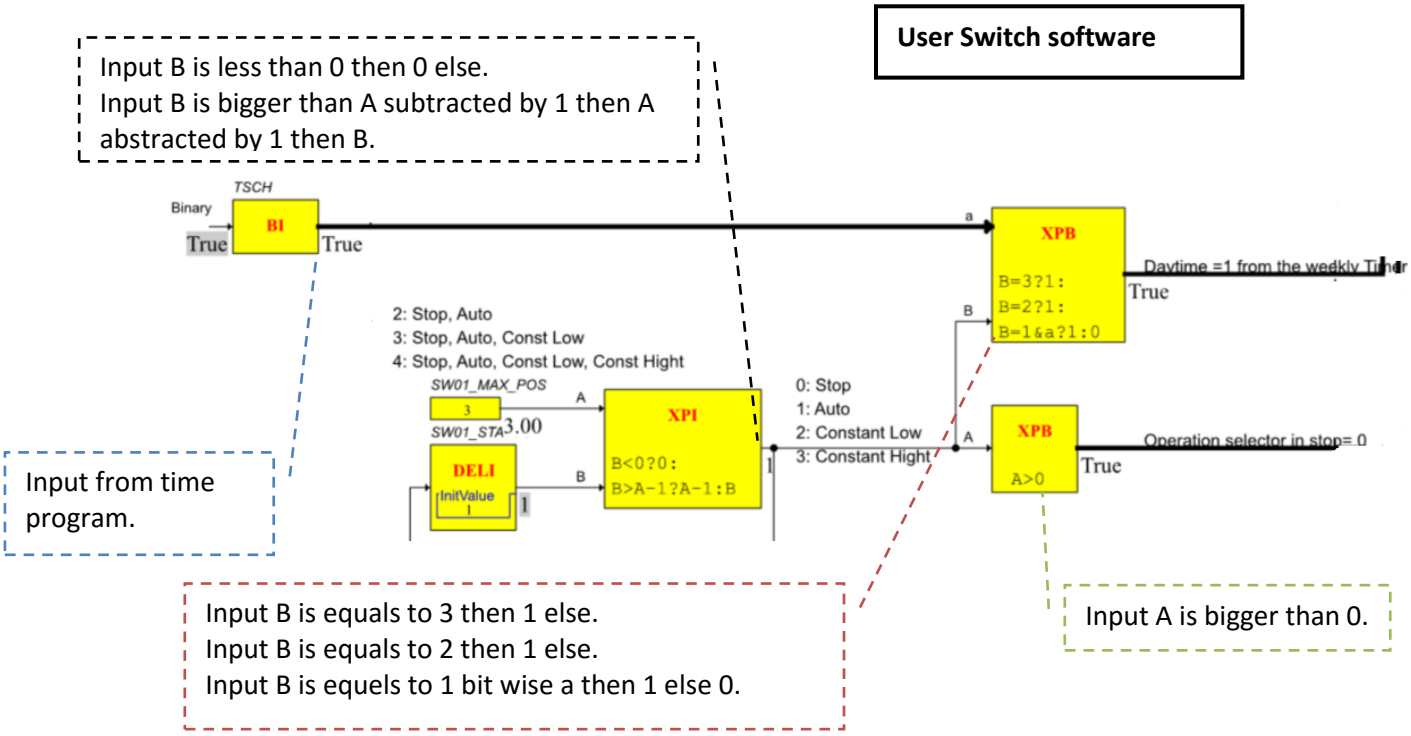
This function block diagram represents the Underfloor heating system for the indoor climate control. Underfloor heating systems sit beneath the stone, floor, or tiles to warm the floors and rooms, in private homes, companies and even in larger organisations. Moreover it will replace the entire radiator which can save space and decrease energy levels. There are two different types of heating system available: one with electrical underfloor heating-based on a dry system, and the other a water underfloor heating-based wet system. The water heating system has different types of pipes which run under the floor to the boiler, which is able to control and manage the heating system. There are other possibilities where you are able to save energy, such as connecting the pipes to the solar water heating system or air source pump. When we look at the energy efficiency of floor heating systems they are much better than radiators. Because the heating is derived from the floor it is more evenly distributed and keeps the water at a lower level. The only downside is it can be pricy to install and the floor needs to be replaced as well.

The prices vary depending on the systems you are looking for. You need to decide which type of system (whether water or electric) you want. In the following writing you will see algorithms which will control the underfloor heating system. The file structure shows how I have structured the algorithm.

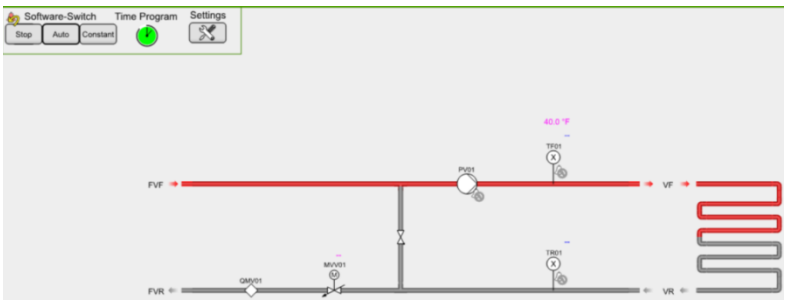


2. Underfloor heating and cooling system step one

In this writing you are going to see how the algorithms are created and what functionality they provide. These algorithms are created from the FBD and have different kinds of functionalities to include smart and energy savings options. In practice, the user will be able to use the algorithm with the specific software on a workstation or via mobile phone (such as through an app). The thermostat devices (Sensors, transmitters) can also have the algorithm, which will allow it to control or regulate the system. This software switch has an optional number of positions and inputs from the digital schedule. The following FBD diagram represents the switch operation functions, similar to a thermostat controller. As the user, you are able to control the floor heating system with the switch (thermostat). The functions are structured in a smart way, so the users are able to control the system manually, automatically etc.



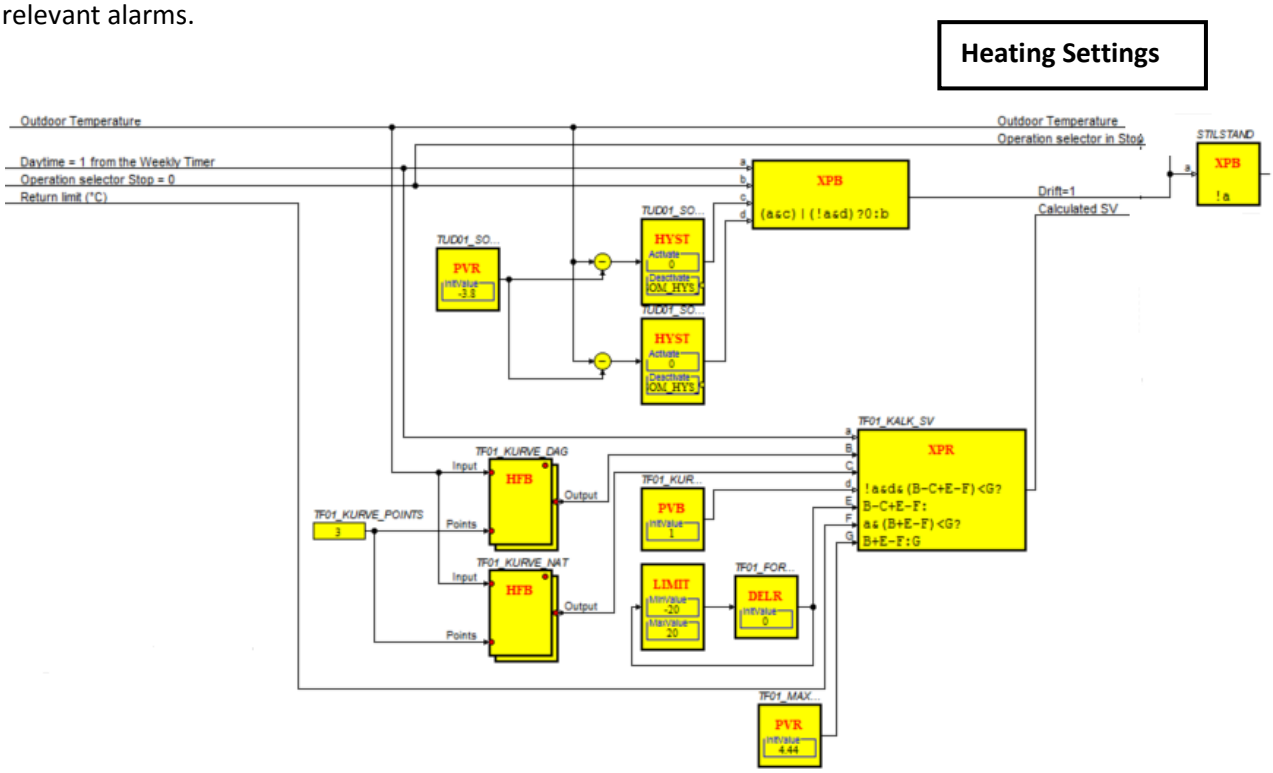

Picture 3.25 FBD Under floor heating and cooling system part one



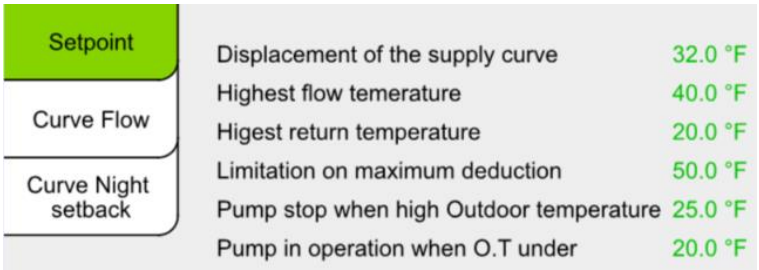

Picture 3.26 FBD Under floor heating and cooling system user interface

3. Underfloor heating and cooling system step two

In this section you can see the FBD controls the heating circuit and stops the temperature during the summer, based on outside temperatures. It contains a curve for Supply temperature and curve setback, based on outdoor temperature. It can be managed to disable setback and maximum limitation of flow so the floors are not damaged. Signal for the return limitation is a limitation of the set point at high return temperature. The signal DISUSE used MIXER-was relevant alarms.

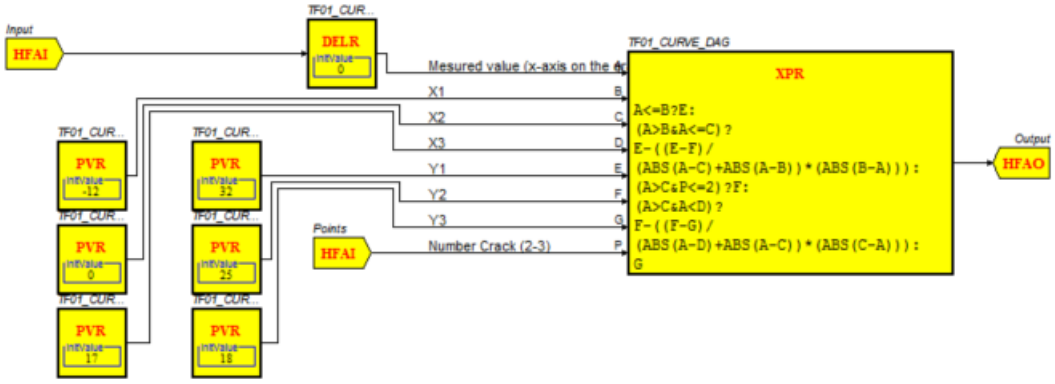



Picture 3.27 FBD Under floor heating and cooling system part two

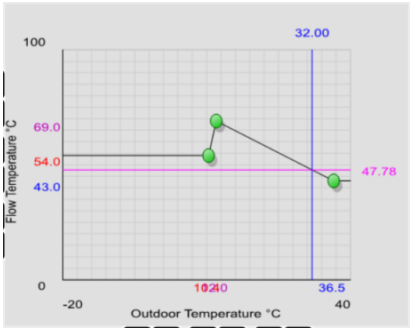



Picture 3.28 Under floor heating and cooling system user interface for setting

Curve calculation on days is performed inside the heating system. This means the users are able to see the measurements and calculations related to day time in the heating system. There are six different types of initial value inputs which are calculated in the expression block.

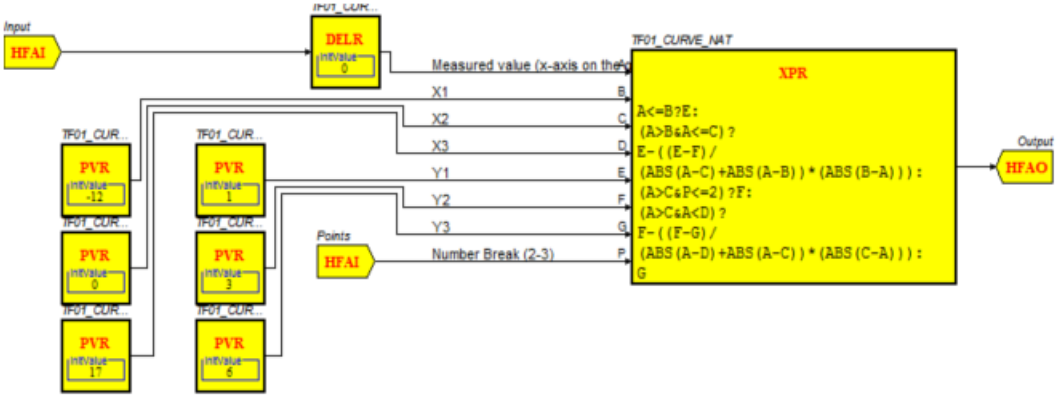



Picture 3.29 FBD Under floor heating and cooling system part three

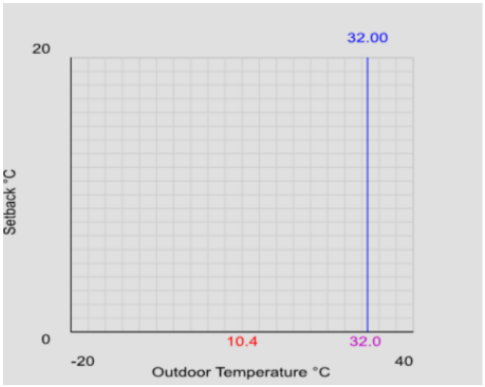



Picture 3.30 Under floor heating and cooling system curve calculation (user interface)

Curve calculation for night which is done inside the heating system. It is a useful algorithm which helps to keep the heating system from breaking down and save energy through smart way of functioning.



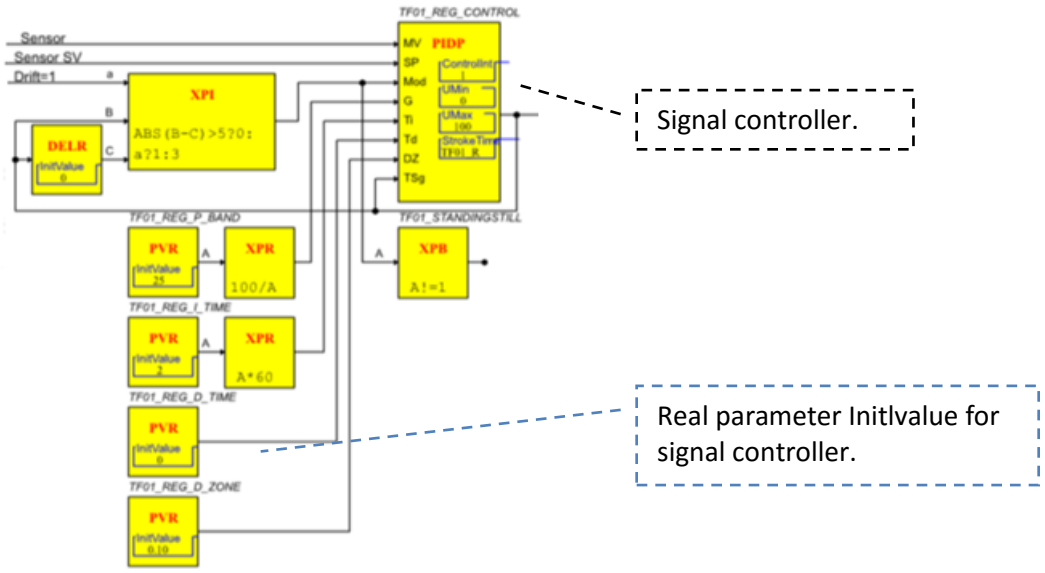

Picture 3.31 FBD Under floor heating and cooling system part four




Picture 3.32 Under floor heating and cooling system curve calculation (User interface)

4. Underfloor heating and cooling system step three

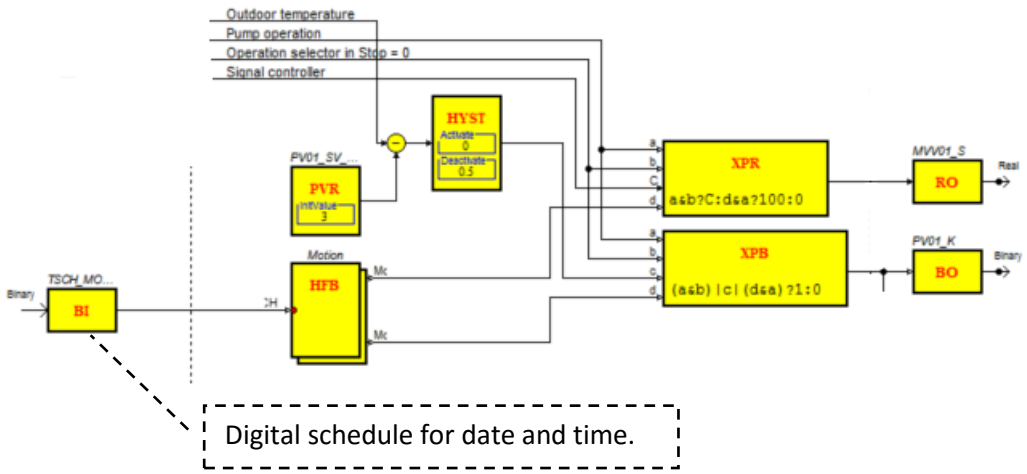
This part focuses on the REG controller for the sensors in control loops for the signal controller.




Picture 3.33 FBD Under floor heating and cooling system part five

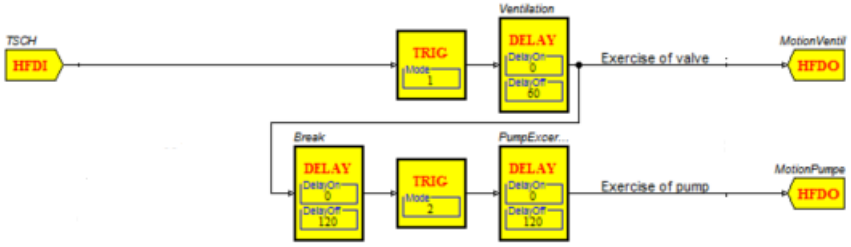
5. Underfloor heating and cooling system step four

Handle Pump & Valve based on the signal from the switch controller. Receiver signal of motion from another macro, unless the switch = 0.



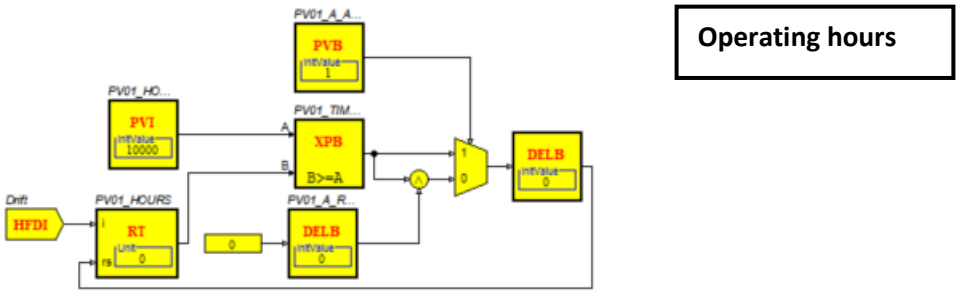

Picture 3.34 FBD Under floor heating and cooling system part six

Exercise of valve and pump. Guided by the time program (Digital schedule) upon activation, is exercised in the following sequence:
- Value exercise for 60 seconds
- Break of 120 seconds
- Pump kicks for 120 seconds

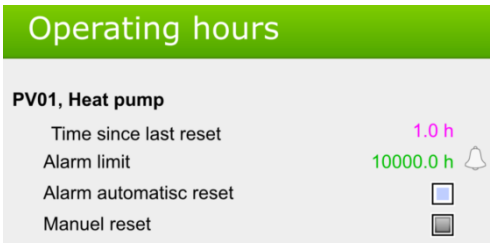



Picture 3.35 FBD Under floor heating and cooling system part seven

Counter number of service hours - you are able to choose whether the system will reset the counter when it reaches a set point, or whether it will be done manually. It must be combined with an operating hour alarm.



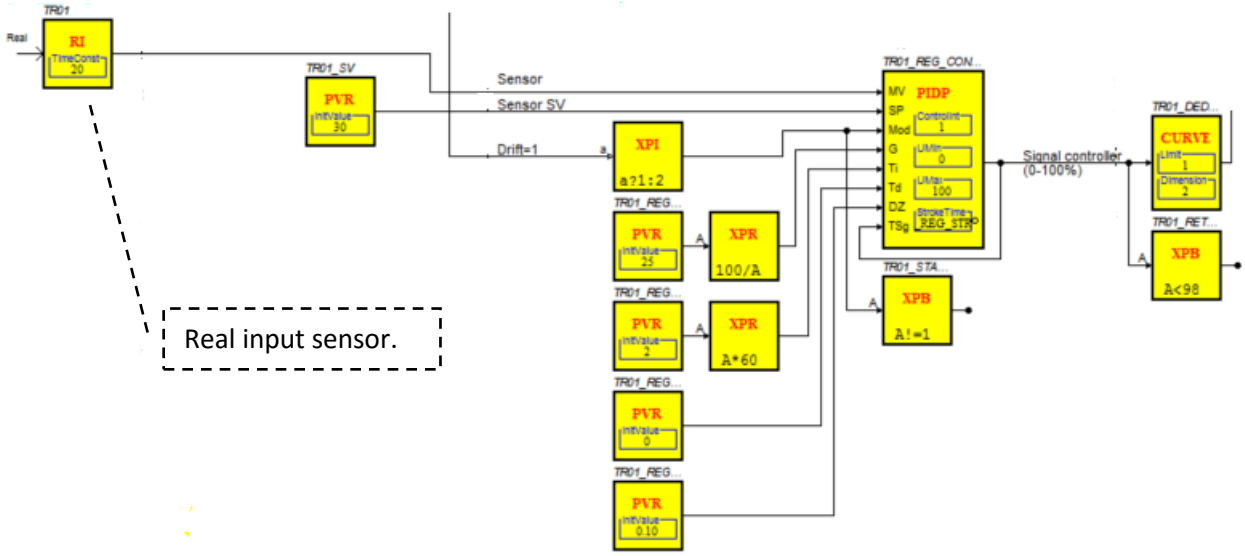

Picture 3.36 FBD Under floor heating and cooling system part eight




Picture 3.37 under floor heating and cooling system (user interface)

6. <u>Underfloor heating and cooling system step five</u>

Regulator for management signal controller.
- One option after the flow temperature
- Second used to return limitation




Picture 3.38 FBD Under floor heating and cooling system part nine

7. Testing on Underfloor heating and cooling system

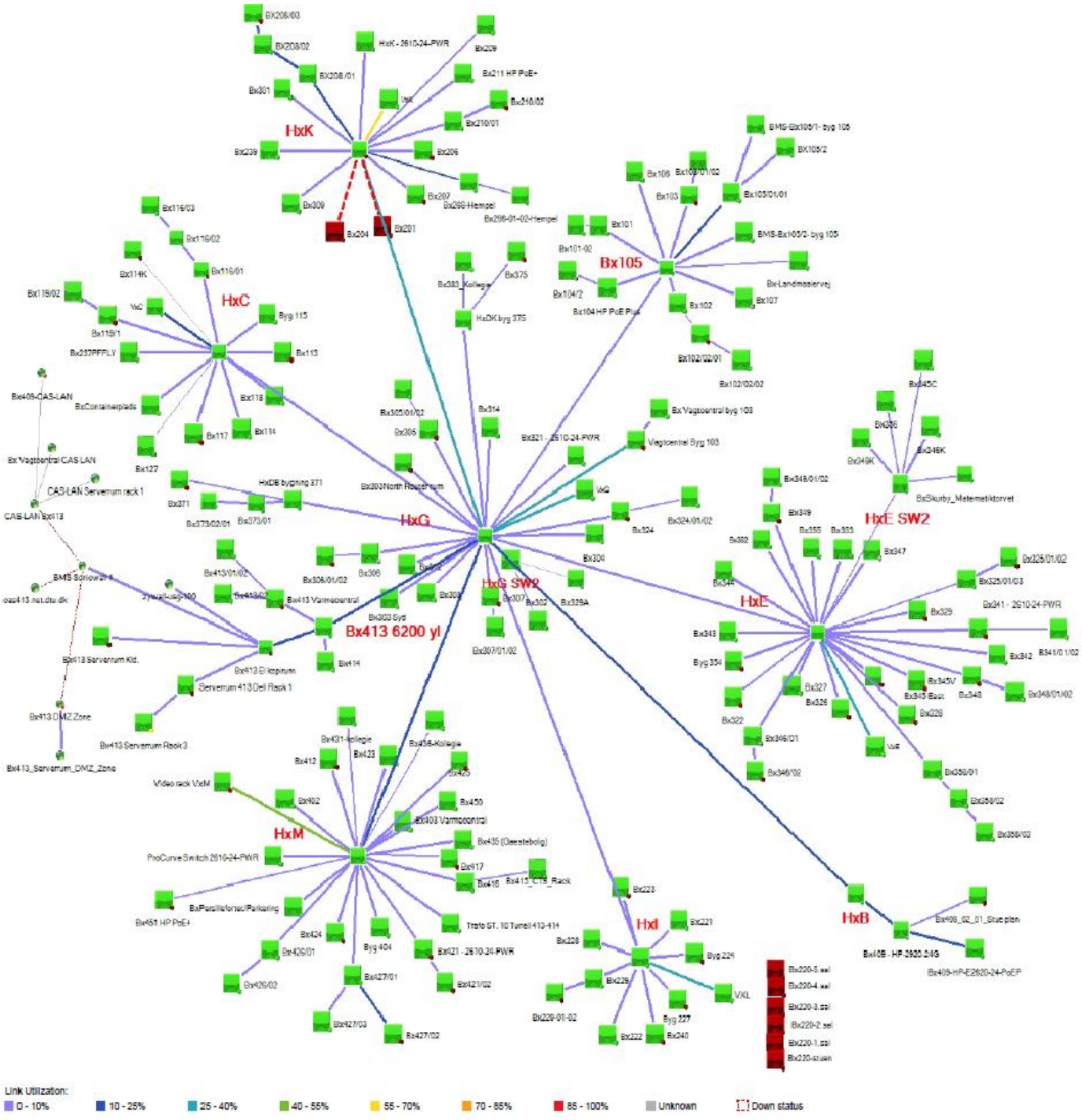
| Test on individual components or designs | Test result |
|---|---|
| Dose the Underfloor heating system save energy? | The actual idea is to replace all the old heating radiator and place with underfloor heating system. It is the smartest way of Heating and save energy. In this manner the controllers are designed, where they are able to adapt the heating. That means they are able to adapt temperature levels for heating. |
| Dose the system vast energy? | The algorithms are smart which is able to find alternative to save energy. Like the system are designed to save energy if required. Like in the holiday times the system can be placed in save mode which saves energy. The system doesn't shut down at all only placed in slower action. |
| What will happen if outdoor Temperature drop or increase? | The algorithm reacts on outdoor temperature and function in smarter way. Such take the outdoor temperature and calculate it with indoor temperature level to keep the room worm. If the outdoor temperature rise the under floor heating will shut down the system if the temperature is beyond the appropriate level. |
| Can user set up their own set point | Yes the user are able to set up their own set point (Highest flow temperature, highest return temperature, Pump stop when high outdoor temperature). |
| Dose the heating system have any automatic option? | Yes it is able to do automation function once the user has setup. Moreover it is able to adopted outdoor temperature with indoor temperature for function the heating system. |

# 4 Solution and improvements on BMS architecture

This section will deal with providing the reader understanding on how the software can be used in the network with different devices and gateways. There are some usable solutions which could be used for DTU buildings and for the current pilot project on DTU smart concept. Moreover this chapter contains the most recent BAS solutions, some of which are available on the market and some which are still under development. The provided network architecture should provide good solution for the DTU buildings where CTS Engineers are able to adopt their current network with new network. Moreover there are solutions on how CTS Engineers can adopt different type of controllers and sensors even more devices to the network. In another words these devices do support different type of protocols, which are not be able to communicate each other. From the flowing writing there is more details descriptions, which shows how these devices, can be used to solve these issues.

## *4.1 DTU BMS Architecture*

From the following picture 44.1, you can see the DTU BMS architecture which gives us an understanding of how the networks are structured. This is the current LAN architecture, where each individual building is interconnected. For instance, when we look at building bx239, which is in the HxK network, it is connected with LAN to the HxG network, which gives access to the other buildings on the same network. The networks represent communications inside DTU for each individual building, but for WAN connections there is a BMS Sonicwall firewall router which gives the access for the outside world. This means the firewall will protect the DTU network from outside attacks and network damage. These networks are controlled from a campus service (Martin), which has the user rights to look for any mistakes or unwanted access to the network. As you can see from the picture, there is only one connection between each quadrant: that means, given there are 4 different quadrants in the DTU buildings, if first quadrant building would like to connect with the third quadrant building, there is only one connection available. This will be replaced with star topology, which gives more possible connections between quadrants and with network traffics.

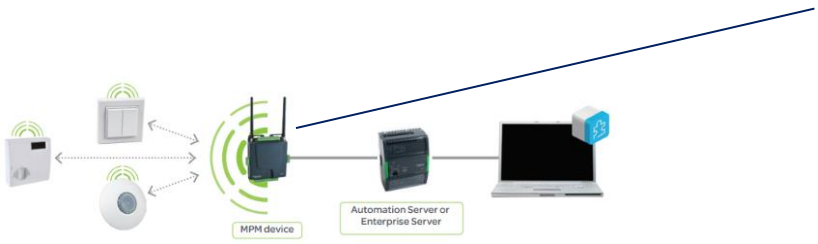



4.1 BMS Network Architecture from DTU

## *4.2 Software design and gateway option*

The StruxureWare software contains password protection, which prevents unauthorized usage unless an operator is logged on. The function's assessments are limited to the operator, to avoid complications. The operator terminal should have a limited number of users (a minimum of 3), where they have the same ID for the same server. In order to create a password, there are some password rules for creating one – for instance, it should not have the same characters as the previous password; the minimum number of characters should be not less than 8, no more than three identical repeating characters are allowed, etc. Through these password rules and the system protection, there is a much higher level of security in the software, which gives the user more security in both the software and in the individual controllers and sensors in the network.

As I have mentioned in previous chapters, there are lots of possibilities for gateways and controllers. In my case, I am focusing on using the automation servers for the controllers and sensors, and these can be connected to the BBMD devices for different network communications. There are opportunities to have wireless sensors or controllers connected to the automation/enterprise server [20]. In the following picture 4.2, you are able to see a more detailed description on the Multi-Purpose Management (MPM) device. The wireless zone manager controls wireless comports in the HVAC and has the ability to be used for wireless and wired zone control, in buildings such as DTU. The control features applies to ZigBee Pro End Device, EnOcean, and StruxuWare Building Expert, and also provides real time response to graphical and scripting programming.




4.2 Wireless access point devie

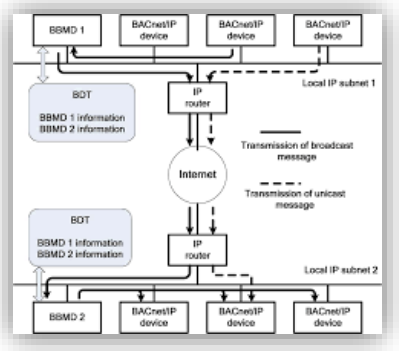
| *MPM device* | *Capabilities* |
|---|---|
| Component type | Universal network controller |
| Device application | Only for BMS |
| Network type | Ethernet and Modebus |
| Protocol type | Zigbee Pro, EnOcean, CANbus, BACnet and Ethernet |

Automation and enterprise servers are programmed in such a way as to control each individual controller and sensor. The controllers are able to manage up to seven sub-network and route BACnet messages between the high speed LAN (Ethernet 10/100MHz), point to point connection, master slave token passing (MS/TP), and Modbus LANs [21]. The building controllers are able to provide global control strategies on any objects in the system to other controllers. The BACnet controllers also have backup if any shutdown occurs. The batteries in the controllers gives the option for the BACnet server to run a temporary power option where the flash RAM can ensure data is not lost. BBMD remote communication has the function via modem to the offsite locations. Each subnet will have one BBMD for subletting (VLAN), where the packages can be transferred from one network to another. This means the BBMD is there to distribute the packets as unicast, so there are no- limitations for the BBMD device. In my case, there are several BBMDs used to connect different networks to provide communication together.

Now we'll look at the BBMD device architecture, and see how they are connected each other. The BBMD devices are responsible for interfacing the Building automation and control network to the internet through BACnet/IP protocol. This means it plays a role in maintaining a communication link between remote controllers outside the building, and field devices inside it. We will also cover the BBMD and its communication manner, and the fault tolerant mechanisms in the BACnet/IP protocol. Furthermore, we will focus on backup BBMD devices and how to improve the connectivity of the network by inheriting from the original BBMD devices, and cover possible attacks on the BACnetIP network with BBMD devices, which can be misused by the attackers.

The main purpose of implementing a BBMD device is to utilize IP router route issues with it. It is designed to maintain communication on controllers remotely and link between field devices. Before looking at the BBMD devices, we have to understand what BACnet/IP protocols are. BACnet internet protocols are a collection of one or more IP subnetworks, and each BACnet number is assigned to a device which has a B/IP address, and then transmits this address through the IP protocol [22]. For example, there might be two different networks (say, network 1 and 2), with both networks having a BACnet/IP device connected to an IP subnet, and these are connected to the BBMD. Between them is an internet which gives a connection to two networks. That means there is a B/IP network where these are interconnected through the Internet.

The operation of the BBMD uses BVLL (BACnet Virtual Link Layer). B/IP protocol defines BVLL (BACnet Virtual Link Layer)'s function as supervising the message exchange amongst BBMD and B/IP devices. When we look at the exchange on the B/IP network, the Broadcast Distribution Table (BDT) contains all the port numbers, IP address and BDM (Broadcast Distribution Mask) of BBMD. Through this option the BBDM knows whether the receiver device on the remote location network is able to use them. Moreover, the FDT (Foreign Device Table) contains the entirety of foreign devices which are temporarily registered to the IP networks. In the following figure 4.3, you are able to see some sample operations of BBMD, such as the BACnet/IP device, send messages to another BACnet/IP device which is on the other side of the network. It uses a local subnet IP to send a message to BBMD 1, which is on the same network. BBMD 1 then looks at the BDT for information to distribute, and sends the message through the Internet to BBMD 2, which sends the message to the BACnet/IP device. This means the BBMS is the main device which manages communication between the two networks. Compared to unicast messaging, it avoids BBMD communication, and sends messages straight to the other devices directly.




**4.3 BBMD operation network model**

### 4.2.1 BBMD process with NAT Router

Network Address Translation (NAT) is used to connect to the Internet, Firewall and IP routers. One advantage to using a NAT device is that it can be used for multiple hosts on a subnet to get access to the Internet. There are ways in which the BBMD can utilise a NAT router function; for example, each individual BACnet device can have several B/IP networks ports, with their own BBMD. In this manner, the B/IP network can have a connection or communication through a NAT router. Doing this can lead to some barriers, such as that at least one device which is on the same network has to have access to the global side. For this particular purpose, all the devices on the NAT router should be on different BACnet networks, where they can be exclusively addressed to use the BACnet network layer. From all other subnet locations, the NAT router should be configured to port forwarding B/IP messages to the BBMD.

The port forwardings are able to forward all directed messages to the specific port locations. In order to get foreign devices onto the NAT router, it should be registered with the BBMD to get to know a return path to the NAT router.

Let us look at one example of a B/IP internetwork which connects two remotes sites using the Internet: there are two different B/IP networks on the same side which are connected through a BBMD router. The NAT server translates the two different B/IP networks, first into a global Internet IP/Port address, and then into a private address. This allows the different networks behind the NAT server to use the same IP/port address, where other networks are connected to the two different private networks using the same IP/Port.

There can be more networks, say four different B/IP networks (2, 3 or 4) where the BACnet devices are connected, and these can be assigned to the BBMD routers and be connected to the internet routers. Behind the NAT routers would be B/IP Network 1, which is designed to get access to the internet. That means any device, such as a foreign one or BACnet, can be connected to the network which has the same B/IP network to gain communication.

### 4.2.2 Attack over BBMD

Nowadays there are a lot of technologies available which perform a lot of amazing tasks. Unfortunately there are also a lot of attackers involved in trying to harm networks or even entire systems. As such, there are potential deficits in BACnet security; for instance there attacks from outside, via the TCP/ IP, into BACnet. This can allow for an internal attack on the actual BBMD device which is placed in the BACnet. The attacker uses the BACnet/IP network to gain access to the BBMD device in the same network. The BBMD device gives all details about the technology within the network, such as HVAC, fire alarms or sensors. These can be abused by the attackers to harm the devices.

### 4.2.3 BBMD Backup in BACnet/IP Protocol

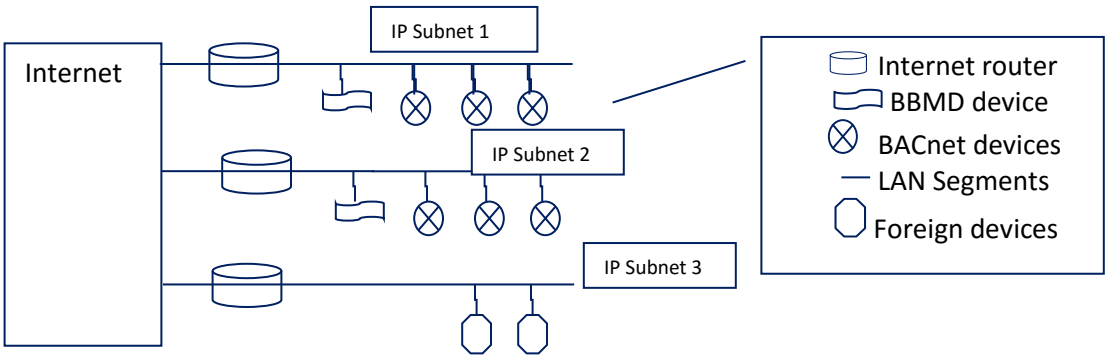
It is possible that faults in the BBMD device can cause a denial of service in the IP sub network on sending and receiving broadcast messages. In this case, each IP sub network can have backup BBMDs which can handle fault tolerance on these devices. The function of the main BBMD is to send broadcast messages continually to the backup BBMDs on the IP sub network, to maintain a connection. These backups can be used if the main BBMD fails to send a broadcast message - the individual BBMDs can act like the main BBMD. Once the main BBMD is functioning again, it will receive all lost data from the

backup BBMDs. In this manner the backup BBMDs must have the same database information as the main BBMD:

The actual real value of RetryConter;
The transmission time;
Information on backup BBMDs such as node number and the IP address;
The value of Broadcast Distribution Mask (BDM) in the present BBMD.

From the following picture you can see how BBMDs are used for different subnets and for different devices. It is possible to place a BACnet Router and use its ability to connect a non-BACnet/IP into a BACnet/IP; this allows for two different BACnet/IP networks to be created without an Internet route option.

The foreign devices have to register themselves with the BBMD device to get activity out of a B/IP network. The BBMD will have all the assigned foreign devices in a Foreign Device Table (FDT), each with a 6-octet B/IP address and 2-octet Time-to-Live value. The BBMD allows 30 seconds for a reply from the device which would like to be connected, but if it fails to reply the BBMD device will delete the foreign device from its FDT list.




Picture 4.4 BACnet network architecture how message are processed

As can be seen from the Picture 4.4 the BACnet architecture is used to broadcast BACnet messages. This architecture processes the message from one device to another device through different networks. For direct communications from one network to another network the IP address should be known, as should the UDP pots which use the B/IP addresses.

When we take the BBMD device which is on the IP subnet 1, which communicates with devices on the IP subnet 2, it has some tasks which need to be done. The BBMD on the subnet 1 has a table of all peer BBMDs, and the broadcast distribution mask which has to be sent to other BBMD devices is on the subnet 2. The receiving BBMD receives the Forwarded NPDU message and sends it to each individual device in the same network. Through these process devices, the subnets 1 and 2 are able to communicate with each other.

We will now examine how foreign devices (Workstations) communicate within the network. Differences can occur in these foreign devices, such as depending on where they are placed, such as within the same subnet or in a different subnet. These foreign devices don’t need any configuration or maintenance on BBMD or BACnet nodes. The reason for this is that they only require registration with BACnet/IP

networks to become a member. There are also possibilities for foreign devices to have the option to talk with any BACnet devices directly without any registration required. Moreover, these foreign devices might be full time or part time nodes on the network, so there is no restriction on access to the internet.

### *4.2.4 How to Network BBMD?*

Depending on the needs required, there are different varieties of topology options available to map the network between BBMDs. The communication between BBMDs is based on the way their relationships are designed in the network. The installation part of the BBMD might be a software application or physical device on the network, where you are able configure it with an IP address and subnet mask.

The star topology is the one of the solutions used to mirror IGMP topology. There are advantages and disadvantages in using a star topology; on the positive side it easily adds new BBMDs, which means no message duplication on the network. On the downside, if one of the links fails the following branches are affected. The rings configuration of BBMDs network is designed to be ring shaped and has some advantages – it's easy and quick adding BBMD devices to the existing network and minimises the number of message required between nodes. However, if the rings configuration based on one of the links break, there are effects on the rest of the link. The star topology is suitable for the B/IP network architecture as it is free of link failure, boasting perfect network structure and a simple configuration process. There are some requirements to be fulfilled, where each BBMD device must know the topology subnet comprising the network and duplication needed within the same broadcast message.

In the following writing we'll examine how to use BBMD devices on DTU buildings. There are two different quadrants present: the first quadrant applies to buildings 101 to 120, and the second quadrant applies to buildings 201 to 225. This network architecture can be extended to the rest of the quadrants at DTU. This is a BACnet based architecture where different BBMD devices are placed to facilitate communication between different networks. I have created the network with B/IP network protocol, with possible IP addresses from the following list. These networks are WAN based multiple remote sites, with BACnet being connected with intranet.

There are differences in IP addresses on private networks which do not have to be unique.
We have the option to protect the private network from both the network translation devices and the different network numbers. From the following list you are able to see different kinds of IP address which are used for the BACnet architecture:

From 10.0.0 to 10.255.255.255 have 16,777 IP address possibilities.
From 172.16.0.0 to 172.31.255.255 have around 1 million IP address possibilities.
From 192.168.0.0 to 192.168.255.255 have around 66 thousand IP address possibilities.

There are possibilities in having foreign devices on the network with a Serial Line Internet Protocol (SLIP) or Point to Point Protocol (PPP) dial-in workstation. These protocols can help if any new devices or work station are added to the network for communication.

## *4.3 Description on network architecture for DTU buildings*

When we look at the network architecture, we are able to see 6 different BBMD devices. The first two are the main BBMD devices (BBMD 1 and 2), which have communication to each individual BBMD in the entire network. In the following list you are able to see the configuration techniques on how the BACnet devices have been connected:

NAT Configuration
Internet IP 192.168.0.15
Forward 192.168.0.15: port 4708 => 10.60.0.: port 4708

BBMD1/router configuration (BACnet Router)
Global IP Address 192.168.0.15: port 4708 (This is the global B/IP address of the NAT router)

B/IP address Network1 10.60.1.: port 4708
BACnet Discovery Tool (BDT) 192.168.0.15: port 4708(Global B/IP of NAT)

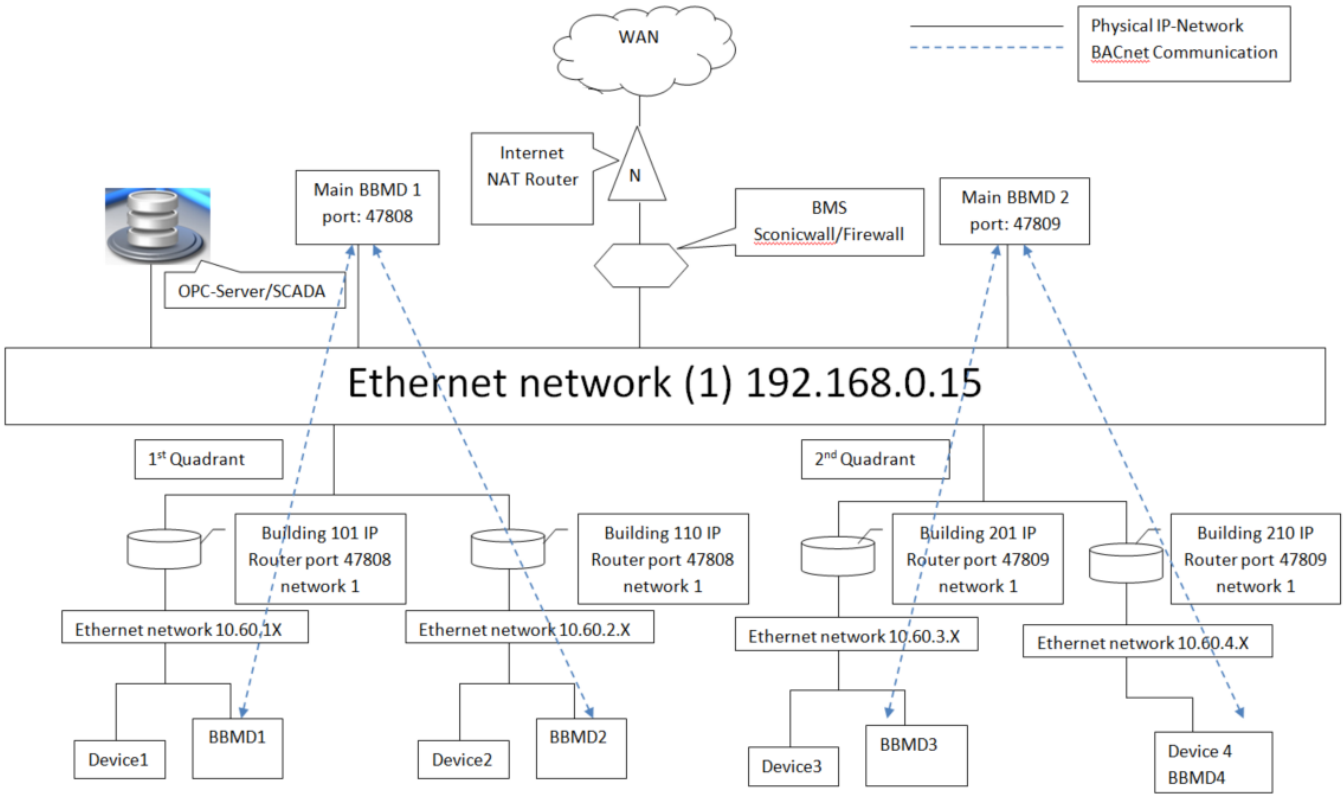
B/IP Address Network1 10.60.2.: port 4708
BACnet Discovery Tool (BDT) 192.168.0.15: port 4708(Global B/IP of NAT)

BBMD2/router configuration (BACnet Router)
Global IP Address 192.168.0.15: port 4709 (This is the global B/IP address of the NAT router)

B/IP address Network2 10.60.3.: port 4709
BACnet Discovery Tool (BDT) 192.168.0.15: port 4709(Global B/IP of NAT)

B/IP Address Network2 10.60.4.: port 4709
BACnet Discovery Tool (BDT) 192.168.0.15: port 4708(Global B/IP of NAT)

There are also different ways to design the network, such as placing NAT routers for each individual network, or adding more networks to the present network with more individual sub networks with more foreign devices to it.




## *4.4 Router configuration on BACnet*

There are differences in models and vendors for how a BACnet router can be configured, but there are some important configurations and settings needed for the routing. For instance, adding a remote field Bus to the BACnet Router should be site-level, with a unique network device object ID and MS/IP network number needed. Sometimes there are BBMD devices needed for the BACnet router for network communication.

The MS/TP MAC layer address of the BACnet routers should work perfectly with other MS/TP devices. Moreover, there are maximum sizes of BACnet application Layer Protocol Data Unit required for the devices as well. There is Max info Frames settings available on the BACnet router, which allow the transmission of MS/TP frame packets for the frame buffers in the router. Compared to Ethernet BACnet/IP, the MS/TP frame packets define a unique identifier for the connection on the router. Some user actions are needed to specify the network number on the BACnet/IP network connection. The device ID should be unique on the entire building's network for all devices, as that is the instance number for the BACnet router.

## *4.5 BACnet Architecture overview*

The main advantage with BACnet is that it provides a way to transport data through hardware and software. This means software/hardware binary input and output are used to schedule information, both event information and alarm. BACnet does not define the data structures or internal configuration of the controllers. The communication network visibility is abstracted from the implementation details

over the use of a standard object. Also, the vendors are able to decide the mapping between the underlying data and the standard objects.

When we look at the Layered protocol architecture of BACnet, we see it is founded on a warped version of the Open System Interconnection (OSI) Basic reference model. There are 4 different BACnet layers:

Physical Link layer: Includes (LonTalk, PTP,EIA -232, MS/TP, EIA -485; ISO 8802-3,ISO 8802-2). This layer is responsible for connecting the devices and provide with electro signals which convey the data.
Data Link layer
Network layer: BACnet Network layer
Application layer: BACnet Application Layer.

Let's look at the protocol layer in more detail in the BACnet. The application layer is represented in two parts: as a group of functions used to exchange the information in devices, and as a model of information contained in a building automation. The BACnet internal configuration and design is different from the vendor. To overcome this problem, BACnet defines a collection of abstract data objects in the properties which represent the various features of the software/hardware and the device operation. The advantages of these objects are that they can access and identify information without the device's internal design information. The device communication software is able to interpret requests for information about abstract objects and interpret those requests to gain data from the real data structures, which are inside the device.

The physical layers are used in BAC protocol, and provide a connection between devices and transmitting electronic signals. To work with packets and frames, the data link layer is organized to both regulate access to the medium and provide error recovery. Furthermore, the network layer is there to translate global addresses into local addresses, through one or several networks. There are differences in the network types and message sizes, such as their sequence and flow control. In BACnet's point of view, the paths are designed logically between devices, such as to eliminate the path routing algorithms. In case more networks in the BACnet internet use different MAC layers, there is a need to recognize the differences between global and local addresses.

In order to provide messages, segmentation, control, sequence and recovery, the transport layer is responsible for guaranteed end-to-end delivery. Moreover, BACnet has error recovery and end-to-end delivery provided for message timeouts and retry capabilities, which are used in process and resource and buffer management for message segments. The reason for this is that larger informed messages are returned, even if they are simple BACnet requests in the application layer, as they are based on a connectionless communication model.

To manage long dialogues between users, session layers are needed as they are capable of handling synchronization and resetting. This can help to avoid restarting and exchanging from the beginning.

The presentation layer is there to get a communication option between the users or parties from the user view point. This user view is presented as data at the application layer to a sequence of octets treated as data at the minor layer. Lastly there is the application layer, which is there to handle the function in BMS, meaning control of the HVAC system and other remote systems.

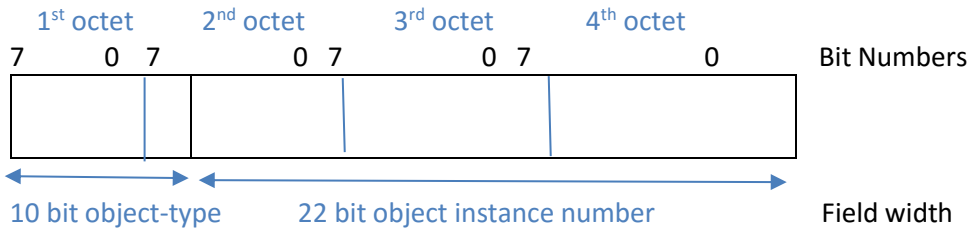
Overall, there is no need to implement all layers on an OSI model, as they are cost effective and less relevant for the current BMS devices and controllers. Also, OSI models offer adoptability on network technologies and can save costs and time.

BACnet defines 18 different standard object-types, which are:

| | | |
|---|---|---|
| Binary input | - | Loop |
| Binary Output | - | Multi state Input |
| Binary Value | - | Multi state Output |
| Analog Input | - | Event Enrollment |
| Analog Output | - | File |
| Analog Value | - | Group |
| Device | - | Schedule |
| Calendar | - | Notification |
| Command | - | Program |

Now let us look at the objects more closely:
**Command:** Is responsible for command procedure for multi action in several devices.
**Calendar:** Is responsible for the scheduled operations of the mechanical equipment, such as which calendars will dictate what days the building is not occupied, or holidays. These will be used to navigate the devices, such as heating or ventilation, on standby mode or saving mode.
**Loops:** Can be used to characterize any feedback control loop, which is a mixture of integral or device control.

**Notification class:** This function helps event or alarm notifications send to multiple devices.
**Event Enrollment:** This is able to describe events and alarms, and define who is able to handle notifications when they occur. Compared to Loop, Binary output and others, it contains optional properties to support essential event reporting capability, and does not need to use Event Enrollment objects. Each BACnet dives have one Device object and an Identifier retrieved from the object that exclusively identifies each with a single device. The device object has a special necessity that requires the object identifier be exclusive over the whole BACnet internetwork. The representation of the object identifier is based on a data structure that involves the octets (8 bit bytes) which you are able to see from the figure:




The instance number field classifies the particular object of the specified type as being referenced. The object type field carries a counted value that matches to a particular object type. The vendors are able to extent the object type for their use and also can be used to identify in a good manner. Looking at the vendor extension in more detail, the BACnet object can be also called ‘object name’, and in a character string it can be used to identify an object. As it has a fixed size, the object identifiers work to identify a

particular object. BACnet properties objects are connected with a conformance code which will specify if the property is elective (0), mandatory to be read, and using existing BACnet service (R). As noted, BACnet architectures are based on four different types of OSI layers (data link, physical, application, and network). The application and network layers are the standard layers which are defined in the BACnet standard. Moreover, data link and physical layers have seven different options provided from the BACnet - these are:

Option 1: Logical link control (LLC) protocol ISO 882-2 (unacknowledged connectionless service) combined with 8802-3 (international standard version "Ethernet" protocol) medium access control (MAC) and physical layer protocol.
Option 2: ISO 8802-2 type 1 protocol with ARCNET (ATA 979.1).
Option 3: MS/TP protocol created for BMS as part of the BACnet standard.
Option 4: Point to Point protocol, used for dial up serial and hardwired mechanisms and synchronous interconnection.
Option 5: Is based on LonTalk protocol.
Option 6: BACnet/IP manages to use BACnet devices to use UDP and IP for standard internet protocol as a virtual data link layer.
Option 7: Used for the wireless data link to ZigBee technologies and provide a master and slave MAC destination token passing with high speed contention MAC.

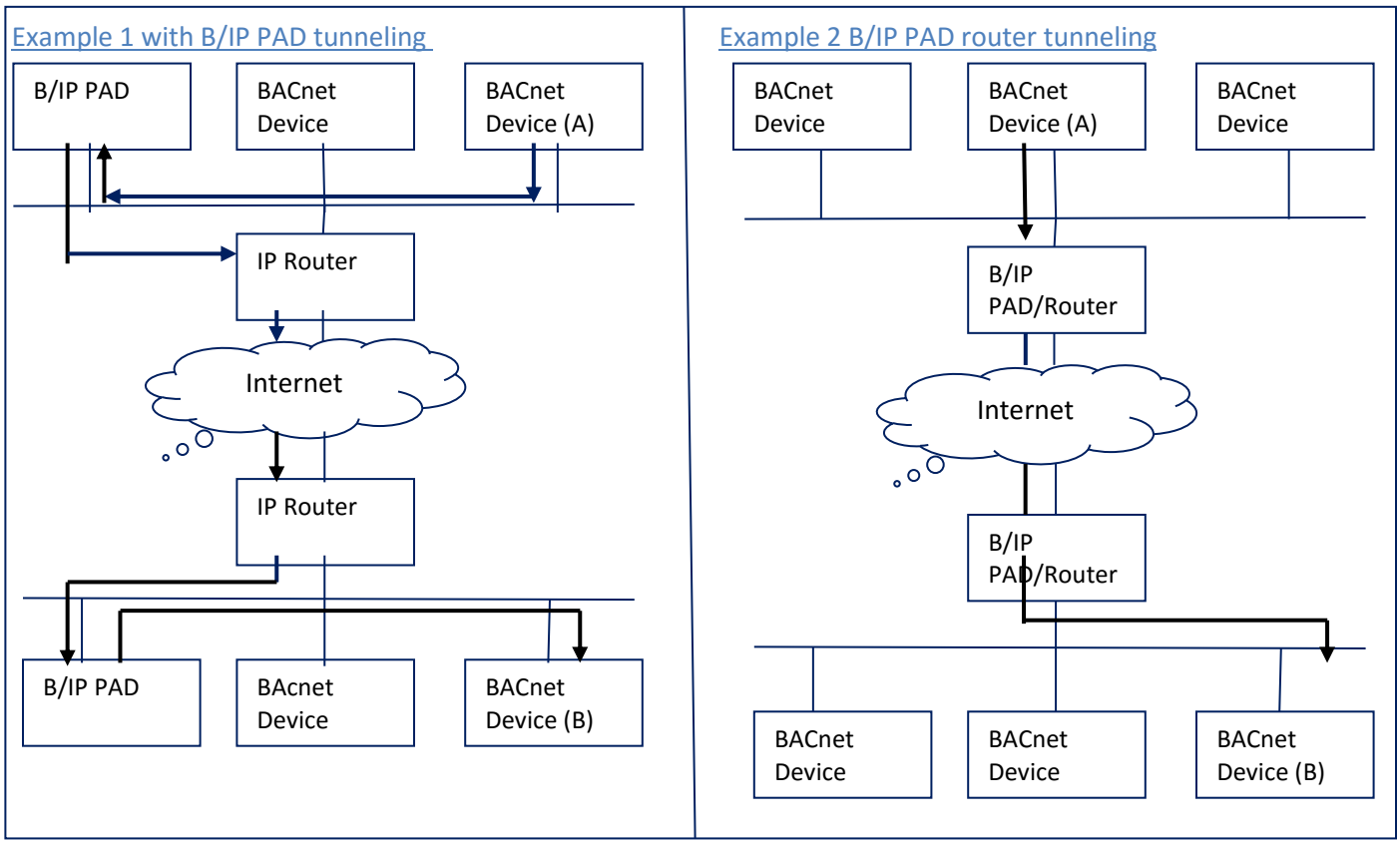
There are requirements in the BACnet network on what layers are required for long distance communication. In this manner, there are communications through the telephone networks, across internet systems, with BACnet/IP. It is dependent on the devices what technologies they are using, and also varies by company.

## *4.6 How to map non-BACnet networks in to BACnet network*

Let us look at how to map non-BACnet networks into BACnet routers. The gateway plays a big role with mapping in the network - the router uses the network connection to gain gateway function to non-BACnet networks. Non-BACnet networks are characterized by their use of the message structures and medium access control techniques, which is enclosed as standard. The procedure to map BACnet to non-BACnet networks is based on the routing table which allows using the BACnet network protocol control information. In the NPCI is a unique two-octet network number assigned for each device, which are then assigned in non-BACnet networks which may not have the actual octets used to address the devices. For that reason the router gateway (which is either in the BACnet or non-BACnet) is designed to translate for the communication.

Now let us look at using BACnet, which is designed by the Defense Advanced Research Project Agency (DARPA) of the Department of Defense (DOD). These are Internet Protocol suites whose methods encapsulate (and in turn decapsulate) BACnet LSDUs, and transmit through an internet using the IP routes as a means of tunneling. For example, the LAN can be configured with BACnet packets, which are differentiated from the IP packets in the LASP contained in the LLC header. The packets also appear twice on the network layer, each with an IP message and BACnet message. To implement the IP routing procedure the BACnet IP PADs can be used to perform the BACnet encapsulation/decapsulation. For example, BACnet device A sends a message to the B/IP PAD, which is on the same network as those using an IP router to get through the internet. From the other side, different IP routers get the message, which then pass to the B/IP PAD to gain access to the B BACnet device which is on the same network. This is the

process known as tunneling with B/IP PAD. In the following diagram you are able to see two examples which show the B/IP PAD and B/PAD routers:



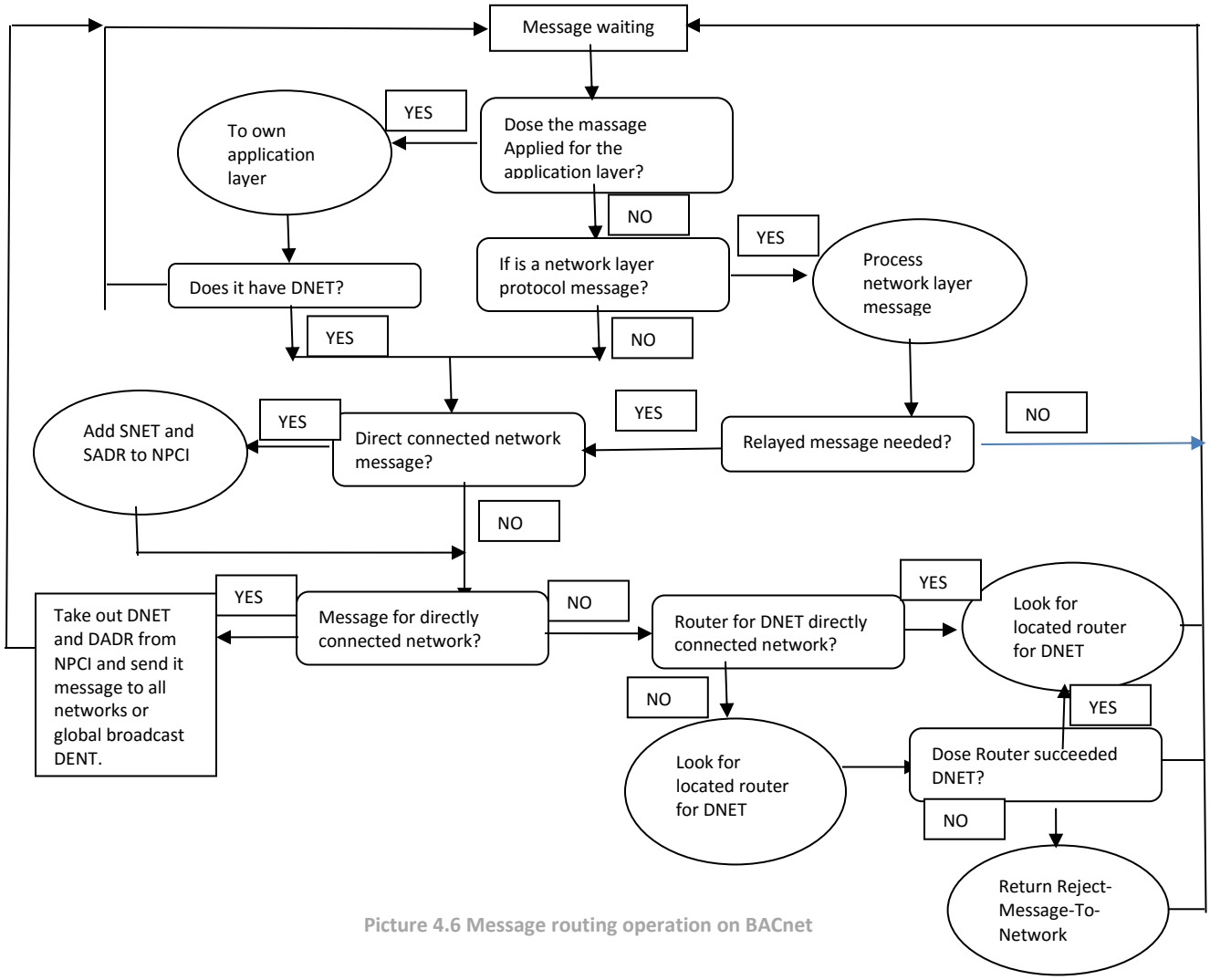

Picture 4.5 Router tunneling with BBMDs

This BACnet with Internetwork Packet Exchange (IPX) Protocol was developed by the Novell Corporation and is known as Internet Datagram Protocol (IPX). These protocol layers are based on the Xerox Network Service (XNS), which uses the Packet Exchange Protocol (PEP). Looking at how the IPX works, the B/IPX PAD device is able to implement both BACnet network layers as standard and IPX layers. The B/IPX PAD device will look for NPCI to see if a DNET network number is included, and then it will consult an internal table to map the BACnet network number. If any entries found in the B/IP PAD encapsulate, the LSSU portion of the BACnet message in an IPX tunnel packets which perform MAC-layer and destination network number. These can be sent from the B/IPX PAD datagram which contains the tunnel packet and sends it to the local IPX router for further use.

## *4.7 Communication perspective on BACnet routers.*

From the BACnet architecture point of view there are different BACnet routers available which are interconnected with different BACnet network. The BACnet router uses the BACnet network layer protocol message to function the routing table also is able to connect multiple network types. The routers are designed to get BACnet/IP or BACnet/Ethernet or BACnet MS/TP.

From the following Picture you are able to see flow chart of router operation which performing the routing task.




Picture 4.6 Message routing operation on BACnet

Abbreviation for the standards: DNET (2-octet ultimate destination network number), DADR ultimate destination MAC layer address, NPIC (Network protocol control information).

In the following writing you are able read about the router operation of BACnet. The Router has to be defined with the Mac address for the network port connection. To look at whether the association network is able to received traffic the “reachability status” should be placed in the network. The Start-up Procedures is there to look at the each port on I-Am-Router-To-Network message containing the

network numbers of each accessible network. Also the startup Procedures enables the routers to build the entries in the routing table for the network number which has the message.

There are different types of routing message available such:
Who-Is-Router-To-Network: Is generated by non-routing BACnet node or with BACnet router. The router with the message Who-Is-To-Network message with network number, will search for routing table to find the network number contained in the message. IF the network number is founded in its table but it the port is not reachable from the Who-is-Router-To-Network was received, then the router will use I-Am-Router-To-Network message which has the specific network number and send it to the node where it can be generated by the broadcast MAC address, where it allowing other nodes on the same network to take advantage of the routing information.
Reject-Message-To-Network: It indicates the reason for the rejection in the network and directed to the node which originate the message being rejected. There could be some reasons why the message was rejected such the router is not directly connected to DNET and cannot find a router to DNET. Also when the router was busy this couldn't accept the message at the present time.
Router-Available-To-Network: Is there to display the message to the network that the routers are now reachable and able to receive traffic form the DENTs.
Point-To-Point-Half-Routers: These routers are different from normal router with the synchronization and establishment point of view. Let's think about two different half routers which are linked with Point-To-Point connection which establish together form a single router. More over the both half routers should be updated their routing tables to update routing information stored by the other half router. The BACnet has to define five different network layer message types to establish the routing learning functions of a PTP half-Router. I-Could-Be-Router-To-Network message presents the establishment that the half router has the ability to connect to the requested network but doesn't have the actual connection. In this manner the Establish-Connection-To-The-Network message gives the establishment to be connected. The Disconnect-Connection-To-Network message makes the active connection to be disconnected. Routing table initializations are performed using the Initialize-Routing-Table-ACK message and Initialize-Routing-Table.

## *4.8 BACnet Interoperability Building Blocks (BIBBs)*

To know about the BIBBs we should first look at the interoperability areas first. There are 5 different interoperability arias available such as scheduling, alarm and event management, trending, device and network management and data sharing. Also we have to make sure what services are needed to ensure interoperability by looking at the list of services it is not clear what type of device initiates a request and what type of device must responds. A Smart sensors will only supply minimum number of services compared to a building Controllers. The question would be what is that minimum? It became a parent that a different method is needed to identify what services must be supported for different classes of devices. The solution is the BIBBs services such as (createObject, GetAlarmSummary, who-Has etc). In this manner BIBBs clarifies what is the service request and what is the service response. BIBBs are grouped into categories that are more meaningful for building automation applications (Data sharing (DS), Trending (T), Scheduling (ECHED), Alarm and Event Management (AE), Device and Network Management (DM)). BACnet device profiles are then defined each based on minimum level on required BIBBs. When talking about BIBBs client and server relationship is important. For example an operating workstation is requesting data from a controller in the jargon of BBBs an A device is called the client which has (ReadProperty-A (DS-RP-A)) and used the data. While the B device called Server provides the data (ReadProperty-B (DS-RP-B)) that means in both devices the Read property are used in both uses

BIBBs. The DS indicates that the BIBBs are from the data sharing groups and these groups are established to clarify the device functionality. When discovering a device the process is bit different then operator workstations sends a Who-Is message to find particular device or all of the devices on the network. The controller response with an I-am indication that is exists and the I-am service is special because it is the only services that can be initiated by a service without a corresponding who-is command. A Server is allowed to announce itself on power up without invitation of the client. BIBBs were develop to classify BACnet devices and these are structured as Device profiles (Building Controller (B-BC), Application Specific Controller (B-ASC), Smart Sensor (SS) etc). From the following Picture you are able to see the Device Profile.

| | B-OWS | B-BC | B-AAC | B-ASC | B-SA | B-SS |
|---|---|---|---|---|---|---|
| **Data Sharing** | DS-RP-A,B | DS-RP-A,B | DS-RP-B | DS-RP-B | DS-RP-B | DS-RP-B |
| | DS-RPM-A | DS-RPM-A,B | DS-RPM- B | DS-WP-B | DS-WP-B | |
| | DS-WP-A | DS-WP-A,B | DS-WP-B | | | |
| | DS-WPM-A | DS-WPM-B | DS-WPM-B | | | |
| | | DS-COVU-A,B | | | | |
| **Alarm, Event** | AE-N-A | AE-N-B | AE-N-B | | | |
| **Management** | AE-ACK-A | AE-ACK-B | AE-ACK-B | | | |
| | AE-INFO-A | AE-INFO-B | AE-INFO-B | | | |
| | AE-ESUM-A | AE-ESUM-B | | | | |
| **Scheduling** | SCHED-A | SCHED-E_B | SCHED-I-B | | | |
| **Trending** | T-VMT-A | T-VMT-I-B | | | | |
| | T-ATR-A | T-ATR-B | | | | |
| **Device &** | DM-DDB-A,B | DM-DDB-A,B | DM-DDB-B | DM-DDB-B | DM-DDB-B[1] | DM-DDB-B[1] |
| **Network** | DM-DDB-B | DM-DDB-B | DM-DOB-B | DM-DOB-B | DM-DOB-B[1] | DM-DOB-B[1] |
| **Management** | DM-DCC-A | DM-DCC-B | DM-DCC-B | DM-DCC-B | | |
| | DM-TS-A | DM-TS-B or DM-UTC-B | DM-TS-B or DM-UTC-B | | | |
| | DM-UTC-A | | | | | |
| | DM-RD-A | DM-RD-B | DM-RD-B | | | |
| | DM-BR-A | DM-BR-B | | | | |
| | NM-CE-A | NM-CE-A | | | | |

Picture 3.3 Device profiles for BIBBs

## *4.9 BACnet Functional levels*

When we look at the functional level of the BACnet it has four different levels. All these levels so have different purposes. First the management level: has the statistical level where servers and workstation are found to manage and monitor the individual devices in the network. Second the Integration level or building level: where controllers are found for managing different third-party building automation networks. Third is the field or floor level: where the field and controllers and sensors are active to optimize the protocol at the field level for better system communication performance. Mange the integration on other networks properties such as Ethernet, MS/TP or ARCnet for the routing gateway.

## *4.10 Network security architecture on BACnet*

The network security architecture for BACnet is important for users as they are dealing with expensive devices. The architecture focuses on knowing about data confidentiality, integrity and operator authentication per entry. It also looks at the router configuration on the BACnet router.

## *4.11 General overview*

There is a lot of network security architecture in BACnet, such as device authentication, data hiding and user authentication. In this manner the BACnet should be able to allow these constraints in these ways:

- Device types (BBMDs, routes, Clients).
- Message types (unicast and broadcast).
- Media types (MS/TP, BACnet/IP, and Modbus).
- Message layer (application, BVLL, network).

These network securities are extended with the BACnet standard for security messages and with other security standards, such as with IPsec, which collaborates on a TCP/IP network and doesn't have to

follow the above requests. But, the above architecture does have the greatest security practices of the standards. However, when we look at security layer functionality, it appears within BACnet as a layer message but there is no actual security layer. In order to share keys, the model is based in the shared key, which allows the user and device to have a message shared signature key, which further allows for actual communication between two parties. Furthermore, the signature keys provide encrypted data hiding for secure payload. From BACnet's security point of view, the key are at all times distributed as key pairs, such as a signature and encryption key. There are 6 different key pairs available (Distribution, Installation, Device Master, general network access, application specific and user authenticated).

### *4.11.1 Secure message on BACnet*

By creating a new Network Protocol Data Unit (NPDU) message type, it will create security on the network layer. In order to do this, plain BACnet messages are secured by placing the NSDU portion into the payload of a security-Payload message. Also, the basic security can be placed by a BACnet message, with a keyed hash message authentication algorithm that marks the message with the source and destination device instances, a message ID and a timestamp [23]. The message ID is able to solve issues in the BACnet message, such as detect the replay of the message and the security response. Compared to timestamps, they are used for preventing message replies and as a source of variability in the message content - repeated messages in content do not generate the same signature.

To achieve a higher level of security in the BACnet, the message in the BACnet should be encrypted in a way where the content cannot be viewed or managed without a suitable key. The sender and the receiver should have the same key to be able to read or write a message.

### *4.11.2 User authentication*

There are multiple BACnet methods available for user authentication, but only one method is currently defined. This is Proxied user authentication, based on software performance and site policies. This enables the client to trust perform user authentication. Some clients don't, however, support security keys that are provided, which leads to untrusted performance of the user authentication. That means, with the right user attention key, the user is able to perform actions, and different clients who look for access to the network will not have trusted access. For that reason, they are given a general network access key to gain trusted and secure access to the network.

### *4.11.3 Security on Device Level*

There are three different types of trusted networks: encrypted, plain, and signed. When we look at the devices, they don't reside on trusted networks - they are placed on non-trusted networks and based on end to end secure communication for security. In this manner, the BACnet devices are configured in a secured way to send and receive messages. When we look at the devices which do not support BACnet, security messages have the option to reside in plain–no-trusted or plain trusted networks. Moreover, secured dives can be used as well on the same network, as they should be set to plain from the base-Device-security-policy.

### *4.11.4 Attacks and Limitation on Network*

Communication between peer devices requires both the proper keys and a device instance number. The reason for this is there can be attacks on destination, and thus the source address information (DNET, DADR and SNET) needs to be changed. Options to address this include gaining access to the secured

device and changing the MAC address switch, which changes the IP address, or adding NAT devices physically, since attacks can also be physically incurred: by moving or replacing the devices in the system, or by altering the wiring technologies, which can cause damage to the network. In order to derive the instance number, the secured device should not allow any changes to the addressing information from any physical switches, meaning that the device instance number should be able to change via secured communications. Moreover, deriving an instance number should be a secure process from the identifier source or destination of a message.

### *4.11.5 BACnet/IP Attacks*

Let's now look at the vulnerabilities which can occur in the BACnet/IP standard. When we look at the package terms in particular, we see there can be non-compliant and compliant traffic, where compliant traffic accomplishes the requirements of the standard and the non-compliant does not. An example of this might be misshapen packages, such as malicious packets, which are used to exploit a thread. When looking at the Who-Is request, a standard complication message can be used by the attackers to gain connection with the network, in such a way to send NPDUs containing application specific APDU messages to investigate the network. The idea is to make the device understand service-related data contained in the payload, making sure to send requests to gain access to the device's load, e.g. HVAC or alarm. In this way, the attacker instigates network mapping to get access to the system. A flooding attack is also possible by malforming the packets in such a way as to get one incorrect bit. The attacker tries to break the device by sending different packets more times than is normal. Through this attack, the dives would not be able to function properly and cause a denial-of-service, which troubles the entire network system.

Vulnerable protocol designs can affect the behavior of devices during the communication procedure. Traffic redirection attacks mean that the attacker creates a route direction where it can gain access to confidential monitoring data, such as in the room HVAC controller.

### *4.11.6 Reconnaissance/device access Attacks*

This is a serious type of action, as the attackers are able to gain access to the network and start collecting or sniffing data without the user's permission. The attackers are able to gain access to the network and steal data for further attacks and damages to the network. This type of device access attack is much more complicated than usual; if the attackers are able to gain access to the devices without the user's knowledge, it can cause serious damage, such as to the manipulation routing table service. The attackers are able to change the devices in ways which make them do not as they are supposed to. This can include denial of the actual service that the device provides or is designed to do.

### *4.11.7 Security on shared key and layer*

In talking about the security on layer, we mean its functionality on the stack as a set of network layer messages. There is no actual security layer provided, but instead it is separated to different layers. BACnet does provide some a key option which has influence on the security model, through use of messages to signature and shared keys. These keys are the main security for the BACnet device, where they are used to hide security data through an encryption key. Looking at the key in-depth, the BACnet security has two different key pairs: one part is an encryption key, and the other is a signature key. Furthermore, there are six different types of key pairs available:

- User- Authentication key: designed for client devices which can be used to authenticate a user's identity for devices which do not have a user interface. The keys are also used for the server to restrict an operation on identity of an authenticated user.
- General-Network-Access key: applied to broadcast network layer messages for encrypting tunnels that are not trusted to authenticate a user. This means the BACnet network has been given a general-Network-Access key pair to have communication on the BACnet network. These keys might have some issues with authentication by the source which can lead to denial from the servers for restricted access.
- Application-Specific key: is designed to create security limitations on application areas, like HVAC and access control. There are some devices which have application-specific keys for sharing a particular application, and can be limited to have secure communication. There are also options to avoid time synchronization or network configuration with a general-network –access key.
- The Device-Maser key: this focuses on distributing the distribution key, and also has the honour of being the securest key form out of all key types. The main specialty of the key is that it is unique for every device, and its use on wires are limited.
- Distribution key: As the name suggests it is there to distribute other keys, such as User-Authenticated, general-network-access and application-specific keys, which can change over time.
- Installation key: Is temporarily distributed to a small set of devices and requires configuration for the BACnet devices. The key is able to provide temporary access for a specific controller, through a configuration tool, to the BACnet network. There might be a need for multiple installation keys to be in use by different devices at the same time, so the different configuration tools can use different installation keys if required.

### *4.11.8 BACnet network security*

BACnet securities are able to adopt end-to-end and secure network security. The purpose of the secure network is to provide security policy for the configuration of all the devices on the network. The devices have a Base_Device_Security_Policy property, which is based on Network_Access_Security_Policies which have the minimum level of security for receiving and sending messages. There are minimum security policies on controlled levels: I-Am-Router-To-Network, Router-Busy-To-Network, Who-Is, and I-Am. Moreover, the routers on the enabled security contain a network policy table for the local objects. A securely contained device should provide a more secure policy to guide end to end communication. The end to end security is there to communicate devices which are located on the non-trusted network to trusted networks. There are some limitations on device security policy; for instance devices that do not have encryption support should be encryption-trusted, and if any cabled devices are in the network, the local policy for the network should be plain trusted.

Devices on the trusted network are trusted either inherently, or by all communications being secured by the protocol – if the devices are essentially trusted the access must be controlled without allowing a means of physical access. In contrast to a non-trusted network, the accesses to the network is not regulated, which can cause non-trusted messages to exchange on the network. The secure BACnet routers are able to be configured to route non-trusted network messages to trusted network messages.

## *4.12 Security thread on BMS and on different standards*

As we know there are two different hierarchical models available on communication networks, which are backbone and control levels. The backbone level provides interconnection for foreign networks (eg. SCADA, internet) and multiple control subnet work. The control level is there to connect each individual device to the performing control tasks. Protection on BMS is a challenge as they have to look at both the backbone and control level –there are possibilities that attackers are able to gain access to the backbone and control levels to manipulate or take control of the system. In this manner there are possibilities to protect the network via the IT world, but these are common security mechanisms which lack network bandwidth and can be individually attacked through the gateway.

There also exists different standards, like LonTalk/LonWork and KNX/EIB. When we look at KNX/EIB, there isn't any guarantees regarding data integrity or data confidentiality, meaning it is only able to provide a basic access control scheme, such as a clear text password. Moreover the KNX and EIB are not able to provide support in distributing and generating keys in a secure manner.

Looking at LonWaks and LonTalk, they are able to provide an authentication mechanism on verifying the identity of the sender, data freshness, and data integrity. But there are some issues on disclosure of confidentiality, as they cannot be avoided as they are transmitted in clear text. There are also restrictions on multicast and uncast protocols, as if any unacknowledged transmissions occur the identity of the sender cannot be verified. From this point of view LonWorks and KNX/EIB are not suitable for the BMS security subsystem. While they are not able to provide effective protection against the security threads, the security on BACnet is still generally more advanced, as can be seen in previous writings. The cryptograph should be looked at in with Advanced Encryption Standard and the protocols as well.

## *4.13 Similar control system compared to Struxurware*

There is similar supervisory level software available such as StruxurWare which do have mostly same functionalities but do vary in different functions. Such the StruxurWare software is focused on to develop automation saver from supervisory level to control level.

The SCADA control system is used for controlling ventilation, cooling, power distribution etc. It is able to control complex systems of physics experiments, or in-house development. It is not a full control system as the name implies, focusing rather on a supervisory level. SCADA stands for Supervisory Control and Data Acquisition, and has part control of a system focusing on the supervisory level. It is a software package which focuses on hardware-based control such as PLC or other commercial hardware modules. The purpose of this system is not only for industrial processes such as power generation or steel making, but also for some experimental facilities. The systems are capable of handling thousands of I/O channels and further developments. When we look at a SCADA environment, it is based on DOS, UNIX and VMS, and more recently moved to NT.

When we look at the common features of its Hardware Architecture it has two basic layers: a 'data server layer' and a 'client layer'. The difference between them is that a data server layer is able to handle or manage the process of the data control activities, and the client layer is capable of supplying machine interaction. There are controllers, such as a PLC, which are connected to the data server via network or directly. The data servers are connected between servers and clients through an Ethernet LAN to allow communication with each other. When we look at the hardware architecture, the Ethernet LAN's main communication points offer connection between Client and Data servers. The Data servers are then

connected to the controllers depending on the network structure. The Software based architecture can multi-task on real-time database locations between different servers. They are responsible for handling processes such as alarm checking, calculation, polling controllers etc.

### *4.13.1 SCADA Communication*

There are different means of communication available in SCADA. Looking first at the Access to device, it provides access to the server, polling data from controllers such as data meters at a user defined polling rate. The polling rate is based on different parameters from the controller to the server. The parameter's process time stamping is achieved in the controller and taken over by the data server. Also, some of the drivers are based on third party products, such as application cards, which have additional costs for them. The advantages of data servers are that they support multiple communication protocols, based on slots for interface cards. When we look at the server to server and server to client communication, it is generally on event to driven basics and TCP/IP protocols.

### *4.13.2 Dealing with interfacing*

There are developments within the standard for SCADA to access the devices through an OPC client. There are a lack of devices and controllers which use OPC server software, meaning that there are some potential pitfalls regarding compatibility issues which should be tackled. Some of these developments on the OPC are being assessed by the CERN It-Co group. They have developed a system known as open data base connectivity (ODBC), using the archive and log for the interface. The API supports C, C++ and Visual basic for developments in accessing the data in the log and archive. The API is not always capable of accessing the actual device internal features, such as reporting or alarm handling. This is capable of providing dynamic data exchange in a way to visualize the data dynamically, in an Excel spreadsheet or by Object linking and embedding.

The products also feature a built-in redundancy on software at the server level, which prevents the user from gaining access to the software, as it is not designed for this purpose.

### *4.13.3 SCADA software functionality*

One of the software's functionalities includes access control, which allows a group of users to allocate the read and write access privilege to the system. This means the users are able to read and write to the product which is monitoring, say, a heating system.

Trending for products is always available for the software, derived in different ways. The software is mostly based in multi-tasking within a real-time database, which is based on several servers. However, the user is able to gain access to different servers to work on or design, such as polling loggings, controllers or alarm checking, and so on. Through this option the user is able to control and design the system to suit their own purpose.

When we look at the SCADA software architecture there are different sections which are responsible for different purposes, such as the SCADA client which is used for alarm and logs display. This function helps garner the user's attention if the controller loses connection between the control units or someone harms the system, etc. Moreover through the SCADA the user is able to get third-party applications to work with the system. On the SCADA server side, it offers a wide number of functionalities, such as an RT and event manager to handle alarms, log, archive etc, which can be diverted through ODBC to a private

application or Excel to work on it. There are also options to control and program via programming logic controls, which can be used for industrial based control.

When we look at the SCADA architecture, we see there is one computer system (Control Centre) which is connected via the main hub (Ethernet board). The PLCs are then connected to the Ethernet board, and this is then connected to the computer system. This means these three devices are connected to read IP addresses for communication. The PLC's devices are connected to several field instruments, such as temperature readers, scanners or sensors, which can be digital or analog. This means the field devices are connected to the PLCs, and the PLCs are connected to Computers via communication network devices. Through the SCADA software from the computer, the user is able to control the field instruments, such as a sensor or heater.

Looking at an example of a SCADA architect, we use a Pump controller, which is controlled via a PLC's controller. PLCs can also control other devices, such as a tank containing hot water also boasting a level sensor connected to the PLC. Thus, different PLCs control different functions, such as the level of the plumbing or the speed of the pump. The PLCs are connected via Ethernet or Modbus to the computers (Control Centre) to allow for supervisory control.

### *4.13.4 SCADA vulnerabilities and challenges*

The SCADA system aims to offer good performance and useful features for the user. But there are some issues that have cropped up over time, and the automation industry has moved on from SCADA communication protocol to an open international standard. That means potential attackers are able to get an easy access to a depth information about the SCADA network. Furthermore there are a number of security issues in SCADA networks where COST hardware and software can be created to operate in the SCADA network. These can be used by attackers to control the devices.

As SCADA protocols doesn't maintain or support cryptography, sniffing communication on the network is entirely possible. If an attacker manages to gain access to the network, they can acquire all the data and control commands. This gives the attackers a free ride with the network to send false messages to control the devices. Through this access, the system can be misused in a way where the devices can be shut down or altered to not perform as they should.

With these issues regarding access control in mind, the SCADA system should be improved. Access to the network should be difficult for attackers. Even if attackers managed to get access to the SCADA network, the system should be able to detect and take action. But the prevalence of these issues is exacerbated in that they are connected to the outside via gateway or with a corporate network. This is problematic as a lot of gateways provide protocol compatibility between the SCADA networks, but do not have security features for it. In this manner there should be a gateway which provides security mechanisms to make sure the confidentiality, integrity and availability on data is maintained.

There could be proper authentication required to allow access to the controls in a manner which login accounts and authorized users have to be utilized, though even logging these attacks can be circumnavigated by attackers attempting to gain network access by sending phishing mail to the users. Through these tricks, people easily fall victim. For this matter, there are smartcard based authentications to get access control to SCADA networks; the smartcard is able to securely save passwords and improvements on key management.

There are also some known issues where SCADA expert versions incorrectly handle web requests, which causes them to throw exceptions. These affect the server machine to make it inoperable, and can leave the user confused as to whether the server machine has been hacked or is broken.

### *4.13.5 Intrusion detection and firewalls systems*

The main purpose of the firewall is to block unauthorized traffic to the network and prevent direct connection from the outside internet to the local SCADA system. This means the firewall is able to filter only traffic to positive protocols. For example, if the SCADA system is designed for Modbus, it can be set up to perform only for this purpose. Moreover, the firewall is able to monitor activities on authorized users or entries in the network. It is able to control the misuse of unauthorized permissions and access for specific services in the SCADA network. A system similar to a firewall in protecting a network is the Intrusion Detection System (IDS), which isn't without its issues – it is more complicated to develop and unable to monitor suspicious behaviors in the SCADA protocols.

Server-to-server and server-client communications works on an event driven basis and use a TCP/IP protocol. This means the client application subscribes to a parameter which is owned by a particular server application. When we look at server-based access, it polls the controllers to the server level for a user defined request, as it pertains to the request level. The data servers poll the requested parameter from the controller and communicate to support unsolicited data transfer. The product's communications of the drivers are used for the PLCs and Modbus, and products which are based on third party products. When we look at the communication protocol based on a single server, it is able to communicate on multiple protocols.

## *4.14 What is OPC*

Why do we need Open Platform Communications (OPC) technology and what uses does it have? As it is an application, it has its own driver for information exchange of industrial communications, particularly on devices between machine-to-machine and machine-to-system. A conversion of Information Technology and Operational Technology can be used with any software, such as Microsoft, Linux, and Mac. As our data driven world continues, real time communication is needed between people, systems and technology. These help the manufacturers to produce products and save time. But years ago there were cases when automation and supporting enterprise systems couldn't talk to each other without expensive custom solutions. Custom solution means there are human actions needed to fix any faults or other things which cost the company lot money.

Integrating a driver's prior technology required vendors to develop numerous communication drivers or repair existing ones in a manner that was cost effective for everyone. The 1996 OPC foundation (which maintained open connectivity via an open standard) developed interoperability for freedom of choice. For the first time, the vendors could use the OPC to build a best of breed system, where generic OPC clients like HMI SCADAs from one vendor could easily consume data from any of the OPC foundation member's servers. This meant that the industries or users were able to link communication between applications, devices and controllers.

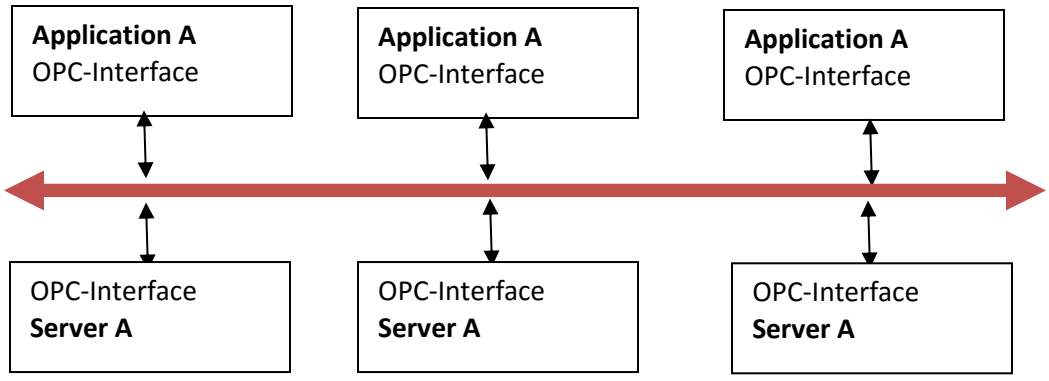
OPCs based on Client/Server technology, such as the client, make a read/write request to an OPC Server, which then translates items to a device protocol-specific request that the underlined machinery

understands. As an example of this, think of a client as a customer in a restaurant. He comes in and selects what he wants from the menu and places his order with the Server. The Server then takes the order to the chef in the kitchen, who prepares the meal and the Server delivers the meal to the customer. Similarly, an OPC Client can make request to the OPC Server, such as asking what the value of 1010 is - the server polls the value from the device and then sends it to the Client. Some of the core standardized specifications come up with OPC data access specification, which provides real-time data access, timestamps, and quality code for each value requested. OPC Historical Data Access (HDA) can be used to retrieve and analyze historical data and enable analysis, trending and reporting. The HDA typically retrieves data from a historian or relational database. OPC Alarms and Events (A&E) provide real-time OPC alarm data where rules can be configured or determined, such as where a signifier goes in an alarm stage, or what level of information is to be made available when an alarm is raised.

### *4.14.1 OPC Communication*

When looking at European countries compared to Asian countries, they understood the benefit and needs of OPC more quickly. But, early 80s OPC was a greater necessity for industries, who started to concentrate on this system. These industries also made different types of technology, such as Profibus, the Can-Bus system used for cars, and Ethernet, which most office networks used, but these came to a troublesome head when the industries tried to mix them up in the process. This came to become a problem for every single bus system - drivers had to be developed to handle these issues.

That meant every individual company tried to develop their own bus system, as they were not interested in letting competitors get open access to the protocol, or show a part of it. Across several applications and server communications, changes and adjustments occurred to the bus system and protocols, leading to system drivers producing changes and updates which caused high numbers of cost-intensive failures. This problem was taken into consideration and resulted in DCOM technology (based on Microsoft's OLE technology), for the access of real time data below the operating system Windows. It is a standard which was named as 'OLE for Process Control'. It gave industries an open participation between companies all over the world. From the following drawing you are able to see Client/ Server approaches.




When we look at the unified architecture of OPC UA, we can see it boasts compatibility with implementation on different vendors. This means you are able to use it on any platform, such as Windows, Apple, and Linux.

### *4.14.2 OPC Alarm and Event (AE) Measurement*

As mentioned previously, the OPC Client/Server exchanges data, information and events. The Alarm and Events Specification is defined to transmit/acknowledge in a structured way between server and clients. The advantage of this technology is that AE servers are able to capture and receive data from different sources. This means the AE server have the ability to collect data from PLC controllers or automation servers, which can analyse data and send notifications if any events occur. The AE server it also able to provide information on any changes in state, such as when something has happened or occurred, like the temperature exceeding the maximum permitted level. Alarm and Event protocol is fundamentally unlike the data access protocol as it does not have a current value on events. That means this protocol is a subscription based protocol and thus requires client support to get access to all events.

### *4.14.3 OPC Data Access (DA) specification*

The Data access state is an interface between a server and client which is able to exchange process data. It is able to access numerous clients and connect from different data resources. In this manner the data access client could be connected to a lot of other data access servers which gives the data thought.

### *4.14.4 OPC Historical Analysis (HAD) specification*

This type of Historical analysis protocol is able to support extensive record sets of data from different data points. The use of it is to provide a combined way to get out and allocate historical data which is stored in a historian system like OSI-Pi or SCADA. The advantage of HAD is it has historian data which can be used for call outsized amount of past data. In other words, it is able to glean old data which can then be used for present activities or for further development.

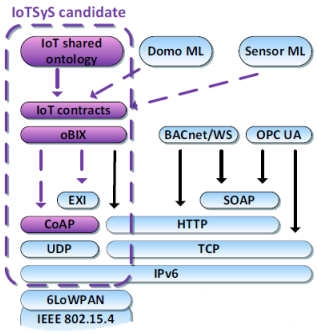
### *4.14.5 OPC UA communication for the Future Smart Grid Automation*

When we look at our current situation, it is based on saving energy in all possible ways. Technology of the future should have connected systems allowing for the needs and accessibility between participating parties like devices and stakeholders. This means there should be a system which is able to offer advanced communication facilities. In this manner there are some focused efforts at communication technologies, such as International Electrotechnical Communication (IEC) which aims to develop standards such as OPC UA, OPC DA and OPC A&E. The OPC UA is the successor to other classic standards and has the ability for extension to the application area to exchange data. When we look at the OPC UA successor it is well applied and accepts intertribal automation. There are more than 22,000 OPC products for companies to choose from, and every industrial automation implements Classic OPC. OPC UA can be used on intelligent devices and controllers to let Windows-based operation systems expose data. OPC UAs can also be integrated into systems such as Manufacturing Execution Systems running Linux using a Java application, or a Windows-based system. When we look at the security part of OPC UA it is built-in, as they are mostly used for Office purposes. It mainly provides high performance data exchange and reliable infrastructure for embedded devices. Moreover, this technology has built-in support allowing models to be hosted in server. OPC UA platforms are independent on the TCP/IP stack communication, and the standard transport layer also has two layers: one to establish a secure connection and another to handle the session. When we look at the transport layer closer, it is made up of HTTPS, SSL or HTTP, on top of TCP/IP. The OPC UA application parts are mostly used for bridging between two or more

communication networks, with different types of OPC servers which is known as tunneling. The GE global discovery servers also have OPC UA support systems for looking at the browsing data structure. Through these developments there are possibilities on including data models to transfer modes from ISA95, PLCopen and BACnet.

## *4.15 Using IPv6 gateway to combine BAS in to the IoT*

In this section you are able to see how to map the current FBD HVAC system into IoT. In the previous sections you read about how IoT works and what purpose it has. Now let us look at how we could adopt our BACnet network into IoT. The solution would be to place Web based communication protocols, like HTTP and XML, over a constrained application protocol (CoAP). The next step would be to make sure what type of standards and technologies are present, like in our building automation. The appropriate way to integrate the building automation into the IoT bridging is to use technology such as BACnet/WS and OPC UA to provide opportunities to use Web service-based protocols. User Datagram Protocol (UDP)/IP is the solution to use for binding to the web, where Open Building Information Xchange (oBIX) are approached as application layer protocols by the UDP/IP. The web service idea is to maintain interoperability and platform independent ways for sharing messages and having XML as a form of message encoding. As can be seen from picture 4.6, these are possible protocol alternatives of an IOT stack. The existing BACnet/WS and OPC UA are designed SOAP and HTTP to TCP which has the accrual protocol stack to IPv6. But when we look at the new modification on stack (which is circled), it shows how an IoT system can be adopted to IPv6. This means the CoAP server can be programmed on at a raspberry-PI microcontroller which provides request/response interaction. The oBIX can be used as application layer protocol for the IoT but need protocol binding from the CoAP server.




4.7 Protocol alternatives (IoTS to Ipv6)

## *4.16 QR Codes for sensors and controllers*

StruxureWare software provides web based applications for users to control or navigate the system. The current web based applications can be accessed via web browsers and apps' applications. Nowadays, most people are able to control and manage the HVAC system remotely. The same technology can be applied to the current algorithm which is present in this project. That means the StruxureWare software is able to pull all the data from the sensors and controllers, such as how many times the sensors are used etc. These data can be adapted to the web based systems, which can be used by the users.

QR Codes (Quick Response code) can be applied for this purpose. QR Codes are 2D bar codes which can be read by an imaging device to read it out as data. It is mostly used for displaying a user's vCard contact information, to open website URLs, etc.

Looking at the Whatsapp application messenger, it is able to access web browsers to allow for chat-based conversations [https://web.whatsapp.com/]. This means the web browser uses the mobile device as a key to get access to the Whatsapp massager account. Similar technology can be applied to the sensor or controllers into the BSM system. As an example, we can use DTU's library lighting system to control or use for data access, such as how much energy has been used within a particular time range.

# 5. Evaluation

In this chapter we are going to look at the question that whether the algorithms accomplish the task they are supposed to do. The first part is devoted to testing the proposed algorithms if they are able to fulfill the requirements. The second part will evaluate the proposed solution, mainly focusing on the test for the ease of use and users' impression.

As I have mentioned in chapter 2 there are lots of systems available to control the BAS but they are lacking some functionalities that failed to fulfill the end user's needs. They are in low level of function with control of the HAVC system to turn on/off when the sensors detect any movements. Also they are not capable of saving energy on each device or controller. My purpose is to create three different algorithms and network architecture solutions which will overcome the current problems on the BAS. As a result I have reached what I wanted at the end of the project. The algorithms are smart enough to do the task assigned. Furthermore the proposed network architecture is designed to fit all requirements. If applying with DTU buildings the network architecture can be used for all the campus buildings (101, 324 or 410). In the following writing you are able to realis more on testing and evaluation on algorithms and network architecture.

## *5.1 HVAC algorithm*

The HVAC algorithm is created to control the rooms or areas in energy efficient manner. The algorithm is able to save energy through the controllers or sensors if they are not active. If the rooms or areas are not occupied the devices are set in standby mode, during the holiday period all the devices are in saving mode, which means they might be low in use or not at all. There are different types of tests been done, which can be read from chapter 3 (Test on HVAC FBD). These tests show the created algorithms are useful and can be used in real DTU BMS for long term use as well. Moreover there are similar software created which will be provided in the presentation.

## *5.2 Weather station from DTU*

The idea behind the weather station algorithm is to pull real-time weather data from the weather sensors placed at DTU. From chapter 3 (Testing on Weather station for DTU) you are able to see some testes, which has been gone through and showed that the weather station algorithm is useful. For instance these collected weather reading data can be used for indoor HAVC system and for any future developments. There are weather readings available for past three days or more, these could be used for calculating how much energy has been used for heating or cooling the area in this period of time. Moreover these data can be kept as long as they are required depending on users' needs. Not only reading data also calculated data can be applied to other algorithms such underfloor heating of the heating system on weather basis. That is taking the outdoor temperature and humidity into the adjustable function of the floor heating temperature.

Overall the weather station algorithm is useful and possesses options for further developments. It can be extended with XML in web based technologies, the Extensible Markup Language (XML) can be used to show data from the weather station on different software platforms. That means the XML are used to interchange of data over the internet. To know more about the function see chapter 2 (2.6 IPv6 multi-protocol gateway).

## *5.3 Underfloor heating and cooling system*

The idea is to reduce energy consumption and use time when placing underfloor heating and cooling system. With the old radiator heating system we spend lots of money for heating and it is time consuming for heat balance. Thanks to the algorithm there is no need to manage the heating system by manual options at all. Algorithm itself is able to assess and manage the room temperature level with outdoor temperature level. If the outdoor temperature drops, the algorithm is able to adjust the indoor climate. There are more testing on underfloor heating and cooling system in chapter 3 showing how they work with temperature. Through this algorithm I have reached what I expected and in my point of view this smart algorithm can be used for DTU campus. There are some issues as they require building cost which might be expensive but for long term it is worth every penny.

## *5.4 Network architecture*

There are many possibilities on network designs, but the provided solutions are based on designation of the network which can be used for DTU buildings on their demands to solve the issues. For instance compatibilities issues can be dealt by different protocols and devices which should be adapted to the network architecture. There are various vendors and peoples (engineers) working on great variety of servers and controllers which have potential to communicate with each other. The provided network architecture is able to handle these problems in a good manner. In the chapter 4 (Description on network architecture for DTU buildings) you are able to read how the network is designed. Also there are more solutions on securities on the network which make it stronger to use the network in safe environment.

# 5 Conclusion

This thesis presented a concept of a smart algorithm which could be used to regulate protocols for the improvement of environmental efficiency, energy consumption and users' quality of life. The algorithm was developed on software provided by Schneider Electric, although other brands can be utilized for the purpose. It was also developed for specific hardware, including individual controllers and sensors, especially with regard to indoor and outdoor temperature sensors. This algorithm was designed with a variety of environments, including small and large scale buildings for private and public use. It was created with different types of communication technology, allowing the ease of transition to newly developing technologies as well as existing forms. This algorithm was created with regard to BACnet protocols, while also allowing the use with other protocols via the aid of controllers and other hardware, but it is primarily aimed at building automations. Data derived from the sensors can also be used in the future, leading more developments. Especially the weather data algorithm gives the users more detailed data of the weather, and help to improve the usability of the system. Furthermore there are some researches done on network architecture with engineered devices. The BACnet solution can be applied to the DTU buildings which avoid fault tolerance and resulted traffic less network.

# 6 Deliverables

| File or Directory | Description |
|---|---|
| **"readme.txt"** | An explanation of the contents of the delivery |
| **"MSc – Puvishanan S.Naguleswran (s0131250).pdf"** | The thesis as such (this document), as submitted to the IMM librarian for print. |
| **Engineering part** | There are Software and Hardware used for the project to crate algorithms. |
| **Thesis** | |
| **"Thesis.docx"**<br>**"Thesis.PDF"** | Files go together with the thesis, e.g. included docx files that were used to generate the PDF, |
| **PIC** | Pictures included as figures and drawings |
| | |

# 7 Bibliography


[1] W. K. Markus Jugen, "Building automation and smart cities," 2011.

[2] J. C. J. Martocci, "Building Automation Routing Requirements in Low-Power and Lossy Networks," Jun 2010.

[3] W. K. G. N. H. M. N. Stefan Soucek, "Communication Systems for Building Automation and Control," 2005.

[4] T. R. Steffen Wendzel, "Covert Channels and their Prevention in Building Automation," 20 November 2012.

[5] S. H. F. J. a. S. G. Sergio Leal, "Implementation of an automated building model generation tool".

[6] S. Electric, "Schneider Electric Healthcare," Schneider Electric , 2010. [Online]. Available: http://blog.schneider-electric.com/healthcare/2014/02/05/8-ways-hospitals-can-benefit-intelligent-infrastructure/.

[7] T. Palmer, "Bring BIG Buildings Automation To the Small Building Market," 2009. [Online]. Available: http://www.automatedbuildings.com/news/sep09/articles/viconics/090819030404viconics.htm.

[8] H. H. H.Merz, "Building Automation," [Online]. Available: https://books.google.dk/books?hl=da&lr=&id=pxPq2CZSVooC&oi=fnd&pg=PR1&dq=intruder+detection+systems+on+bacnet&ots=i6EePoXa0Q&sig=zwMLQcclNMcAUgK-lxHMSbeMJlc&redir_esc=y#v=onepage&q&f=true.

[9] Cimetrics, 2010. [Online]. Available: https://www.cimetrics.com/b6000-bacnet-mstp-router.

[10] [Online]. Available: https://www.cimetrics.com/B6001-BACnet-IP-to-MS-TP-Router-Module .

[11] [Online]. Available: http://openrb.com/example-knx-to-bacnet-gateway-with-lm2/ .

[12] S. Electric, "Automation solution guide," 2008.

[13] W. K. G. N. a. F. P. Wolfgang Granzer, "Security in Networked Building Automation Systems," 2011.

[14] C. P. Klaus Kursawe, "Structural Weaknesses in the Open Smart Grid Protocol," 2011.

[15] "IPV6 in automation technology," 2013.

[16] J. W. Markus Jung, "A transparent IPv6 multi-protocol gateway," *Internet of Things.*

[17] W. Kastner, "Integrating Building Automation Systems and IPv6".

[18] "Integrate Building Automation Systems in the Internet of Things".

[19] K. Technologies, "OPC Quick Hepl," 2015.

[20] "Planning BACnet networks," [Online]. Available: http://www.kmccontrols.com/images/com_kmcproducts/products_documents/an0404a_revb.pdf.

[21] S. H. Hong, "Implementation of Fault Tolerant Mechanism in the BACnet/IP Protocol," *School of Electrical Engineering and Computer Science.*

[22] Schneider Electric, [Online]. Available: http://www2.schneider-electric.com/sites/corporate/en/products-services/buildings/smartstruxure/videos.page.

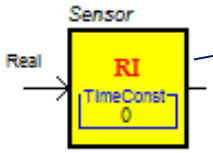
[23] Product Comparison Guide, [Online]. Available: http://download.schneider-electric.com/files?p_Reference=CG-EnOcean868&p_EnDocType=User%20guide&p_File_Id=793454545&p_File_Name=CG-EnOcean868-EN_A4.pdf.

# 8 Appendix Description on FBD

***Function Block Diagram***

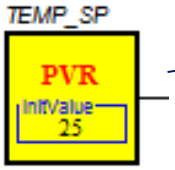
**In this appendix manual you are able to read about the Function Block Diagrams which have different function. All block do have different functionalities and van be used for different purposes.**

***Real input Function Block***



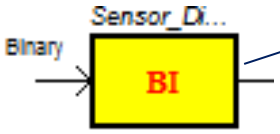

This is a real input FB which is able to connect signals between the block. That means you are able to connected sensors to measure CO2 or temperature.

***Real Value Parameter Function Block***



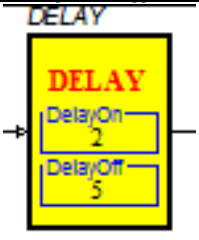

This Bock is used to get real parameter value to an input from different block. That means you can have real value from the sensor to set a value. When you set up initial value with 20 C it will output the value to other block.

***Binary Imput Function Block***



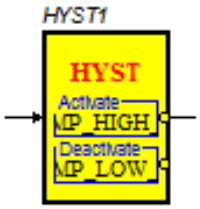

Binary Input Block is used for connecting signals between I/O modules. Which are able to get digital signals from PIR sensor to control damper motors and updated during each program execution.

***Delay on/off Function Block***



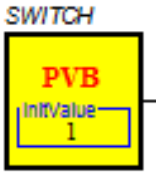

The delay bock is able to delay the transition for input signal. When the signal comes from PIR sensor it can be delayed for couple of minutes or hours. Also the output signal can be delayed as well.

***Binary hysteresis Function Block***



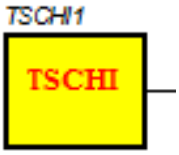

This block implements a real function with hysteresis. The parameters are If Active is greater than deactivate then:-Output false (0) and the input signal exceeds the activation threshold output changed to true (1). If the active is less then deactivate the true output (1), and if the input signals are more than deactivation threshold the output will be false (0).

***Binary Value Parameter Function Block***



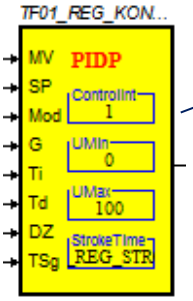

Used for user selectable binary parameter value for another block to get input signal. To get access to the block from the network it should be set as public.

***Binary Value Parameter Function Block***




It is a Time Schedule input block which can be used to define the time. This smart block is able to handle the function of the system such what time should stared and stop the heating systems or lights etc. Mend to be saving energy during holiday time.

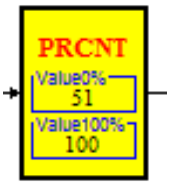
***PID Controller Function Block***




This PID blocks is used for control loop algorithms for the controllers and for different controllers in a way as analogue physical output. When we look at the operating mode of the controller is depends on the input signal mode.
Mode = 0 => off, controller stopped
Mode = 1 =>Normal control.
Mode =2 => Controller output are forced to UMax.
Mode =3 => Controller output are forced to UMin.
If Mode =0, the controller output will look for the tracking signal (Tgs) input. If the Mode < 0 or Mode>3, the controller operating mode will be off (same as Mode =0).
The PIDA block is bit different from the PIDP in a way the saturation is longer in time then PIDA block. When by using PI or PID the set point will not cause a step changes in the PIDP block.

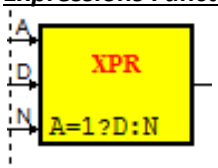
| *MV* | *Real input* | *Represent measured value* |
|---|---|---|
| *SP* | ***Real input*** | ***Set point value*** |
| *Mode* | ***Integer*** | ***Operating mode for controller*** |
| *G* | ***Real input*** | ***Controller gain*** |
| *Ti* | ***Real input*** | ***Virtual time in second*** |
| *Td* | ***Real input*** | ***Derivative time in second*** |
| *DZ* | ***Real input*** | ***Dead zone*** |
| *TSg* | ***Real input*** | ***Tracking signal is able to get value from previous signal*** |
| *Controller* | ***Real input*** | ***Control interval per second*** |
| *UMin* | ***Real input*** | ***Minimum allowed control signal*** |
| *UMax* | ***Real input*** | ***Maximum allowed control signal*** |
| *Stock Time* | ***Real input*** | ***Actuator full stroke travel time per second*** |
| *OUTPUT* | ***Real input*** | ***Read and write*** |

***Percentage Function Block***



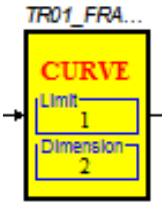

Percentage Block is used for the transformation of the input signal. That means the Block will take the input signal and transform as percentage. Examples get input signal and show as percentage for a heating controller such if the heating motor starts it will shows the percentage value and from 0% to 100%.

***Expressions Function Block***



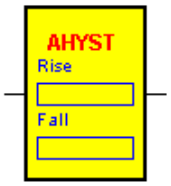

The expression block have different output values such real, integer and binary outputs. It can have different inputs depending on the expression. Such if the inputs letters are capitalized such (A, D or N) it will be analog input but if the inputs letters are in lower case (a, b, d or c) then binary inputs. There are two different Constance (numeric and alphanumeric) these have effect on sign such +, -, :, !, ect. The output signal will be varied from the different blocks. The XPI block result will be converted in 16 bit signed integer number. The XPB binary results are zero, the output will be zero and if the value is different than zero the output will be one. The last one is the XPR block which has the real number output and gets from the evaluation of the expression.

***Curve Function Block***




These curve function block have 2 different inputs (limit and dimension). The binary limit function limit =1 or limit = 0 for the selector. The Dimension are listed with coordination on x and y for the curve function.

***Analog Hysteresis Function Block***




This AHYST block is able to implements an analogue hysteresis function. If the Rise less then fall the hysteresis will be looped in clockwise but if Rise bigger the loop s counter clockwise as indicated in the figure.

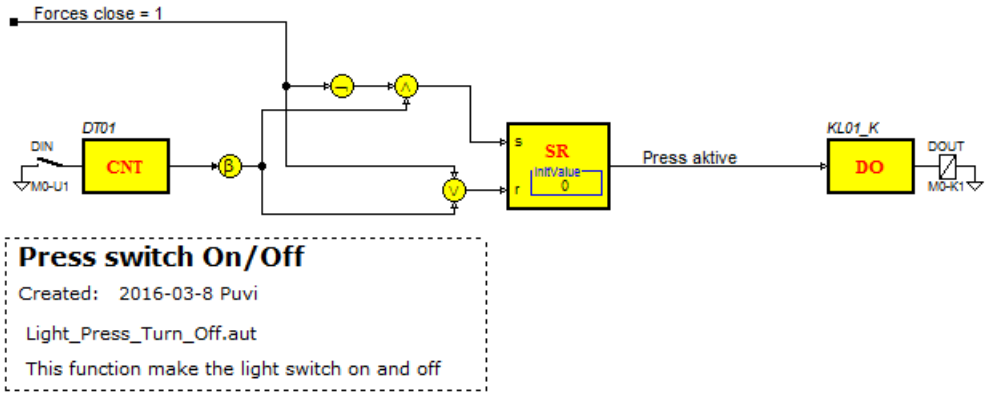
# 9 Appendix More Algorithms on FBD

***Function Block Diagram***

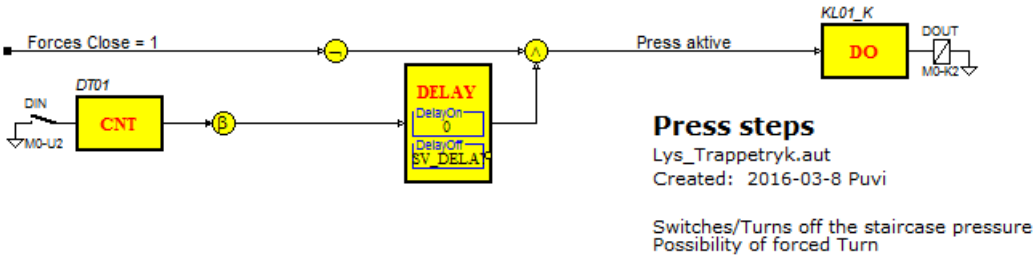
**In this appendix there are more developed algorithms presents which has different functionalities. These algorithms can be used for further developments and do have some smaller effect on simple function. Example the first FB gives function on how lighting system can be used or used for further development.**

***Press switch on/off Function Block***

**This FB algorithm is used for switch function where users are able to turn on/off the light switch or any other ventilation. This FB is used for the Programmable digital underfloor heating Thermostat.**

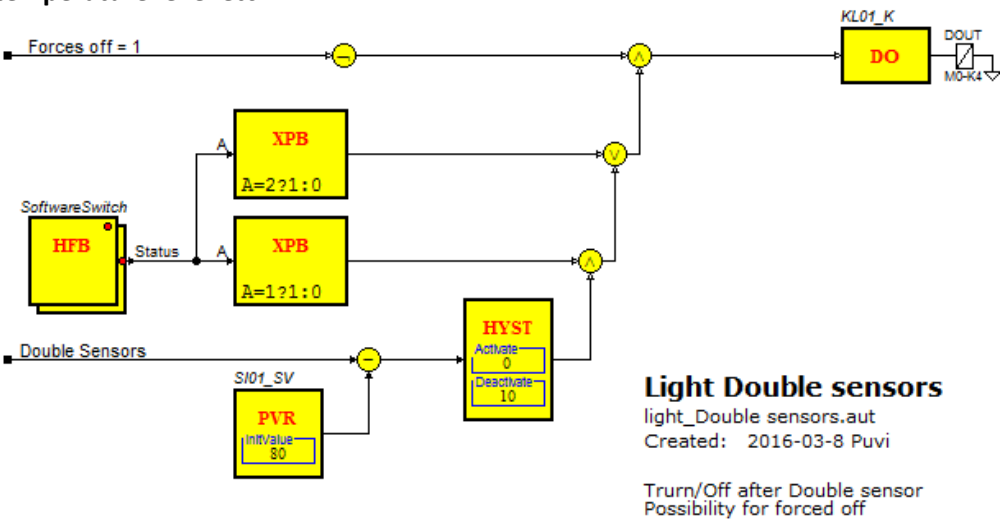


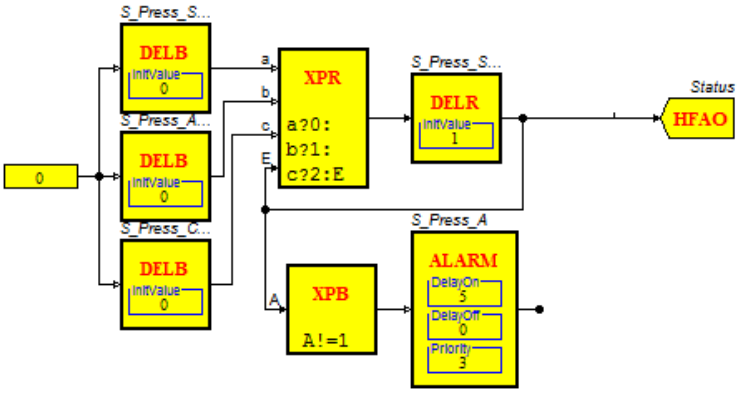

***Stare case pressure Function Block***




***Light Double sensors Function Block***

**This FB algorithm is used for switch function for light Double sensors which you are able to see from the underfloor heating system. This algorithm is used for thermostat controllers to regulate the temperature level etc.**






## Software switch with. 3 press

Software Switch_3.aut
Developt: 2016-03-8 Puvi

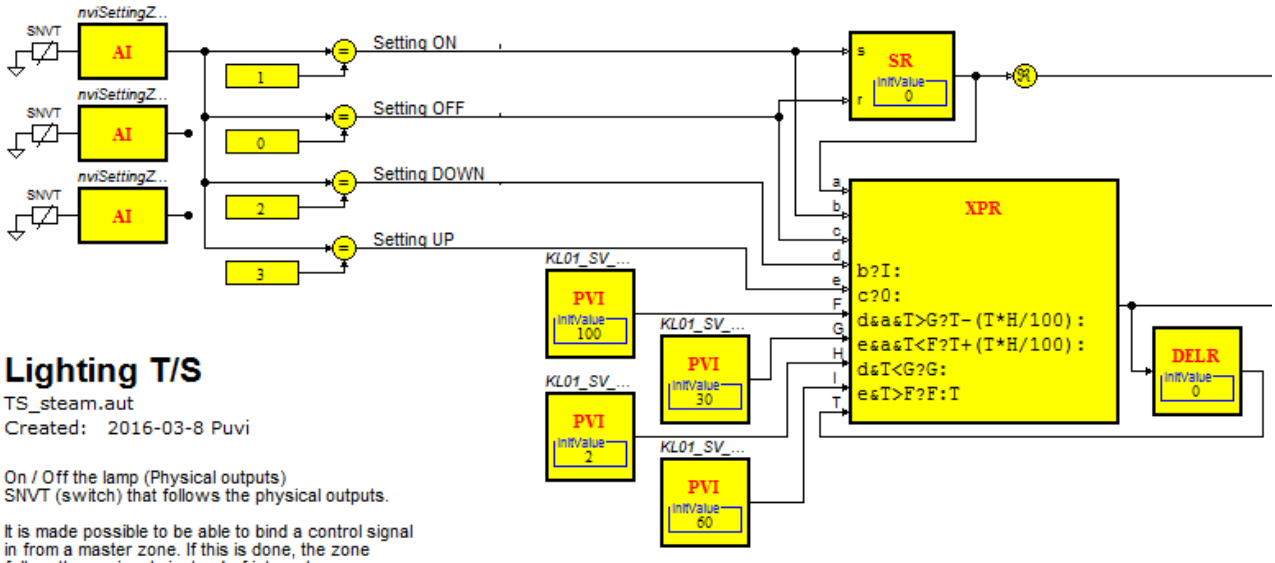
Switch with the following buttons:
- Stop
- Auto
- Constant

There is alarm when the switch is not in Auto

***Lighting SNVT setting Function Block***

**This FB algorithm is used for controlling the lighting system. Not only to control it also able to work with lux sensors. That means the lux sensors are able to deliver how dark or bright the aria is such if the room are brighter the algorithm is able to adjust the light level which has positive effect on energy. Moreover there are possibilities to use the algorithm to different FB diagram for further developments.**

## SNVT Setting



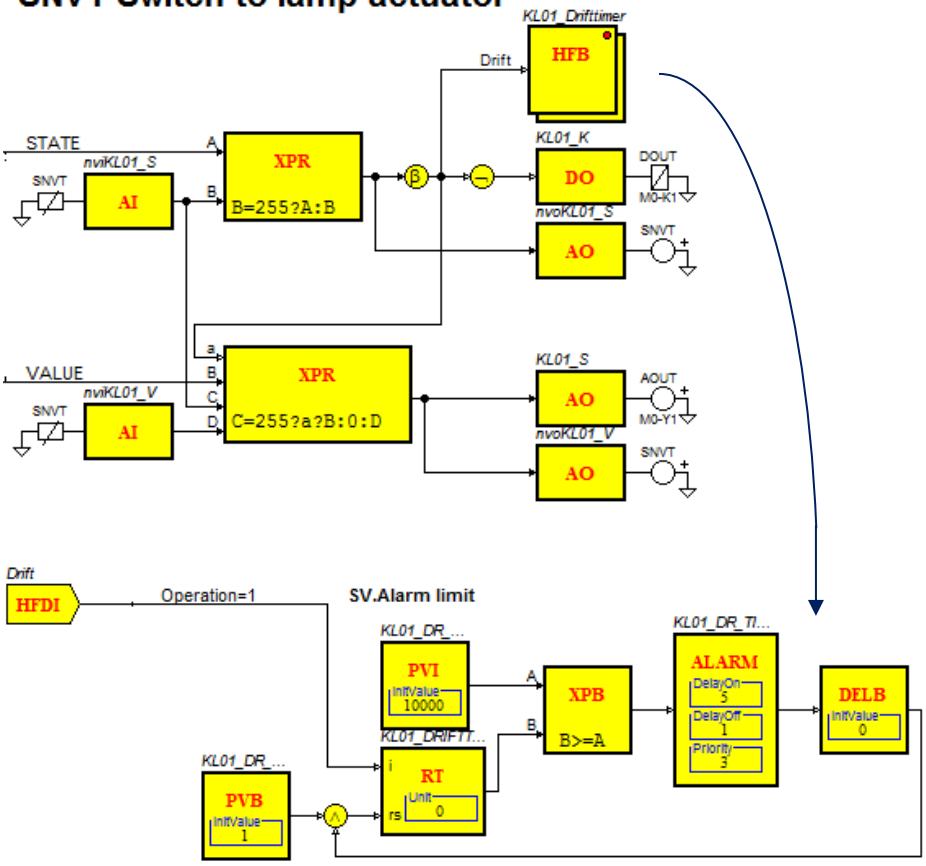

## Lighting T/S

TS_steam.aut
Created: 2016-03-8 Puvi

On / Off the lamp (Physical outputs)
SNVT (switch) that follows the physical outputs.

It is made possible to be able to bind a control signal in from a master zone. If this is done, the zone follow these signals instead of internal.

## SNVT Switch to lamp actuator




## Operating hour registration 5

Operation hour_5.aut
Created: 2016-03-8 Puvi

Drittimetal recorded.
An alarm is triggered by exceeding the alarm limit.
It is possible Automatic alarms