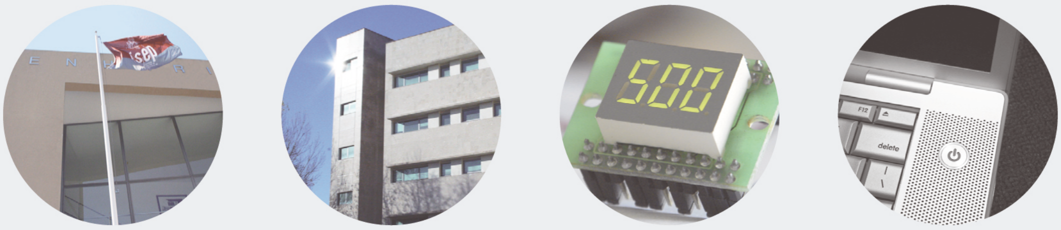
INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO

MESTRADO EM ENGENHARIA ELECTROTÉCNICA - SISTEMAS ELÉCTRICOS DE ENERGIA



Radio-Frequency communication in a SCADA system for the monitoring and control of intelligent building and office blocks

TOM COPPENS

Junho de 2017

POLITÉCNICO
DO PORTO

Radio-Frequency communication in a SCADA system for the monitoring and control of intelligent building and office blocks

Tom Coppens

isep Instituto Superior de Engenharia do Porto

Departamento de Engenharia Eletrotécnica

Mestrado em Engenharia Eletrotécnica – Sistemas Elétricos de Energia

2017

Relatório elaborado para satisfação parcial dos requisitos da Unidade Curricular de DSEE - Dissertação do Mestrado em Engenharia Eletrotécnica – Sistemas Elétricos de Energia

Candidato: Tom Coppens, Nº 1161954, 1161954@isep.ipp.pt
Orientação científica: Professor Zita Vale, zav@isep.ipp.pt

Empresa: GECAD Research center

Supervisão: Professor Zita Vale, zav@isep.ipp.pt

Cossupervisão: Pedro Faria, pnfar@isep.ipp.pt

Departamento de Engenharia Eletrotécnica

Mestrado em Engenharia Eletrotécnica – Sistemas Elétricos de Energia

2017

ABSTRACT

The efficient use of electricity and how people approach it, is a topic that has a big impact on the environment and society. The consumption management will be improved by the monitoring and the controlling of electrical installations. By creating a management of the industrial installations people will use the existing and new energy resources more careful. Communication is a key part in this process and that is why the improvement of data transmission is very important to obtain a controlled process. Transferring data is achieved by sending an electromagnetic signal by means of radio waves, electrical voltage, etc. by means of different types of communications channels.

The main goal of this report is to contribute GECAD developing a connection between a superior network and an external one to create the possibility of monitoring and controlling devices linked to the networks. The communication devices used are modems which use radio waves to make the transmission. The two advanced radio modems (ARM-SE) that are used during this assignment have the ability to connect with slave devices using different types of communication protocols.

All the different protocols to achieve a data transfer between the two networks have been investigated and analyzed to find the best solution to connect a programmable logic controller to the network of GECAD. A program has been created to access the data of an analyzer to obtain knowledge on how to implement analyzers in a SCADA system to improve monitoring of an electrical installation. This assignment will achieve a better understanding of the different protocols and operation modes used in the industrial sector to create intelligent buildings and office blocks.

The whole assignment is set up to monitor the data of a power analyzer (CIRCUTOR) which makes it possible to test all the operation modes and develop the program to retrieve data from the analyzer. Thereafter the program was used to create a SCADA system to retrieve data from other analyzers (PM130) connected to a PLC on an extern location. This is made possible because both analyzers are compatible so after changing some parameters, data could be retrieved easily. Despite a lot of difficulties with the modems, which creates a doubt of their reliability, it concludes that they are useful devices to transmit data for the intelligent buildings.

Keywords: Intelligent building; SCADA system; Matlab®; MODBUS TCP/IP; ARM-SE; radio transmission

ACKNOWLEDGMENTS

By starting this report, I would like to thank all collaborators off the research lab GECAD for their help and dedication during the assignment and for the nice environment to work in. My special thanks go out to Pedro Faria and Omid Abrishambaf for their help with the complex and difficult issues and to Professor Zita Vale for arranging the assignment. The assignment was about a whole new technology that was unknown for me. I have enjoyed these few months at the research facility very much because of their educational value and knowledge about radio communication and all the various protocols that I was able to acquire.

Furthermore I want to thank my family, friends and my girlfriend Charlotte De Vriendt for the support during this period. Without them nothing of this would be possible because they have been supporting me my whole life.

My last mention goes out to KU Leuven and Odisee to give me this opportunity to study abroad and giving me the experience of my life. I would recommend everybody to do the same experience as me.

Content

List of Figures

List of Tables

List of abbreviations

A	Ampere
Bit	Binary Digit
Bps	Byte per Second
Dec	Decimal
GECAD	Research Group on Intelligent Engineering and Computing For Advanced Innovation and Development
Hex	Hexadecimal
IP	Internet Protocol
ISEP	Instituto Superior de Engenharia do Porto
I/O	Input/output
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
TCP	Transmission Control Protocol

CHAPTER 1: Introduction

1.1 Motivation

The consumption of energy is a topic that raised much concern over the last decades. The environmental impact and the exhaustible supplies are problems that are inevitable. There is a focus to avoid more problems concerning renewable energy and the consumption of the exhaustible sources.

Buildings are one of the biggest energy consumer with a lack of attention on how to deal with an efficient energy use. With the growing world population and urbanization, the focus lies on how to manage an efficient energy consumption of energy in buildings. Intelligent buildings have technology that creates a more productive solution to this problem. By monitoring internal and external elements that influence the energy consumption of a building it is possible to consume in an efficient way. The use of smart devices and software, which are specifically developed for this purpose, allows to achieve a coordinated use of energy. This electrical system is known as a smart grid and uses the information of the installation to manage and improve energy consumption.

The industrial sector is important to integrate these intelligent systems. It is projected that in 2040 industry will consume more than half of the global delivered energy. Fossil fuels are still the biggest energy supply however the nuclear and renewable energy are growing fast. This means that the use of these energy sources has a big impact on the development of systems to control the energy consumption. As an example, solar panels contribute during the day but depend on the weather and other factors. This create an inconsistent source of energy that needs to be controlled and managed for an efficient use. Besides the solar energy, there are other sources, such as energy from wind, that are also fluctuating and unpredictable. This complicates the fact that renewable energy sources are the future of the energy business because of the still rising growth of greenhouse gases.

There are two main types of buildings, residential and commercial. Furthermore the industrial and transportation sector are also major consumers. When talking about smart buildings it can easily be extended to smart cities on a larger scale. The smart grid is the base of the intelligent controlling of systems and actively managing of the consumption [1].

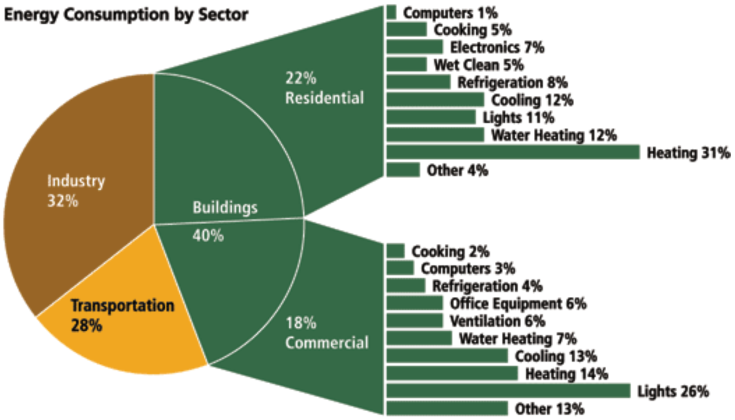


Figure 1 Energy consumption by Sector

Connectivity and management are the pillars of the intelligent systems to reflect on the consumption in the different sectors. It is important to react where necessary to create an efficient consumption with an environmentally friendly focus. Intelligent algorithms are designed to access the information needed to manage the installation. These algorithms are created to be integrated easily in a process because they are flexible and can be wirelessly connected to an operating system. The use of a SCADA system makes it possible to collect, process, display and manage information for the intelligent buildings.

The assignment is creating the ability to control and monitor an extern network to manage production and the consumption in the future using a new radio modem that GECAD has bought. The aim is to establish data transmission, creating a link between two separated networks and retrieve usable data. The focus is on the connectivity and creating an own SCADA system to monitor and manage an extern installation [2] [3].

There are many different ways to achieve data communication to reach connectivity of intelligent buildings such as Ethernet, LAN, Wi-Fi, serial communication etc... Avoiding hardwiring is often useful because of its substantial costs or when it is not geographically possible. But sometimes it is the cheapest way to create the communication.

Wireless communication has many advantages which are created by applying new techniques to improve the quality of the radio bridge. Over time there has been many different data transmission systems and they all have the same requirements. The first requirements is the transfer distance which has increased drastically over the years with decreasing probability of failure. Capacity and speed of the transfer are also really important to send as much information as needed. Furthermore, the geographic aspect and the costs of an installation are also influential aspects. The combination of all these factors is determining for the type of communication channel fits best for a specific data transfer.

The only negative aspects of a wireless transfer are the lack of security due to wireless connecting with another network and the impact on health of prolonged exposure. The lack of security can be bypassed using encryption of the data transfer and the health issue has been improved during the years of research [4].

1.2 GECAD

GECAD is a research group in ISEP, Instituto Superior do Engenharia do Porto, which is specialized in information technologies. The core activity of the facility is on intelligent engineering and computing for advanced innovation and development. The research unit has two main departments: Intelligent Systems and Power Energy Systems. This assignment has covers both because its focus is on the consumption of new energy resources integrated into intelligent systems [5].

1.3 Assignment

This report describes how an integrated SCADA system, Supervisory Control And Data Acquisition, realized using the program Matlab®, will be using radio waves and Ethernet with the Modbus protocol to connect with analyzers (PM130) of a PLC. This creates a perfect simulation of the communication of industrial installations used in real-life. It also provides the possibility for increasing the number of analyzers and other devices on the network in the other location in the future.

In the GECAD laboratory, a SCADA system is already integrated which allows the researchers to monitor and control the energy consumption in the building. The next step in the process is to add an external network to the one of GECAD so it can be integrated in the existing SCADA system. Thereby the researchers will be able to access the data of the electrical installation in another building.

With the use of the ARM-SE modems it is possible to connect these network together. Thereby the data of the new network can be monitored and controlled with the existing system. The modems will be analyzed if they are suitable to connect the external network to the one of GECAD. The different protocols of the modem will be tested to find the best solution to transmit the data to the GECAD network. The chosen protocol needs to access and read the data so it can be reachable for the SCADA system. A simulation is created with a slave energy analyzer, CIRCUTOR, which will be accessed from the GECAD network using the modems. This way it is clear how the protocols operate and if the CIRCUTOR can be a part of the SCADA system.

This is possible because the CIRCUTOR can be effectuated inside the research lab of GECAD. This ensures the best option to connect both modems with the analyzers (PM130) of the PLC because both analyzers use the same protocols. The created bridge will be used to send small amounts of data and increasingly test its capacity and limits to determine all the possibilities of the different operation modes. In this phase of the assignment, the program is tested in Matlab® to reach the data of the CIRCUTOR with Modbus.

If the tests are positive the slave can be changed with the analyzers, PM130, operating in the external network. If they are also able to send data to the GECAD network, it can be integrated in the SCADA system to monitor and control the electrical installation. By reaching the network of GECAD using a PLC of the laboratory a SCADA webpage can be created and the data can be monitored.

A summary of the described tasks is shown below which creates a clear view on the goals of this report.

- Configuration and identification of the modem.
- Testing different operation modes to create the best connection with the analyzers.
- Creating Matlab® program to reach the data of the CIRCUTOR.
- Installation of the modems and antennas in the different buildings.
- Implementation in SCADA system to monitor the electrical installation. This is also the main goal of this report.

CHAPTER 2: Equipment and systems

This chapter contains all the information about the equipment and system used during this assignment. The information about the radio modem and energy analyzers describes the operation of the device and includes important settings important during the installation. Furthermore, this chapter describes the programs used during the assignment to complete the mission.

2.1 Advanced Radio Modem

2.1.1 General

ATIM is a French manufacturer of radio communication devices since 1992 and is specialized in industrial communication. The ARM, (Advanced Radio Modem), is a data communicating device, manufactured by ATIM, using a license-free high-frequency band which means there is no license or permission required to communicate on these frequencies. The frequency band used is located between 863MHz and 870MHz and is suitable for industrial, medical and scientific applications. The ARM is designed to function in various situations such as data transfer, remote control, etc. and is mostly used in places where hardwiring is not the best solution. It had a good track record for transferring data and managing different types of input and output over long distances without failure. The applications for this modem are endless: camera control, energy management, industry, etc. [6].

Figure 2 ARM-SE

2.1.2 ARM-SE

The research lab, GECAD, uses the ARM-SE which can operate with serial ports RS232 and RS485 or Ethernet as an alternative of Wi-Fi as the communicator with the network. With this device, it is also possible to establish access to other devices using distance I/O. ATIM created an embedded web page for the configuration of the device which makes it easy to use. By means of Hayes AT-commands, this is also possible if the operator has no access for using the web pages. In this report the settings and configuration are managed using the web pages and data are retrieved using operation modes Ethernet, serial and Modbus [7].

In Figure 3 all these modem connections, which can be used for transmission are presented. AQlso indicated are the connections for the power supply and for the antenna.

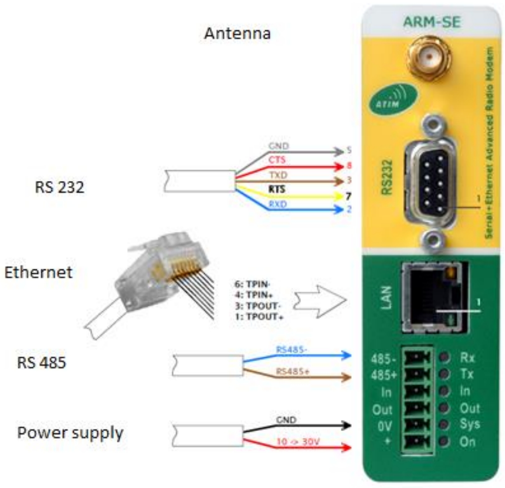


Figure 3 ARM-SE with connections

2.1.2.1 Thumbwheel

On the back of the ARM-SE, a thumbwheel is integrated which allows the device to switch channels between the frequency's 869,8 MHz and 869,757 MHz. The wheel has 16 positions, hexadecimal from 0 to F and with every step corresponding to a difference in frequency of 50 kHz. This thumbwheel creates the opportunity for the ARM-SE to switch between different channels to avoid interference with other radio devices in the area. It is important that the frequency of all the participating modems are the same to avoid an error in the communication. Some of the frequencies have a different achievable range and power compared to others. The largest power is around 500mW which can reach over 5 km of range [8].

The thumbwheel can also operate with other application when going into test mode in the case to perform a factory reset. ATIM has created a tab on the webpage to allow digitally changing the frequency channel when the thumbwheel is used for these other applications.

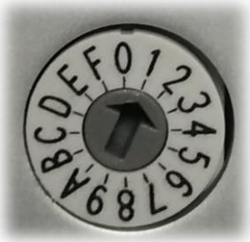


Figure 4 Thumbwheel

2.1.2.2 Side components

Power supply for ARM-SE

The ARM-SE needs a power supply set between 10V – 30V DC which is rectified and filtered to create a pure voltage. The research lab uses a SAIA PCD convertor of 24V DC to power the modems. In the case of the modem installed next to the PLC, also a power unit of 24V is available.

Ethernet connection

The connection between the network of the computer and the modems consist of a CAT 5 crossover cable. The Modbus gateway operation mode also uses the same cable as for the Ethernet mode given the protocol can be used over Ethernet.

RS232 – RS485 Serial link

The ARM-SE is specially designed to establish a connection between Ethernet and RS232 or RS485. To connect the modem a 9-pin cable is required to plug into the interface of a PLC. The connection is made with the RS485 for both sorts of analyzers.

Antenna

To send and receive data, every modem is connected to an antenna which creates the radio communication. There are various types of antennas for each situation and all affect the quality of transmitting data. The antenna used in the test set up is the ANT868-BZ or “Bazooka” which is an omnidirectional antenna, especially designed for mast fitting. This allows the antenna to be situated 20 m from its respective modem [8].

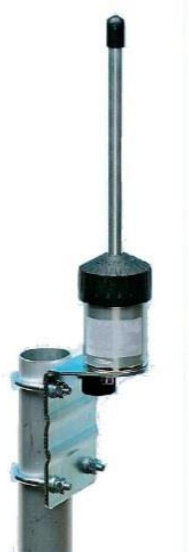
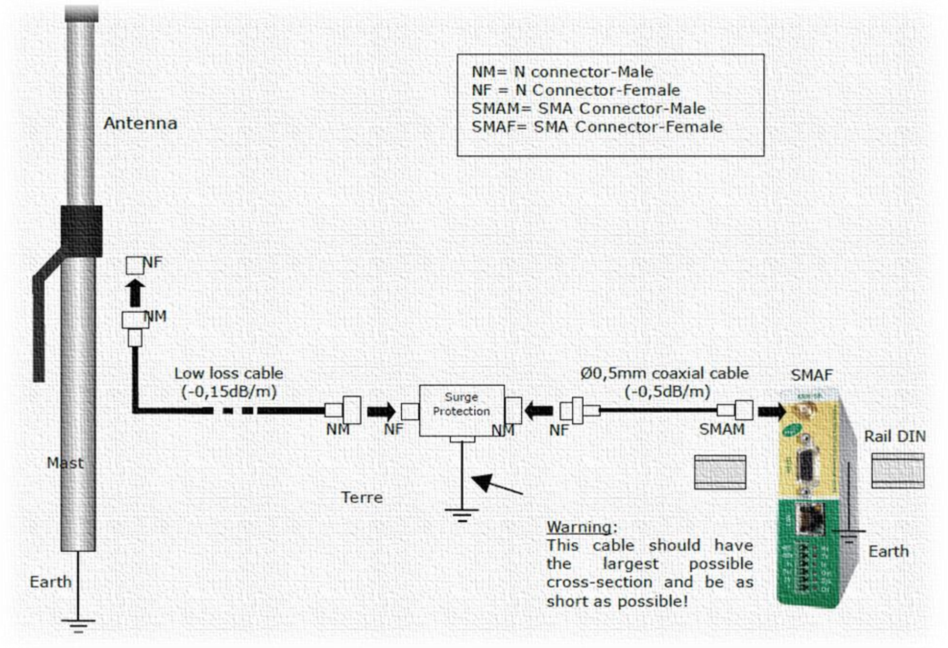


Figure 5 ANT868-BZ

2.1.3 Installation

The installation of the different components is vital to achieve a perfect radio bridge. The antenna is connected to the modem using a low loss cable as it is essential that the attenuations are minimized. This requires the cable to be short and the modem to be protected from high power. Therefor a surge protection with Terre is attached in the middle of the cable.



Warning:
This cable should have the largest possible cross-section and be as short as possible!

Figure 6 Connection between antenna and modem

The placement of the antenna is crucial to avoid huge losses and bad data transfer. After choosing the right antenna and its corresponding cable, placing both in their line of sight is a priority. But there is another phenomenon known as the “Fresnel zone” that has to be considered as well. The height of the antenna is proportional to the distance of the second antenna which means that the antenna needs to be higher when wanting to transmit further. The Fresnel zone can be indicated with an ellipse between the two antennas as shown in Figure 7.

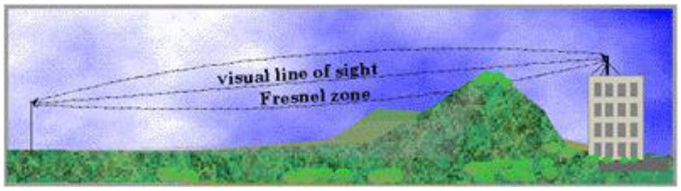


Figure 7 Fresnel zone

During the installation, it is necessary to ensure that the frequency, used for the data transfer, is free. The embedded web pages are equipped with a spectrum analyzer which checks frequencies that are already being in use. The thumb wheel, previously cited in *2.1.2.1 Thumbwheel* on the side of the ARM can changes the frequency by means of rotation [7] [8].

2.1.4 Operating modes

The ARM-SE is equipped with a serial mode, Ethernet mode or Gateway Modbus mode and these modes are integrated into the software of the modem. Via the webpages, the different operating modes can be accessed through Ethernet or Modbus. The image below shows the organization chart of the ARM-SE with all the operation modes and their options. It gives a clear view of all the possible ways to make the data transmission.

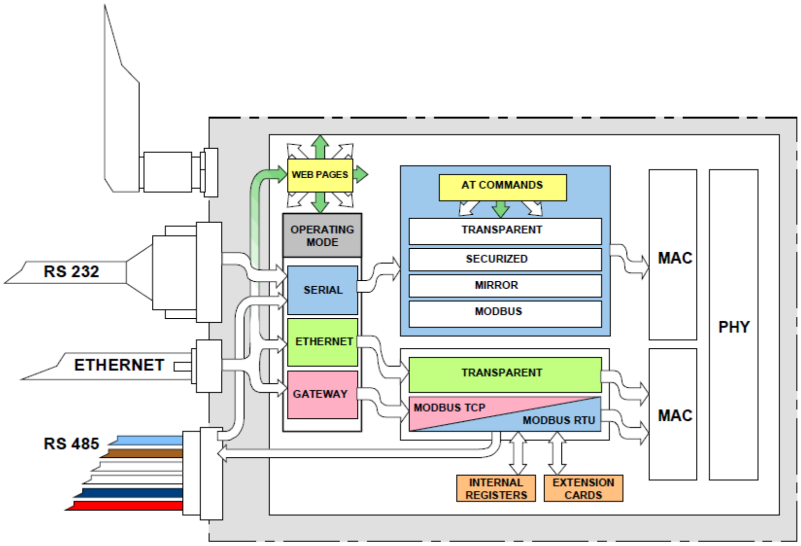


Figure 8 Diagram of the different operating modes

Every operation mode has a different way of transmitting data and can be programmed with the embedded webpages or by using the Hayes AT-commands. For the assignment in this report it was sometimes necessary to develop an extern tool to create an interface to display the request and its corresponding response. This was necessary to test all operation modes at once without installing too many devices [9].

2.1.4.1 Ethernet

Ethernet is an operation mode used for computer networks technologies. It is commonly used in local area networks (LAN) and can connect to many different protocols. Ethernet is used for wired interfaces as it is a physical layer. Over the years Ethernet has grown thanks to research and new technologies to a fast and reliable link for data transmission. Ethernet has backward compatibility which allows it to operate with older systems. Using this operation mode the ARM-SE is sending Ethernet frames to other occupants using the CAT 5 crossover cable [9].

2.1.4.2 Serial

Serial communication is also commonly used in data transmission but more for long-haul communication where parallel communication with other occupants is difficult. This operation mode sends one bit at a time in a sequence with the possibility of error checking. Because of its simplicity there requires a protocol in the connected device like the Modbus protocol in a PLC.

Two serial interfaces, RS232 and RS485 are widely used. RS232 is for single-ended operation modes while the RS485 is for differential modes. The differential mode is preferred for communication with higher data rates or over longer distances to create a better performance. This is the reason why most serial devices use RS485 and why it was used in this study setup [10].

2.1.4.3 Modbus

Modbus is a serial protocol for communication with programmable logic controllers developed in 1979 by Modicon, today known as Schneider Electric. The protocol has become a common tool for transmission between various kinds of electrical devices. Modbus connects a supervisory computer with a SCADA system. It can connect several different communication systems by means of RS232, RS485 or Ethernet which makes transmission compatible with old and new devices. After decades it is still a trustable way to create a link and it is free for use.

Modbus protocol operates between a client and a server however it can also be interpreted as master and slave. The client and master have the same function as server and slave for Modbus which can create confusion. They have not the same functions when the ARM-SE is configured because the slave and client are different devices. This will become clear later in the report when talking about the operation mode Modbus Gateway in 3.3.2. The protocol shows bits in hexadecimal which means that it exists out of blocks of 4 bits which go from 0 to F.

Many different protocol versions for serial and Ethernet exist. In this report the focus is on the Modbus RTU and Modbus TCP/IP [11].

Modbus TCP/IP

The name itself refers to a protocol that communicate over TCP/IP networks mostly over port 502. It was developed when Ethernet was introduced to profit of its benefits. TCP stands for Transmission Control Protocol while IP stands for Internet Protocol. Modbus TCP/IP is just an RTU command with an Ethernet TCP/IP wrapper.

A Modbus TCP/IP frame fabricated for a transaction is called the ADU, (Application Data Unit), which exists in two parts: the protocol data unit and the Modbus application header. Both parts create the message for the transaction.

The Modbus application header consist of 4 fields who all identify the message that needs to be send.

- Transaction identifier: This first field is to identify the sort transaction for the request or response and is projected in 2 bytes.
- Protocol identifier: This field contains also 2 bytes that indicates the used protocol for the transaction. To indicate the Modbus protocol, these bytes have the value ‘0’.
- Length: The 2 bytes who indicate the length are the number of bytes that are in the message following the last two identifiers.
- Unit identifier: This field contain a value between 0 and 255 to identify the slave connected to the modem. It is used to reach the right device while not reaching other devices.

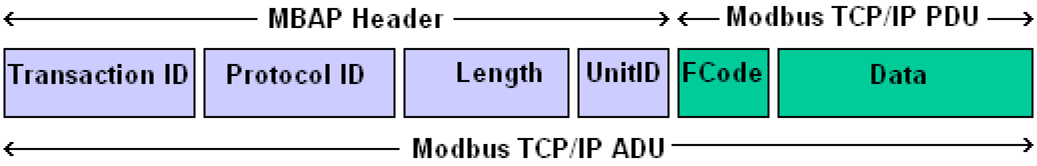


Figure 9 Frame of Modbus TCP/IP

Following the MBAP is the Modbus PDU, protocol data unit which exists of the function code and the actual data that needs to be send. The function code is to indicate the server which purpose the message contains and during this assignment it is ‘03’ which indicates on reading the holding registers [12].

Modbus RTU

Modbus RTU is an implementation for serial communication and is one of the most commonly used. RTU sends a message wrapped in a TCP packet over a network instead of a serial line. This means the MBAP is not included anymore because the server looks for the IP-address of the slave. It also features an error check before sending the data continuously. It is very common for communication in industrial control networks because there is a wide range of software that supports it.

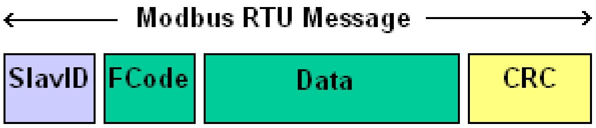


Figure 10 Frame of Modbus RTU

The similarity with the TCP frame is obvious but the differences are the 1 byte slave ID in front of the frame and the two bytes CRC at the back. The slave ID is to identify the slave so it needs to be the same value as the ID of the slave [12] [14].

2.1.4.3.1 **CRC**

Data corruption is a phenomenon that can occur when there is digital data sent or saved. This has been a problem since the start of the computer science and for serial data they found the solution in a parity bit after every byte. This solution can only be effective is there is odd chance of bits in a byte while a change of even bits will not be detected.

At the end of a Modbus RTU frame there are two bytes that serve as CRC, cyclic redundancy check. CRC is a solution that avoid the problem of data corruption by giving every data a checksum. After sending, the check values should match like before otherwise corruption occurred [13].

2.1.4.4 Operating principles

A connection between two or more modems can be achieved by two main configurations, which are both described below. During this assignment, both configurations were tested but the accentuation is on the principle that allows a larger number of devices to communicate. There are only two modems available to test these principles but it can be enlarged to communicate between lots of different industrial devices [9].

2.1.4.4.1 **Point to Point (P2P)**

This configuration is the simplest way to communicate between the modems because the data just has to go from one point to another. There are no other devices and modems involved besides the two original modems.

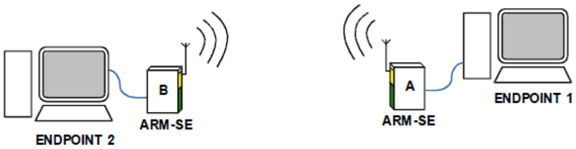


Figure 11 Point to point principle

2.1.4.4.2 **Point to multipoint**

The ‘point to multipoint’ configuration is split between two main functionalities, the access point and the clients. The Access point can interact with each client, together or separately, while the clients can’t communicate with each other. This principle is used to monitor different devices on one network which can be used in the industrial sector. In this assignment, there is only one client given the lack of more modems but it still can be a presentation of reality when using more devices.

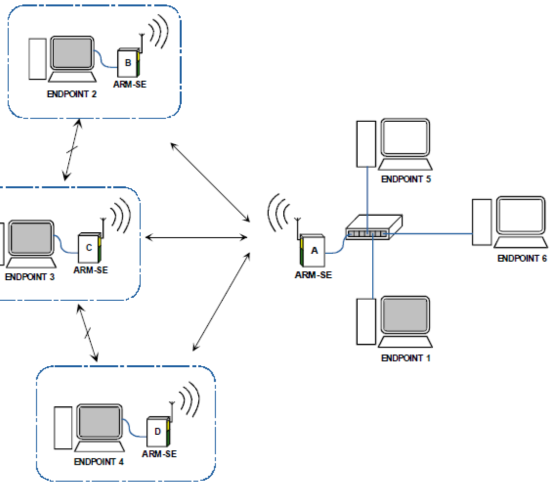


Figure 12 Point to multipoint principle

2.1.4.4.3 **Operating principle during assignment**

The setup in Figure 13 below creates the possibility to use both principles. For the Point to Point there are only two modems required but even for Point to Multipoint this setup can work. The following figure creates a visual image of the setup on which the remaining part of this report can rely.

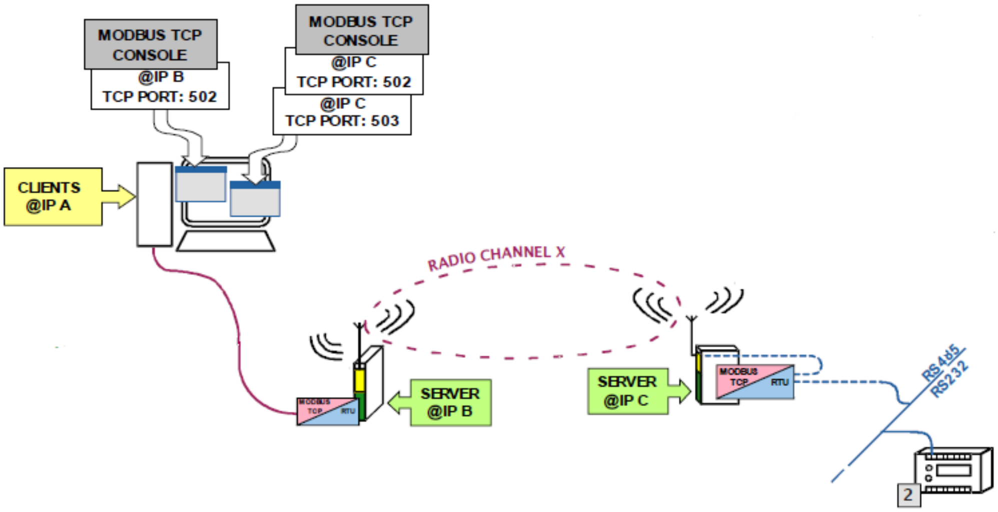


Figure 13 Diagram of the used operating system

2.1.4.5 Alerts

The webpages provide a system that can alert the person who uses the modem in case of emergency. The tab ‘Alerts’ gives the opportunity to detect an error and to warn the operator. Watchdogs are an integrated function that measures the time that no data are transferred to see if an error occurred. It also compares the number of bad packages compared to the total number of packages sent to analyze the quality of the signal during an operation.

With the tab ‘e-mailing’ the status of the watchdog can be sent to an e-mail address when certain triggers are activated. These triggers also can be adjusted in the settings on the webpage and depend on the status of the watchdog or the input and output of the modem.

2.2 Energy analyzers

2.2.1 CIRCUTOR CVM-MINI-CM

The attached slave used in the first part of the assignment, is the energy analyzer CIRCUTOR CVM-CM with integrated Modbus and is indicated in the picture Figure 14. The CVM-MINI used in GECAD is a programmable device used for measurements in electrical installations. It has a lot of different options to measure, calculate and display the main parameters for the most common electrical systems. It can be used in a three-phased, balanced or unbalanced industrial system. The CIRCUTOR can measures a lot of different parameters from basic frequency, current and voltage, harmonics and many more.

The datasheet of the analyzer with the functions of the analyzer can be found in the attached files. There is also a memory map on page 23 of the file with codes needed to get the data. It contains the registers for the Modbus connection. This device is chosen because a PLC also works with the Modbus protocol and then this device is a good indication for connecting a programmable logic controller [17].

Parameters to connect with Modbus:

- Serial interface: RS-485
- Transmission speed: 19200 bps
- Slave ID: 8
- Parity: NO
- Integer format: 8 bit

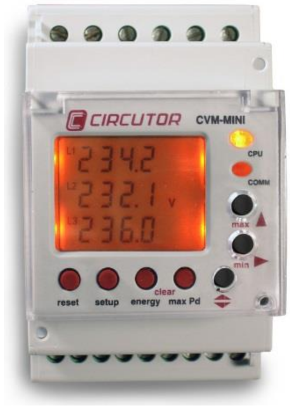


Figure 14 Power analyzer CVM-MINI

2.2.2 PM130 PLUS POWERMETER

The PLC is connected with 3 PM130 PLUS analyzers which are also a multifunctional 3-phase meter as the CVM-CM. The option of this analyzer are equal to the CIRCUTOR but the interface is better by means of the integrated LED screen. It is commonly integrated in panel boards who function with a SCADA system because of its intelligence in the power metering. It is operational with Modbus, IEC 60870-5-101/104 and I/O modules. The serial interface used by the analyzer is RS485 but the difference is located in the Modbus integer format which is, for the PM130, 16 bits or 32 bits. This means the analyzer will react on another type of request then the previous 8 bit [18] [20].

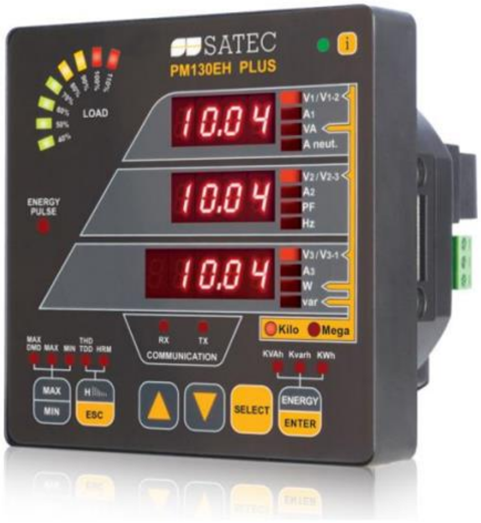


Figure 15 PM130 Analyzer

- Serial interface: RS-485
- Transmission speed: 19200 bps
- Slave ID: 2-4
- Parity: NO
- Integer format: 16-32 bit

2.3 SCADA System

SCADA, the abbreviation of Supervisory Control And Data Acquisition is a system to display and arrange measurements of control systems. It is a system that is integrated into the industrial sector because it creates an easy visualization and exchange of data for an operator. Furthermore, it can control the operations and warn the occupant when there is a problem in the system.

SCADA communicates with Ethernet RS232 or RS485 and runs on an extern computer and it can be created by a programmable logic controller. The software, downloadable from the site has a customizable interface which can operate a machine by writing data to the control unit, in this case, a PLC. This type of system can access the data of the analyzers through a PLC and display them in graph forms [15].

2.4 Matlab®

The system that serves as the SCADA system for this assignment can be reproduced as a program made in Matlab®. It is well-known in engineering facilities. It can be used both in industrial situations and for academic purposes given its mathematical and computer science complexity. It is the abbreviation of Matrix Laboratory and is already been used by GECAD to retrieve data through Modbus.

The purpose of using Matlab® is to create an own SCADA system. Via M-codes it is possible to create a program that can reach the IP-address of the extern network and transmit the needed data. With the Matlab® scripting language, this programming tool can access, manipulate and execute data requests.

The program will generate a request after connecting with the right IP-address to enable a response to be retrieved. In the Matlab® program this response can be recalculated and displayed in graphic formats for a specific time [16].

CHAPTER 3: Realization of communication

3.1 Introduction

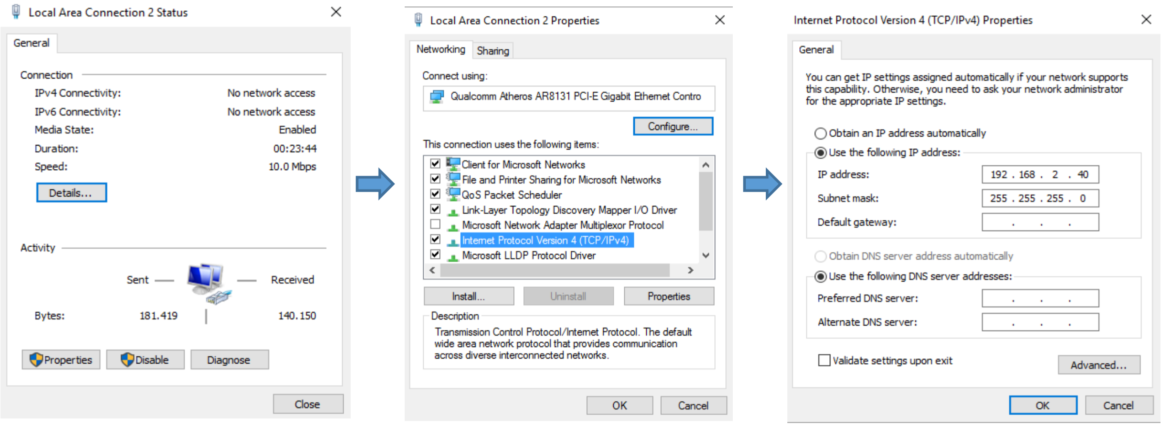
The overall task explained in the previous chapter is to connect two modems and ensure data transfer between both or create a remote for the PM130 analyzers of the PLC to be monitored and controlled from distance as a SCADA system. The two modems need to be configured and subsequently linked to each other before the start of the overall task. Following the configuration described in this chapter, some tests can be run to examine the radio signal. All the different operation modes will become clear in this chapter [9].

3.2 Configuration

The configuration can be accomplished using the webpages integrated in the software. Other possibilities are via SNMP firmware or Hayes AT-commands but these are not used in this report.

3.2.1 Adapter settings

To reach the embedded webpages of the modems, the IP-address of the external computer used, t link with the modem, has to use the same classification as the modems IP-addresses. This means that the third number in the IPv4-address must be the same which is zero in this case. In the network and sharing center, there is the possibility to change the IP-address. This functionality can be found in Figure 16 below the change adapter settings by selecting the local area connection, which refers to the modem. Under properties and after selecting the Internet Protocol Version which in this case was TCP/IPv4 the IP-address can be changed to the same class.



Connection

IPv4 Connectivity: No network access
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:23:44
Speed: 10.0 Mbps

Activity

Sent — — Received
Bytes: 181.419 | 140.150

Connect using:
Qualcomm Atheros AR8131 PCI-E Gigabit Ethernet Contro

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Microsoft LLDP Protocol Driver

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 2 . 40
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

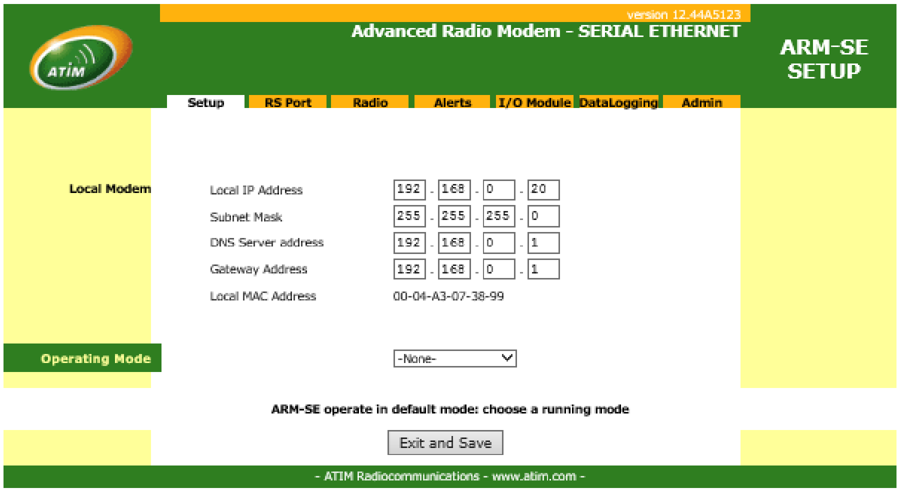
☐ Validate settings upon exit

Figure 16 Adapter settings to change IP-addresses

3.2.2 **Identification**

The first step in the process is to identify each modem that is part of the communication network, this to obtain perfect control over every device. It is important that each modem has a different identity to avoid miscommunication which can lead to serious problems. If there are only a few modems in the communication each of them can be given a different IP address. However, in case of too many devices to control this is not the best option. In case of a network with multiple modems it is best to create a main modem that functions as an access point with one IP-address. Then all the other modems, who function as clients, can be identified in the subnet created under the main modem's IP-address. This Point to Multipoint principle was not used in this assignment because of the lack of multiple modems, each modem could have its own IP-address.

To reach the embedded webpage of the ARM-SE, ATIM created an IP address which is reachable when the modem is connected to a network for the first time. In the memory of the modem the default IP address is'192.168.0.20', which links to the webpage in default mode when the IP address is not changed yet.



Local IP Address 192 . 168 . 0 . 20
Subnet Mask 255 . 255 . 255 . 0
DNS Server address 192 . 168 . 0 . 1
Gateway Address 192 . 168 . 0 . 1
Local MAC Address 00-04-A3-07-38-99
Operating Mode -None-

ARM-SE operate in default mode: choose a running mode

Figure 17 ARM-SE webpage to identify the modem

The local IP address is where one can change the default IP address to a new one. After changing the IP-address, the adapter settings need to chance again if the address belongs to another class. Otherwise the embedded webpages cannot longer be reached.

3.2.3 **IP-address**

The IP-addresses to identify the modems are chosen in function of the Point to Multipoint operating principle. From here on both modems are referred to as 'the access point' and the 'client' in this report.

The chosen IP addresses for the two modems, which are used for this assignment, are described below. It is important to know the address and their respective status to work without failure. For the Ethernet operation mode, cited in 2.1.4.1, another IP-address was given to the access point to create the data transfer.

IP address client (C):	192.168.0.20
IP address access point (B):	192.168.2.100 (normal)
	192.168.0.39 (Ethernet)

3.2.4 Remote connection

A modem can connect to every modem located within its range if the settings are configured in the same way for each of them. However in the settings there is the possibility to allow remote devices to manage inputs and outputs with only respective modem.

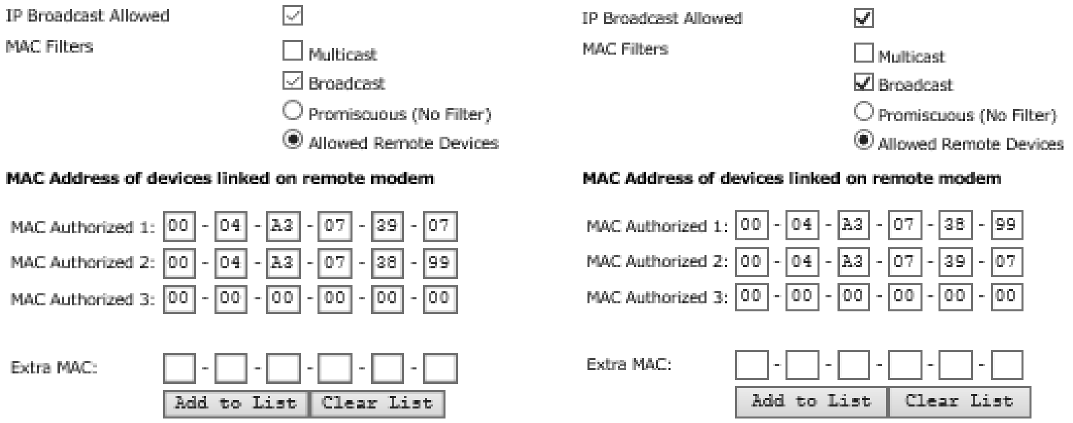
By linking the MAC addresses, a unique identification number for every device, on the remote modem, a filter in the network is created. In Figure 18 Identification using MAC-Addresses Point to Pointshown below are the LAN filters where the allowed MAC address of the necessary modems can be entered. This enables to optimize the data flow between the modems so they cannot interfere with data flow of the modems that are not selected.

MAC address of the respective modems by figure 13.

MAC address client (C):	00 04 A3 07 38 99
MAC address access point (B):	00 04 A3 07 39 07

3.2.4.1 Remote connection for Point to Point

The ‘MAC Authorized 1’ is the MAC address of the editable modem while MAC authorized 2 is the Mac address of the receiving modem. This is the same for the other endpoint, however the addresses are switched. So for Point to Point, the first address is always its own while the second belongs to the other respective modem.



IP Broadcast Allowed ☑
MAC Filters
□ Multicast
☑ Broadcast
○ Promiscuous (No Filter)
● Allowed Remote Devices

MAC Address of devices linked on remote modem

MAC Authorized 1:	00	04	A3	07	39	07
MAC Authorized 2:	00	04	A3	07	38	99
MAC Authorized 3:	00	00	00	00	00	00

Extra MAC: [ ] - [ ] - [ ] - [ ] - [ ] - [ ]

Add to List | Clear List

IP Broadcast Allowed ☑
MAC Filters
□ Multicast
☑ Broadcast
○ Promiscuous (No Filter)
● Allowed Remote Devices

MAC Address of devices linked on remote modem

MAC Authorized 1:	00	04	A3	07	38	99
MAC Authorized 2:	00	04	A3	07	39	07
MAC Authorized 3:	00	00	00	00	00	00

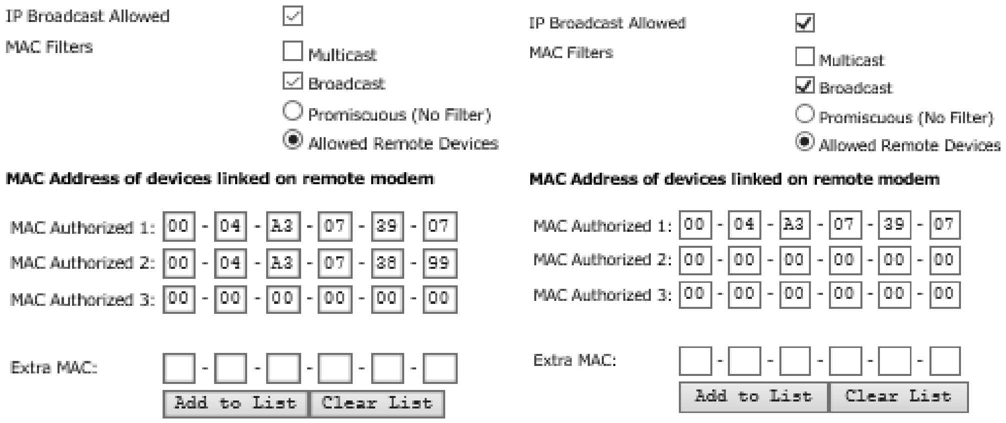
Extra MAC: [ ] - [ ] - [ ] - [ ] - [ ] - [ ]

Add to List | Clear List

Figure 18 Identification using MAC-Addresses Point to Point

3.2.4.2 Remote connection for Point to Multipoint

Using Point to Multipoint changes the receiving end of the transmission. A client can only receive with the access point and not reciprocally with the other clients while the access point can communicate with every client. This means that the access point needs to be linked to its own MAC address in the first row and the addresses of all the clients in the second and following rows. On the other hand every client only needs the MAC address of the access point. This is shown in Figure 19 below.



IP Broadcast Allowed ☑
MAC Filters
□ Multicast
☑ Broadcast
○ Promiscuous (No Filter)
● Allowed Remote Devices

MAC Address of devices linked on remote modem

MAC Authorized 1:	00	04	A3	07	39	07
MAC Authorized 2:	00	04	A3	07	38	99
MAC Authorized 3:	00	00	00	00	00	00

Extra MAC: [ ] - [ ] - [ ] - [ ] - [ ] - [ ]

Add to List | Clear List

IP Broadcast Allowed ☑
MAC Filters
□ Multicast
☑ Broadcast
○ Promiscuous (No Filter)
● Allowed Remote Devices

MAC Address of devices linked on remote modem

MAC Authorized 1:	00	04	A3	07	39	07
MAC Authorized 2:	00	00	00	00	00	00
MAC Authorized 3:	00	00	00	00	00	00

Extra MAC: [ ] - [ ] - [ ] - [ ] - [ ] - [ ]

Add to List | Clear List

Figure 19 Identification using MAC-Addresses Point to multipoint

3.3 Data transfer

The advanced radio modem is designed to communicate with different protocols. All these operating modes have a different advantage to use in an industrial connection network. In this section, all the possibilities are used to make a connection between the modems and on this basis, the most optimal connection to the SCADA system will be used to connect the modem to the supervisory network. There is also the possibility to run a test to check the radio link between both modems. It is recommended to run these tests first before testing the operating modes [9].

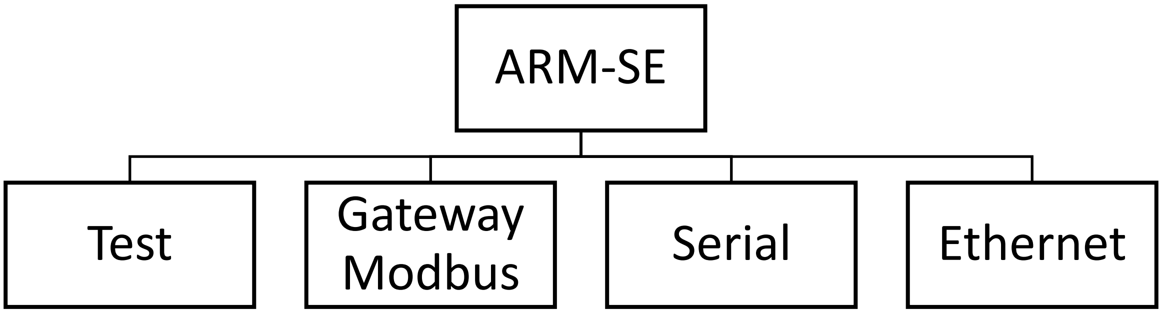


Figure 20 Flowchart of used operation modes

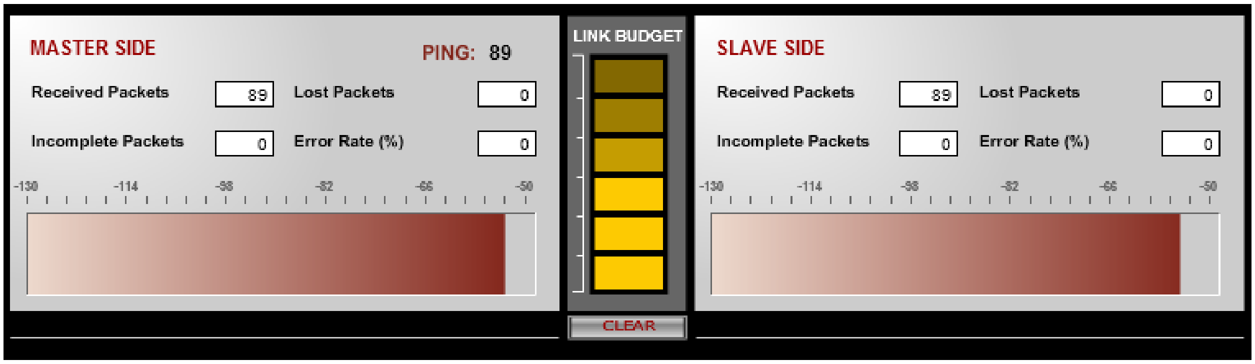
3.3.1 Test mode

There are different possibilities to run the tests to examine the connection between the two modems but the most obvious in this situation is by using the test mode integrated in the embedded webpages. Before the tests can be started, both modems need to be interconnected as described in the configuration in 3.2, so only their mutual connection can be monitored.

There are three different tests to check the quality of the radio transmission between the modems which are described and applied for the connection between the two modems.

3.3.1.1 Ping-Pong mode

This mode checks the quality of the communication by sending packages of information from the master to the slave modem. By setting the status of slave to one modem and master to another, this test shows how many packages were received and how many packages were lost. A perfect connection has no losses of packages and maintains a stable connection. In this particular situation the access point modem is serving as the master while the client has the role of the slave.



MASTER SIDE PING: 89

Received Packets 89 Lost Packets 0

Incomplete Packets 0 Error Rate (%) 0

SLAVE SIDE

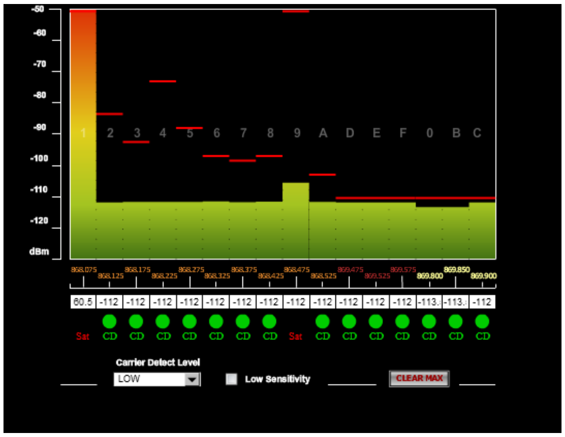
Received Packets 89 Lost Packets 0

Incomplete Packets 0 Error Rate (%) 0

Figure 21 Ping-Pong test

3.3.1.2 Spectrum analyzer

This test shows an interface with all the ARM-SE spectrums available on the modem. The graphic gives the information which of the channels are in use and allows to detect when there is an interference with other connections. The interpretation of the test, ran in Figure 22 below, displays the use of channel 1 while the other channels are unused. This test has to indicate the same channel for all the modems who need the same connection otherwise both modems are not on the same channel or there is interference.



60.5	-112	-112	-112	-112	-112	-112	-112	-112	-112	-112	-112	-112	-113.	-113.	-112
Sat	CD	CD	CD	CD	CD	CD	CD	Sat	CD	CD	CD	CD	CD	CD	CD

Carrier Detect Level: LOW

□ Low Sensitivity

Figure 22 Spectrum analyzer

3.3.1.3 Carrier emission

This test sends a ‘pure’ carrier signal, which is a transmitted signal with no modulation. The carrier emission test is executed to see if the modem can transmit a clean radio wave during 30 seconds.

3.3.2 Sending data with Modbus protocol

The situation represented in Figure 23 is the main situation for Point to Multipoint communication using only one client. This is already described in 2.1.4. The first way to communicate is to attach a slave to the client modem, working with the Modbus protocol. The slave used during this operation is the CIRCUTOR energy analyzer in 2.2.1. Modem B will try to access the data trough radio, given to modem C by the slave. The next pages contain the setting for both modems to establish the transmission with Modbus. Following these settings, two examples are elaborated where the access point modem B communicates with the CIRCUTOR. The response of the first example consist of a hexadecimal code that refers to the voltage between a line and the neutral of an energy analyzer. The second example contains the temperature of the analyzer. At the end, the hexadecimal code will be convert to decimal numbers to get the actual data.

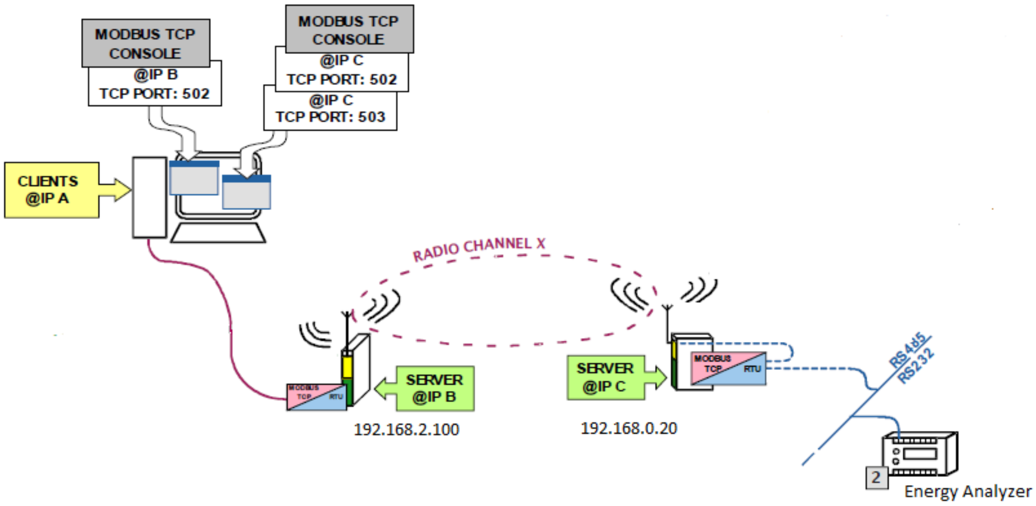


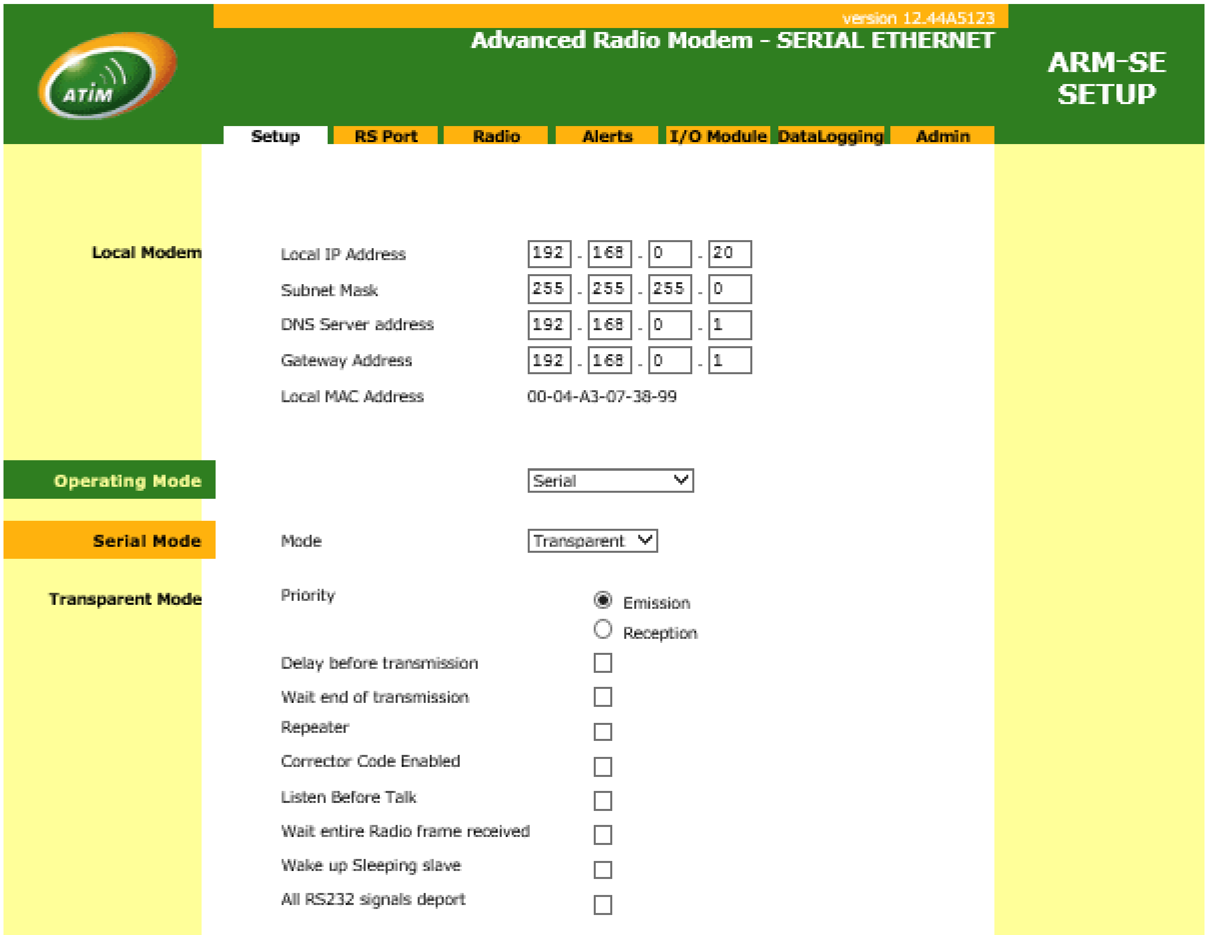
Figure 23 Diagram of the used operating system

In Figure 23, the IP-addresses are displayed to clarify the setup while the used energy analyzer is the CIRCUTOR.

This paragraph contains in the end also the program to connect with the CIRCUTOR using Matlab®. There is a review of the program with a graphical form of the voltage to show the operation.

3.3.2.1 Settings Modem client

To accomplish the link between both modems the used operating mode is the first difficult choice. The client Modem C (192.168.0.20) operates in the serial operating mode where it is in transparent mode. In the transparent mode only the physical data is managed which means that every byte will be copied to the receiving modem without an error check. For this mode to work there needs to be a communication protocol which in this case is the Modbus of the energy analyzer.



Local Modem

Local IP Address 192 . 168 . 0 . 20
Subnet Mask 255 . 255 . 255 . 0
DNS Server address 192 . 168 . 0 . 1
Gateway Address 192 . 168 . 0 . 1
Local MAC Address 00-04-A3-07-38-99

Operating Mode: Serial

Serial Mode — Mode: Transparent

Transparent Mode

Priority ● Emission ○ Reception
Delay before transmission □
Wait end of transmission □
Repeater □
Corrector Code Enabled □
Listen Before Talk □
Wait entire Radio frame received □
Wake up Sleeping slave □
All RS232 signals deport □

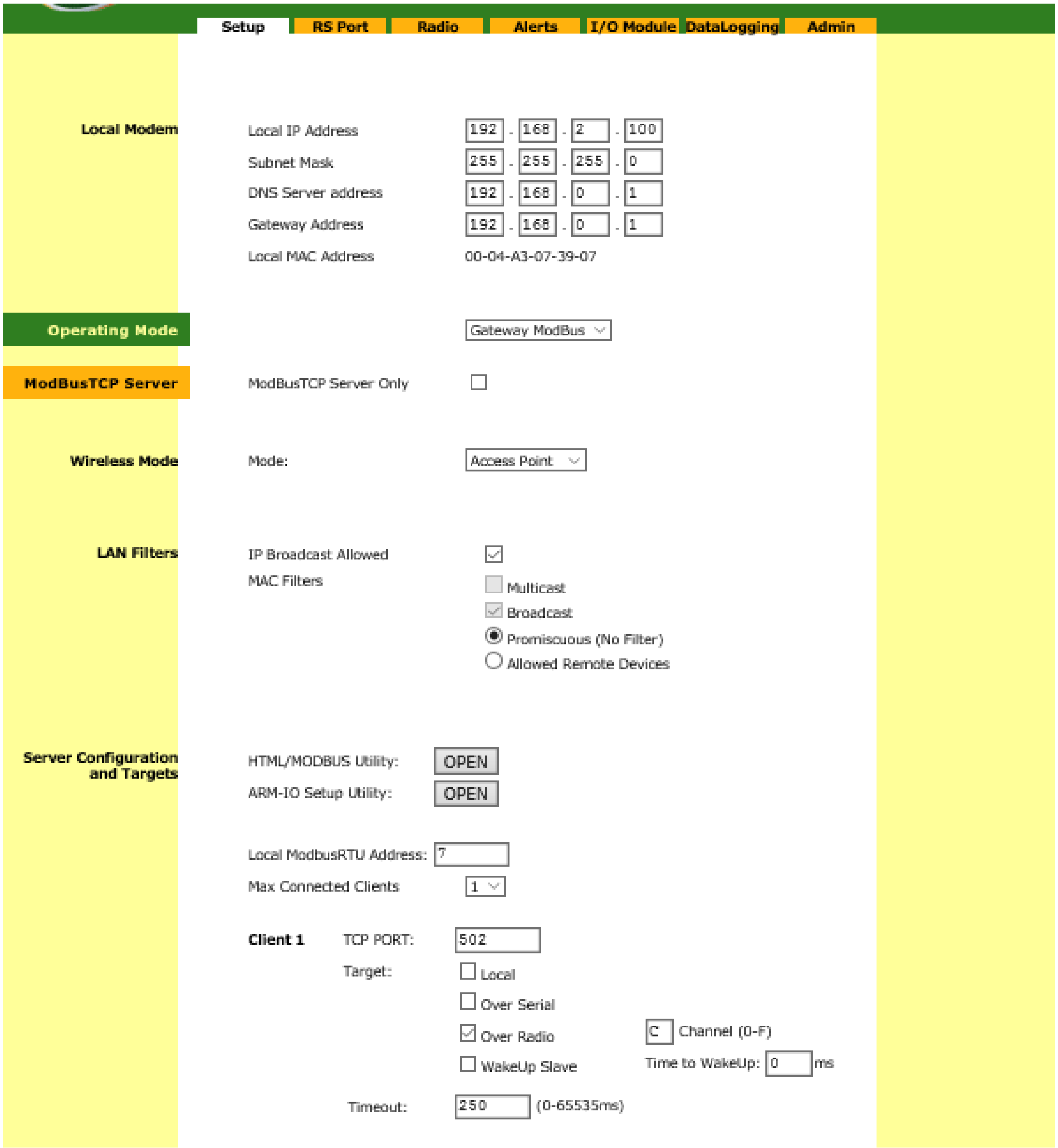
Figure 24 Client with Serial operation mode

The settings in transparent mode obtain a priority, which either is emission or reception depending on the function of the modem. During this operation Modem C has to have priority of emission so it can sends the data of the energy analyzer to the access point.

The other settings serve to specific situations which can occur during a transmission process. When needed, the user can check the most obvious setting. The repeater is a setting that is necessary to use if the reception is bad because of the reliability of a radio transmission. These settings are analyzed in this report and can be found in the attached file [8].

3.3.2.2 Settings Modem access point

The access point modem (192.168.2.100) has to be in the gateway Modbus operating mode to access the data sent by the client. The wireless mode is configured to the access point because of the status of the modem. There is only one client to communicate with and this target can be reached by using radio waves on a chosen channel.



Local Modem

Local IP Address: 192 . 168 . 2 . 100
Subnet Mask: 255 . 255 . 255 . 0
DNS Server address: 192 . 168 . 0 . 1
Gateway Address: 192 . 168 . 0 . 1
Local MAC Address: 00-04-A3-07-39-07

Operating Mode: Gateway ModBus

ModBusTCP Server: ModBusTCP Server Only □

Wireless Mode: Mode: Access Point

LAN Filters

IP Broadcast Allowed ☑
MAC Filters
□ Multicast
☑ Broadcast
● Promiscuous (No Filter)
○ Allowed Remote Devices

Server Configuration and Targets

HTML/MODBUS Utility: OPEN
ARM-IO Setup Utility: OPEN

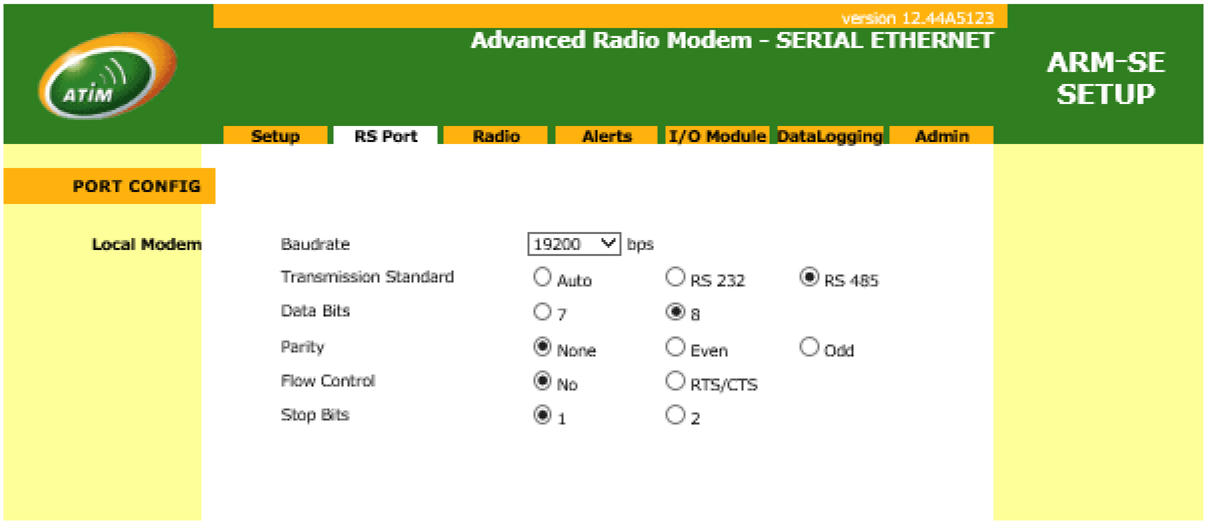
Local ModbusRTU Address: 7
Max Connected Clients: 1

Client 1 TCP PORT: 502
Target:
□ Local
□ Over Serial
☑ Over Radio — C Channel (0-F)
□ WakeUp Slave — Time to WakeUp: 0 ms
Timeout: 250 (0-65535ms)

Figure 25 Access point with Modbus Gateway

3.3.2.3 Settings RS Port

Both modem need synchronized settings with the serial slave or energy analyzer otherwise there will not be any connection. This means that the baud rate (bits per second), transmission standard, data bits and parity should have the same value for both devices. The value of these parameters can be found in the analyzer's settings and for the modems you can change them under the tab RS Port. The power analyzer is connected to the RS 485 gate on the client modem which means that this value for the 'Transmission Standard' should be indicated. In Figure 26 the other settings are given for this particular transfer between the energy analyzer and the modems.



Local Modem

Baudrate 19200 bps

Transmission Standard ○ Auto ○ RS 232 ● RS 485

Data Bits ○ 7 ● 8

Parity ● None ○ Even ○ Odd

Flow Control ● No ○ RTS/CTS

Stop Bits ● 1 ○ 2

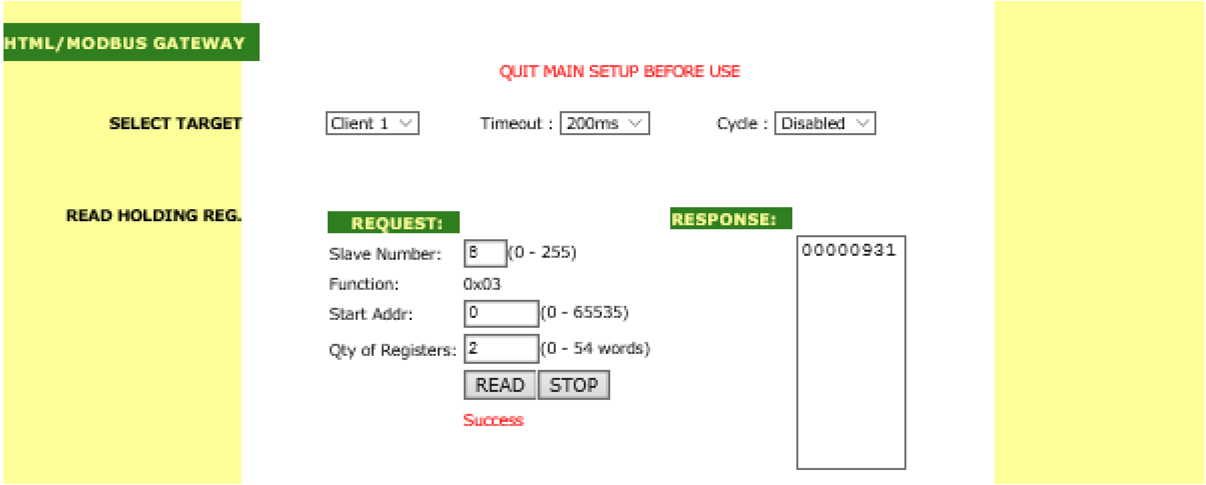
Figure 26 Settings RS-port

3.3.2.4 Examples

As a next step it is required to open de html/Modbus Utility on the setup page of the access point modem and fill in the request to create a response from the energy analyzer. Number 8 is chosen as the slave number, which corresponds with the settings of the energy analyzer. The start address is the value of the memory map where the modem starts to read the values. The 'quantity of registers' is the number of values the modem will read starting of the start address, the first register. The examples below are executed to obtain the voltage between the first line and the neutral and for the temperature of the analyzer.

To reach the voltage the start address must be 0 which can be found in the memory map 7.2.After pressing the 'read' button the modem will create a hexadecimal response which can then be translated to a mathematical number system. With the 'quantity of registers' the number of measurements can be adjusted to the wanted value.

3.3.2.4.1 **Example voltage**



HTML/MODBUS GATEWAY

QUIT MAIN SETUP BEFORE USE

SELECT TARGET Client 1 Timeout : 200ms Cycle : Disabled

READ HOLDING REG.

REQUEST:

Slave Number: 8 (0 - 255)

Function: 0x03

Start Addr: 0 (0 - 65535)

Qty of Registers: 2 (0 - 54 words)

READ STOP

Success

RESPONSE:

00000931

Figure 27 Response of example voltage

Response: 00000931 is translated into decimal number 2353.

PARAMETER	SYMBOL	Instant	Maximum	Minimum	Units
Voltage phase	*V L1*	00-01	60-61	C0-C1	*V x10*

Table 1 Register of voltage of the power analyzer

The response is the voltage between phase 1 and the neutral, which means after the recalculation with the given units, this can be interpreted as 235,3V. This value is about the 230 - 240V it should be shown in Figure 28.

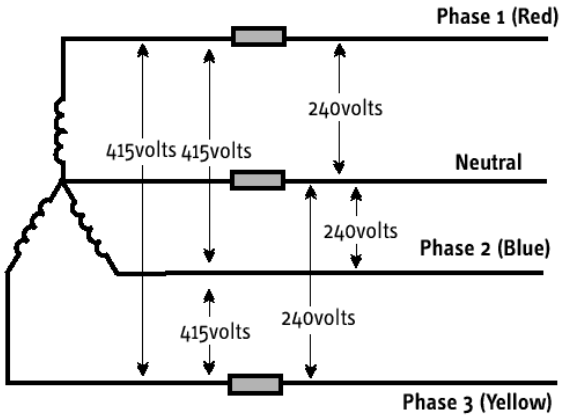
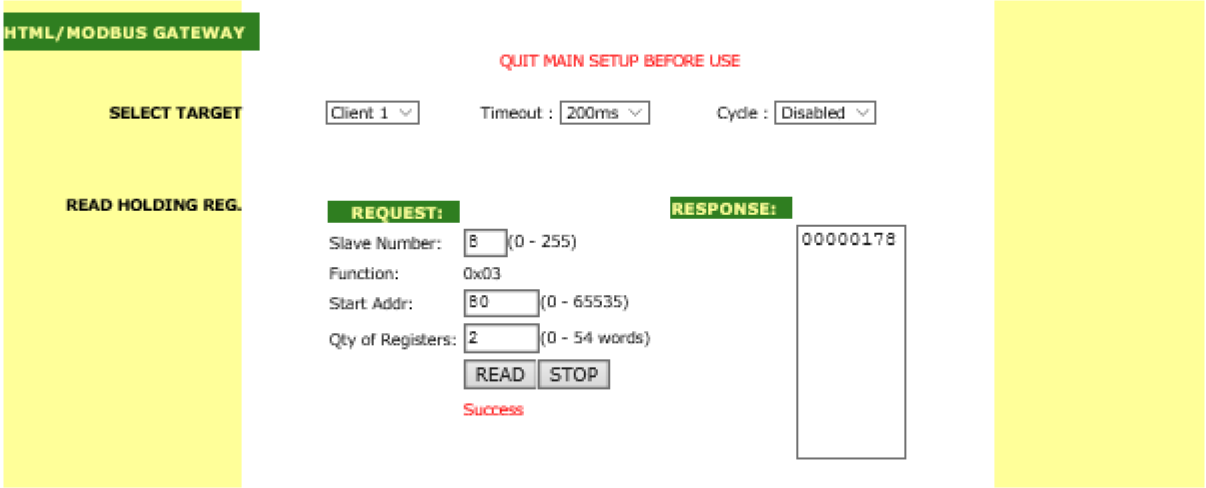


Figure 28 Three phase Star connection

3.3.2.4.2 Example temperature


HTML/MODBUS GATEWAY

QUIT MAIN SETUP BEFORE USE

SELECT TARGET: Client 1 | Timeout : 200ms | Cycle : Disabled

READ HOLDING REG.

REQUEST:

Slave Number: 8 (0 - 255)

Function: 0x03

Start Addr: B0 (0 - 65535)

Qty of Registers: 2 (0 - 54 words)

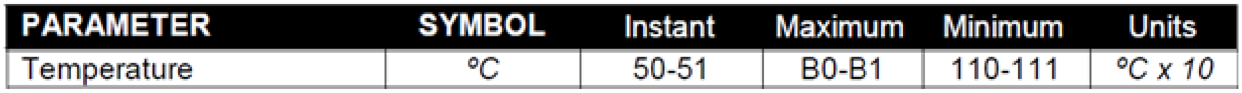
Success

RESPONSE:

00000178

Figure 29 Response of example temperature

Response: 00000178 is translated into decimal number 376.



PARAMETER	SYMBOL	Instant	Maximum	Minimum	Units
Temperature	°C	50-51	B0-B1	110-111	°C x 10

Table 2 Register of the temperature of the power analyzer

The measurement is the temperature in the energy analyzer after the recalculation with the given units. This can be interpreted as 37,6 °C after calculation.

3.4 Algorithm to retrieve data

The purpose of this program is to access the data of a device and display it in a graphical form to monitor the situation of the PLC. Over a time lapse of 30 seconds a request for data is generated every 0,5 seconds and all the values of the responses are displayed in the graph. This creates a reliable view of the surroundings with which the analyzers have to deal.

The first program is designed to access the data of the power analyzer and after that the program can be adjusted to access the PM130 next to the PLC. At first it is the basic request for the voltage of the analyzer but this can be extended later to request more data. If the program runs successfully for the analyzer it can work for the PLC after adapting the message send by the program.

3.4.1 Program in Matlab®

The code can be found in the appendix 7.4.

Line 0-12

Before starting the program, all the windows of previous runs need to be closed. The next step is to define the fixed inputs of the time, step time and the addresses. The addresses can be found in the datasheet of the analyzer and as previously said the address of the voltage is ‘00’. This means that the program will only look for this address on the analyzer but the program can be adapted so more addresses can be reached.

Line 13-25

Next are the lines of code that arrange the addresses and responses in arrays for storage. That is necessary to create the graphical forms.

Line 25-29

Thereafter is the configuration of the TCP/IP channel in which the IP-address and port of the TCP/IP need to be identified. In this case the IP-address is 192.168.0.39 and the port for TCP/IP should be 502.

Line 29-51

After the configuration the connection can be opened with the IP-address using ‘t=*tcpip(IPADDR_, PORT)*’. In the program there is also a loop included to check the status of the connection and to display if the connection is open or not.

Line 51-80

The next section is the assembling of the message that is sent to the analyzer. Just like using the Arduino the sent message needs to obtain certain parameters to find to right data. The parameters to create the messages are already explained in paragraph 2.1.4.3.

Transaction ID:	03
Protocol ID:	00
Bytes remaining:	06
Slave ID :	8
Function ID:	3
Starting register:	00
Number of registers to read:	02

Table 3 Modbus parameters message to analyzer

Line 80-90

When the message is created it can be written on the analyzer and with the read function the response can be found. The received response needs to be transformed in a decimal response by using the command ‘bitshift’. The result of this transformation must be divided by 10 to get the actual voltage which is exactly the same calculation used in paragraph 3.3.2.4.1.

Line 90-97

After the response is received and transformed into the right value the graphs is created. The created values are stored in different arrays, which makes it easy to locate them. The run is also closed here using ‘fclose(t)’.

Line 97-133

The graph is created by opening a window in the first loop with the titles, color, etc.. Subsequently all the values will be displayed by using subplots.

The created graph of the voltage L1 of the analyzer is shown below in a time-lapse of 30 seconds.

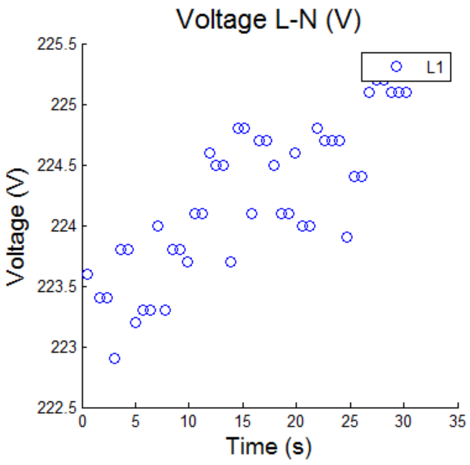


Figure 30 Graph of the L-N voltage retrieved of the power analyzer

In Figure 30 the voltage between phase 1 and the neutral is displayed during 30 seconds. It fluctuates between 222,5 and 225,5V.

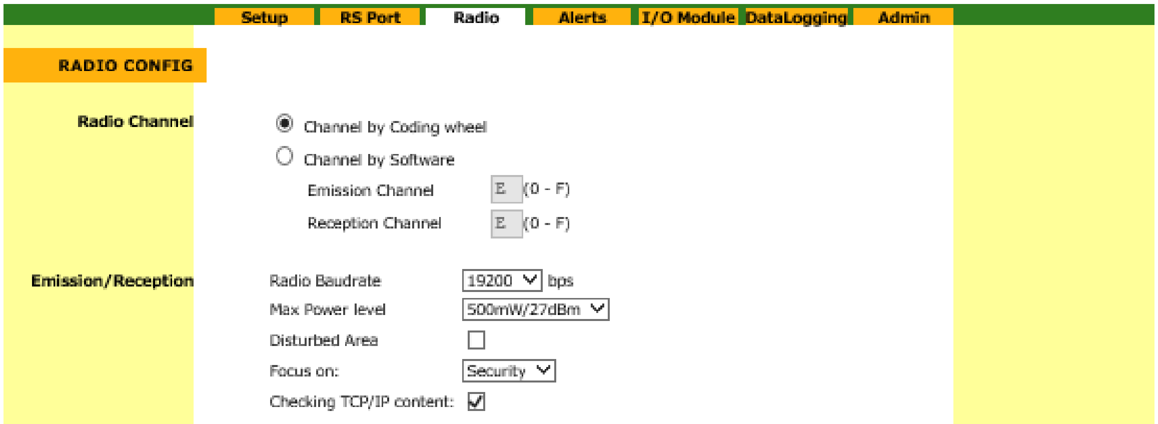
3.4.2 Sending data with Ethernet

3.4.2.1 Settings

This paragraph describes how to create a link in the Ethernet operating mode between the two modems. Because there is no interface available for the Ethernet operation mode it is difficult to create a request and response. Using the command prompt of an extern computer, attached to the modem for this case, a simple PING-signal is transmitted to test if there is a good transmission. If the transmission is succeeded, a request could be fabricated on an external interface but this is not available in GECAD which means only the PING-test is executed in this report.

It is important for using the Ethernet mode that both modems are of the same class. In this case both modems are part of the class: 192.168.0…. . The client remains 192.168.0.20 while the access is changed to the free IP address 192.168.0.39 using the adapter settings in the paragraph configuration 3.2. When both modems are ready the Ethernet tab in the operation mode can be selected via the webpages. Both modems require the same settings when the wireless mode is Point to Point. There is a different setting using Point to Multipoint because the access point has priority over the clients.

Before the connection can succeed, the radio configuration (Radio tab) also requires to be set for the emission and reception of a signal. In the Ethernet operating mode the data transfer has the possibility to give priority to speed or security. Security uses ‘RTS/CTS (request to send / clear to send)’, while priority of speed does not need the access. It is recommended to use the security option except when the response time is more important.



RADIO CONFIG

Radio Channel
● Channel by Coding wheel
○ Channel by Software
Emission Channel E (0 - F)
Reception Channel E (0 - F)

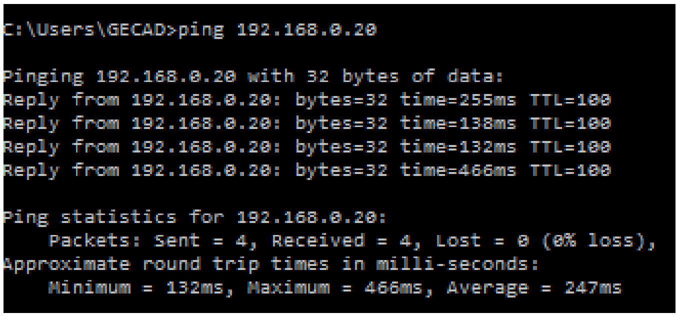
Emission/Reception
Radio Baudrate 19200 bps
Max Power level 500mW/27dBm
Disturbed Area □
Focus on: Security
Checking TCP/IP content: ☑

Figure 31 Radio configuration

3.4.2.2 Example

To test the created link between the modems, a PING can be sent from one to another to check if it is received. This resembles the ping-pong test in the test mode. The PING is sent with the command prompt, available on the computer. The transmission is tested by typing 'Ping' followed by the IP address of the receiving modem, by example 'PING 192.168.0.20'.

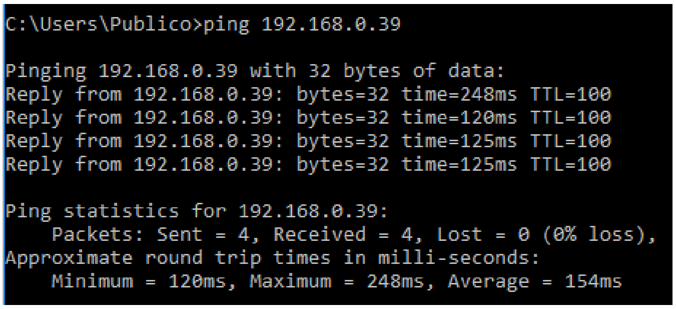
In Figure 32 the PING test from the access point looking for the IP address of the client modem is shown.



```
C:\Users\GECAD>ping 192.168.0.20

Pinging 192.168.0.20 with 32 bytes of data:
Reply from 192.168.0.20: bytes=32 time=255ms TTL=100
Reply from 192.168.0.20: bytes=32 time=138ms TTL=100
Reply from 192.168.0.20: bytes=32 time=132ms TTL=100
Reply from 192.168.0.20: bytes=32 time=466ms TTL=100

Ping statistics for 192.168.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 132ms, Maximum = 466ms, Average = 247ms
```

Figure 32 Ping test with client

All sent packages are received which indicates to a perfect connection between both. In the next Figure 33 the same PING test is executed, but the packages are sent from the client to look for the IP address of the access point modem.



```
C:\Users\Publico>ping 192.168.0.39

Pinging 192.168.0.39 with 32 bytes of data:
Reply from 192.168.0.39: bytes=32 time=248ms TTL=100
Reply from 192.168.0.39: bytes=32 time=120ms TTL=100
Reply from 192.168.0.39: bytes=32 time=125ms TTL=100
Reply from 192.168.0.39: bytes=32 time=125ms TTL=100

Ping statistics for 192.168.0.39:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 120ms, Maximum = 248ms, Average = 154ms
```

Figure 33 Ping test with access point

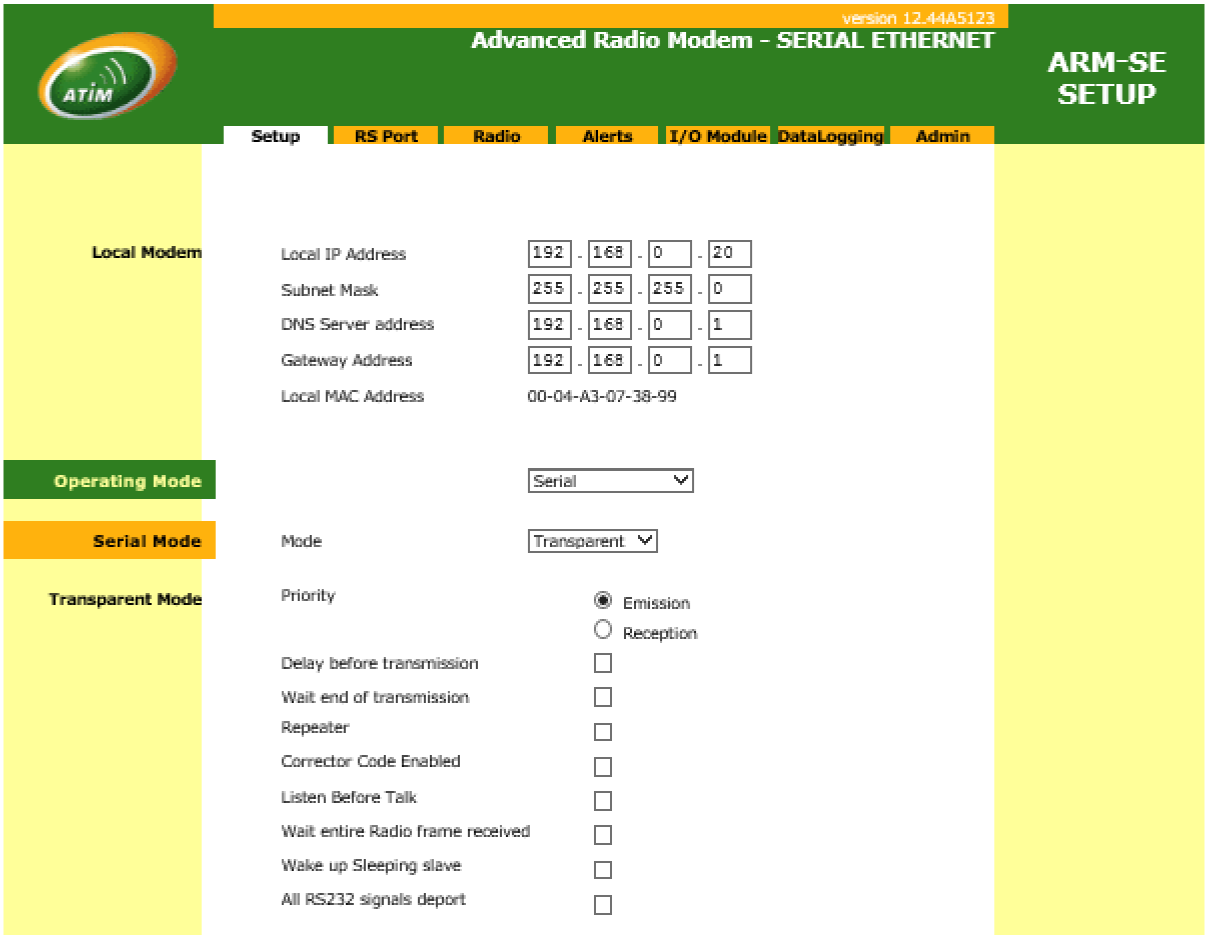
The figure makes shows that also the sent packages are received without failure. These packages are sent in both Point to Point and Point to Multipoint with the same result. But the small change applied to the settings of the MAC addresses needs to be remembered as this is crucial for success.

3.4.3 Sending data with serial

To test the serial operation mode an Arduino is used to create an interface. Arduino is an open source computer hardware and software company which designed a platform to ease the use of microcontrollers. The platform can create occupants that can react in a system by means of input and output signals. In this case the Arduino can reach the input by serial interface of the power analyzer and send an output the other way around. The device is connected to the access point which is connected to a computer. With a program it is possible to access the data of the analyzer and furthermore the PM 130 analyzers of the PLC.

3.4.3.1 Settings of modems

It is known that in the configurations in previous paragraph 3.2 the CIRCUTOR uses Modbus RTU and TCP/IP. Both can only be linked using the serial mode of the modem. The Arduino also uses Modbus RTU, which is the same configuration as the analyzer. Figure 34 shows the configuration of the client and it is obvious that the settings for both the Arduino and the analyzer are the same.



Local Modem

Local IP Address 192 . 168 . 0 . 20

Subnet Mask 255 . 255 . 255 . 0

DNS Server address 192 . 168 . 0 . 1

Gateway Address 192 . 168 . 0 . 1

Local MAC Address 00-04-A3-07-38-99

Operating Mode Serial

Serial Mode — Mode Transparent

Transparent Mode — Priority ● Emission ○ Reception

Delay before transmission □

Wait end of transmission □

Repeater □

Corrector Code Enabled □

Listen Before Talk □

Wait entire Radio frame received □

Wake up Sleeping slave □

All RS232 signals deport □

Figure 34 Settings of both modems with the serial operation mode

In transparent mode, it is important to consider the transmission delay and end of transmission waiting times. This can enable a radio frame “hole” phenomena that needs to be avoided. For example, for a serial link rate of 2400 bps, without the use of delays, the modem sends each byte separately in each radio frame.

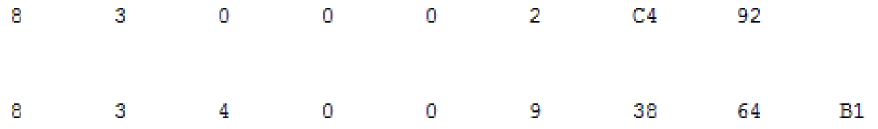
3.4.3.2 Example

The Arduino is used to check the communication link between the modems by reaching out for data on the energy analyzer. By sending a request with the Arduino to the analyzer, over the modem’s radio, a response will be generated. A program is required to retrieve this information and fabricate a request and thereafter the response can be received.

Because the Arduino operates on the Modbus RTU principle there needs to be two bytes of the CRC, Cyclic Redundancy Check at the end of the request cited in paragraph 2.1.4.3.1. The CRC configuration for the Arduino is shown below can be calculated on-line [19].

080300000002 → CRC-16 (Modbus) **0x92C4**

The used program can be found in the appendix 7.1. The request is created to access the analyzer however the settings need to be configured equal to the device. Which means the baud rate is 19200 bps and the devices need to operate with an 8 byte message. The slave ID has the value ‘8’ which matches the value of the analyzer.



Request	→	8	3	0	0	0	2	C4	92	
Response	→	8	3	4	0	0	9	38	64	B1

Table 4 Request and response produced with the Arduino

The first line is the request sent by the Arduino while the second line is the responds of the analyzer received by the Arduino received. After conversion of the hexadecimal 938 to decimal numbers the response is: 236,0V. The recalculated voltage is equal to the voltage using the Modbus Gateway mode in 3.3.2.4.1.

CHAPTER 4: SCADA system for building monitoring

4.1.1 Introduction

The main task of this report is to connect an external electrical building to the SCADA system of GECAD. In Figure 35 the process is displayed on how the data of the analyzers can be reached by the SCADA network. The SCADA network is connected with the computer which is connected to the GECAD network. Communication with the analyzers can be achieved by using the modems on the Modbus gateway operation mode explained in paragraph 3.3.2.

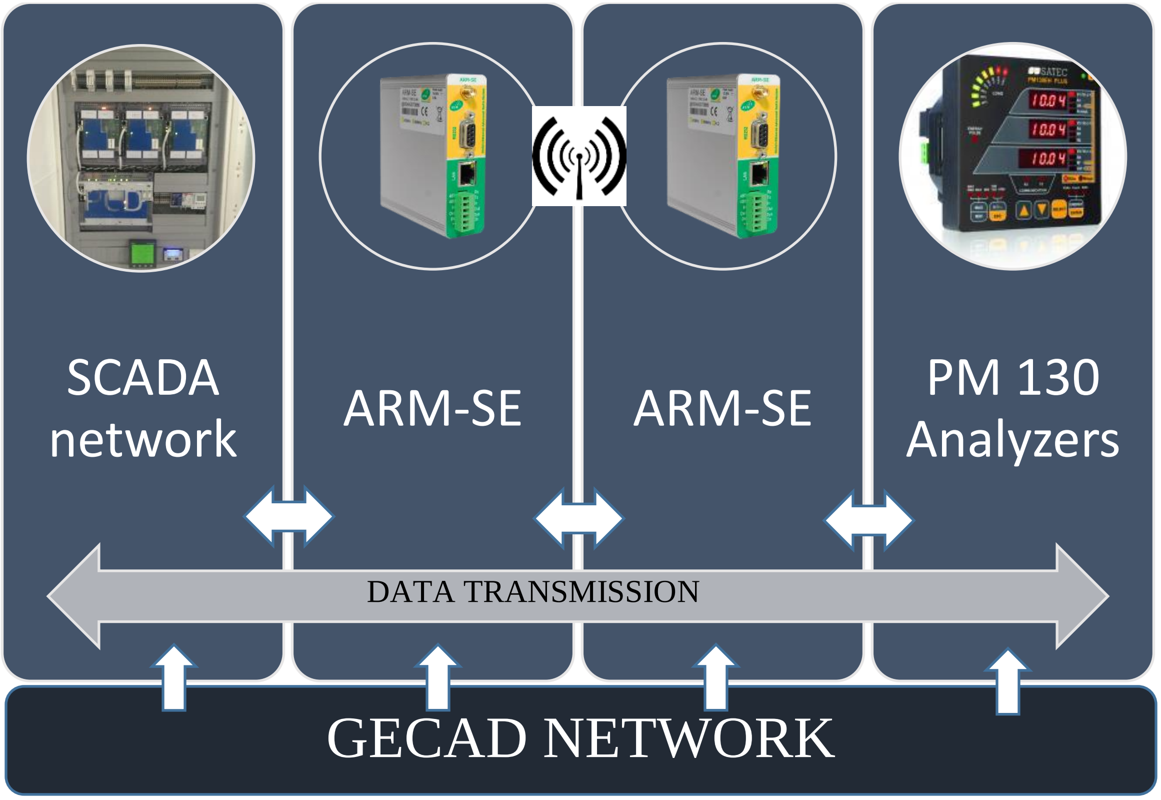


Figure 35 Flowchart of SCADA process

Using this process, creates the possibility to monitor the analyzers in another building. The SCADA system will monitor all the necessary data by sending requests continuously. The response will be translated and monitored to control the installations.

The last step in the process is to access the data response trough a PLC in the GECAD laboratory with the computer to create the SCADA system. In the software of the PLC is shown which accesses the data and send it to a SCADA webpage, created by the PLC. The Client is identified and the message created to access the data on the left side while the response, the three phase voltages, is shown on the right in Figure 36.

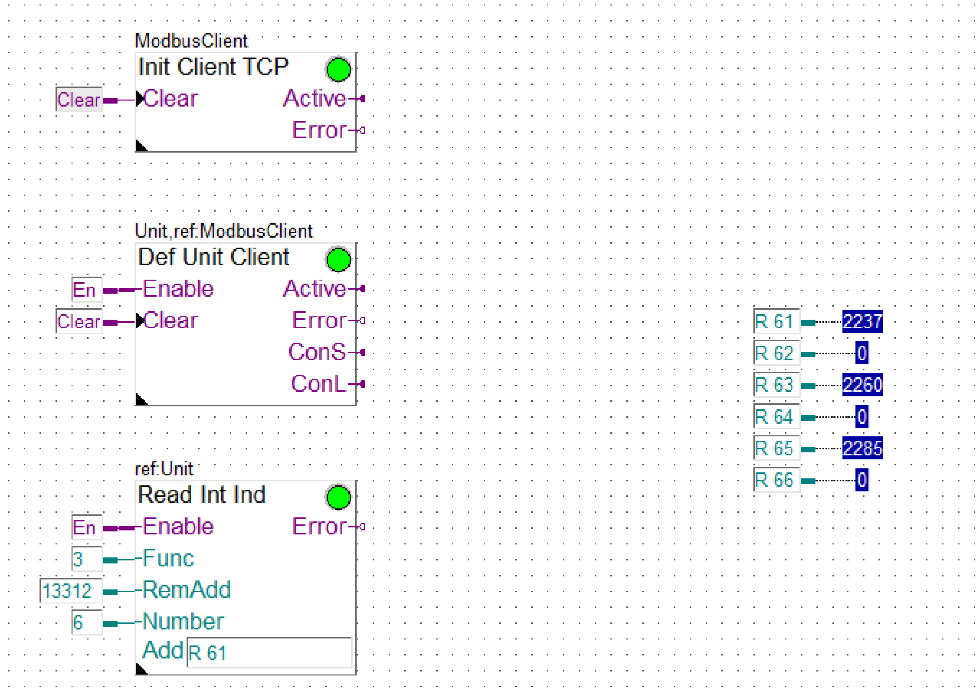


Figure 36 PLC program to access data for SCADA

4.1.2 Changes to retrieve data of PM130

To create a link with the PM130 analyzers the request described in the previous paragraph needs to be transformed, despite the fact that both analyzers use the same protocol, the settings are different. The differences between the analyzers are shown below.

- The messages send to the PLC are made out of 16 or 32 bits which is more than the 8 bit request of the CIRCUTOR.
- Port changes from 502 to 5502.
- The IP address is also changed because of errors that occurred during the assignment. The new address for this program is 192.168.2.144.
- The used registers can be found in the appendix and are totally different comparing to the registers of the energy analyzer.

The SCADA system for the PLC uses the same method to extract data but the differences with the program for the CIRCUTOR shown above change the request a lot. Not only need the settings to be modified but also the amount of registers that will be accessed, are increased. Instead of collecting data from one register, this program needs to collect all of them and display them in graphs. This means the period and interval need to be chosen carefully to collect all the data so no error can occur. If there are too many requests in a small time-lapse the data will not be received anymore or it will lead to data corruption.

CHAPTER 5: Case study

5.1 Situation

The main aim of this report is to use the ARM-SE to integrate the data of an external building into the SCADA system in the GECAD laboratory. This means, creating a data transmission between the research lab and PM130 analyzers located in another building to monitor the installation. The analyzers are connected to a PLC and measure the electrical installation of the building. The modems want to retrieve that data to monitor the building. The PLC is situated in the F-building and can be reached using an antenna and the client modem. The testing of every operation mode has been described in the previous paragraph 3.3. The most suitable modes and parameters have been selected in view of achieving the best transfer. First the created program in described in 0 is used to extract data of the power analyzer to check the quality of the transmission. Subsequently the CIRCUTOR is changed with the connection of the PM130 analyzers of the PLC to fulfill the assignment by collecting data of the electrical installation [20].

5.2 Location

The research lab of GECAD is located in the N-building on the most southern point of the campus of ISEP. The access point modem is installed at this location. The PLC is located on the 4th floor of the F-building which is located next to the lab. At both locations the modem and antenna are installed and tested to verify that a connection is possible. The only obstacles are the threes located between the two buildings that can hinder a transmission.

Before the actual installation the antennas are placed in both buildings and the test needs to be successful before it is possible to transmit data between the two locations. The test consists of a request to the client using the Modbus Gateway mode. If the access point receives the requested data, this indicates that the antennas are in the right place. As described in paragraph 3.3.2 the request and the corresponding response were generated successfully from the CIRCUTOR power analyzer indicating a successful connection. This test is executed with the power analyzer CVM-MINI as this is the most efficient way to retrieve data.

The modem located in GECAD needs to be connected to the network to be accessable in the whole laboratory.

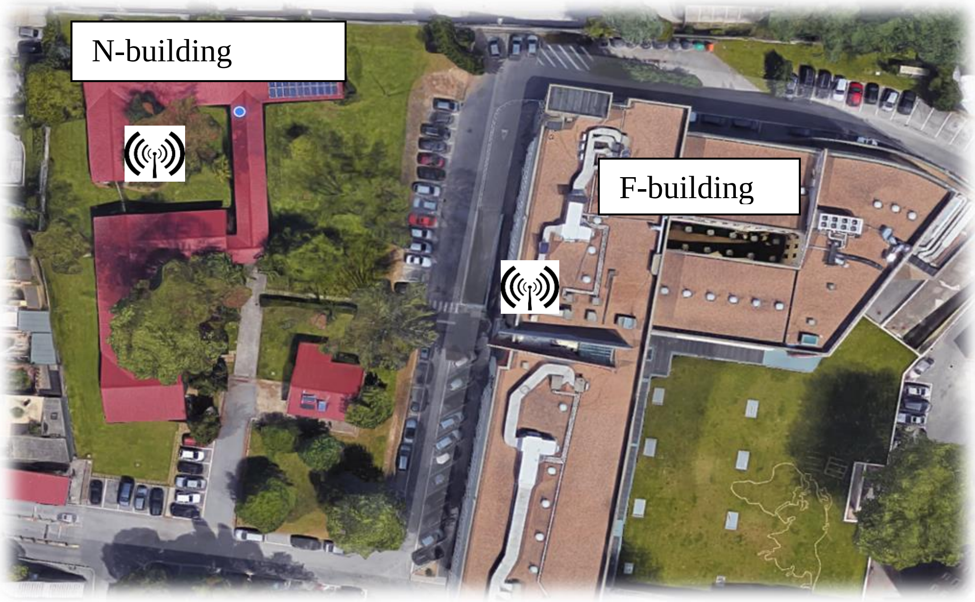


Figure 37 Location of the antennas on map

In Figure 37 is a ground map of the two buildings and the antennas are also indicated with the symbol. It is noticeable that the trees can have an influence in the communication between the two modems.

5.3 Settings

5.3.1 Access point modem in the N-building

The antenna is placed on the roof of the N-building and connected to the building using a cable. The modem will be installed on the wall and connected to the network of the GECAD-building to enable everyone to have access to the data by making the connection with the IP-address using the Matlab® program.

To connect the modem to the network of GECAD certain changes to the IP-address are required to make sure the network does not fail. The IP-address is changed to ‘192.168.2.119’ which is connected to the MAC-address of the modem.

5.3.2 Client modem in the F-building

The antenna of the client is attached close to the window to have a good reach while still being located close to the PLC. The modem itself will be installed next to the PLC to enable it to take power from the controller which is also 24V. The IP-address of this modem does not require corrections. The modem can operate on the default address which is: ‘192.168.0.20’.

5.3.3 Choice of operation mode

Modbus is a serial communications protocol which makes it compatible to communicate with the serial operation mode of the ARM-SE. The Modbus gateway is using the Ethernet cable while the serial operation mode uses RS485 or RS232. As mentioned before the PLC is compatible with the serial operation mode since the device has the Modbus protocol. This means that the PM130 analyzers can be connected to the RS485 of the client modem the same way as the CIRCUTOR power analyzer. The access point modem can run on the Modbus gateway operation mode which makes it accessible using the Matlab® program. The reason for choosing Modbus TCP/IP and not Ethernet is the purpose of the design. Modbus is especially used to transmit data while Ethernet is used for other purposes. The Modbus TCP/IP protocol is used on an Ethernet layer but it can be found on other networks as well and can be used like a SCADA system, as mentioned before.

The PM130 can be connected to the modem exactly as the CVM analyzer which makes the choice for Modbus and serial obvious. There is a port available above the PLC with RS485 connection where the cables can be connected. It is shown in Figure 39 in the paragraph underneath next to the power supply.

5.4 Installation

The installation of both device is displayed in the pictures below to indicate how they are connected. It shows where the power supply, modems and slave are situated. In Figure 39 the installation is created with the energy analyzer CVM-MINI-CM and not with the PM130 analyzers of the PLC.

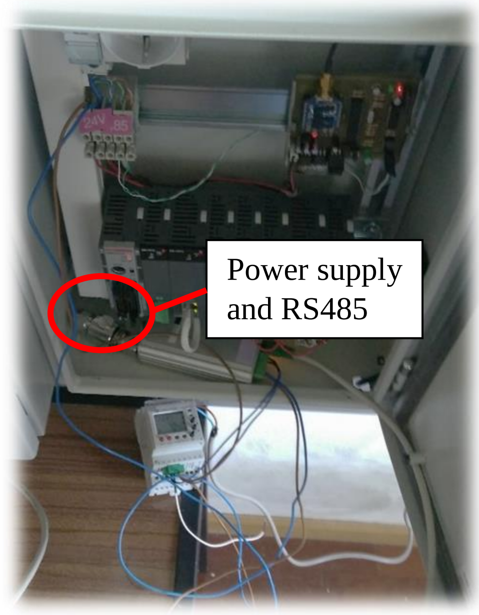


Figure 39 Installation F-Building

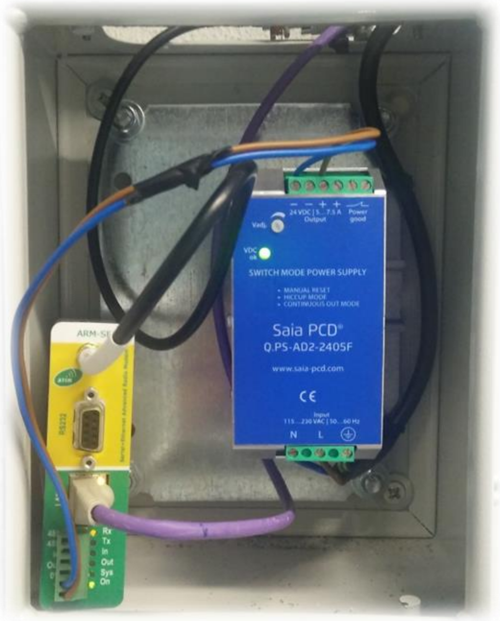


Figure 38 Installation N-building GECAD

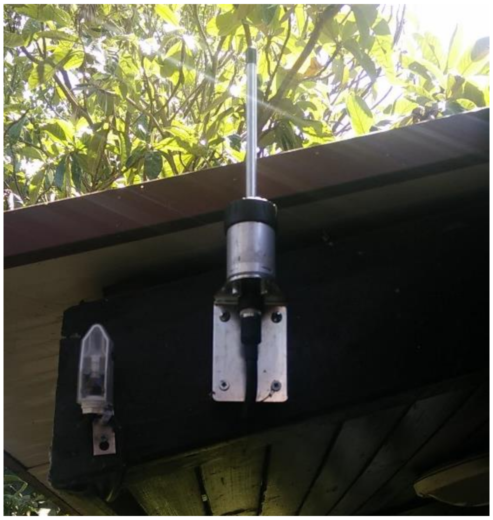


Figure 40 Antenna in N-building

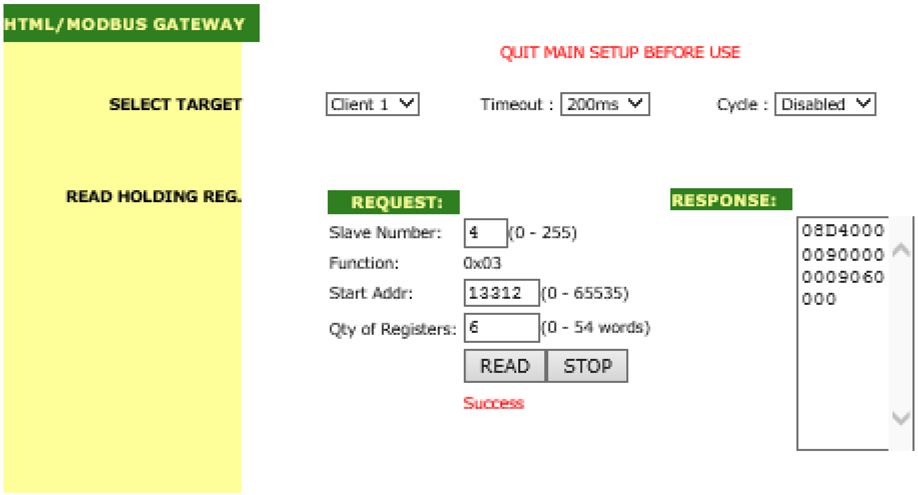
5.5 Collecting data

The installation with the CIRCUTOR can be reached using the network of GECAD which means a test can display the same graph of the voltage as in paragraph 3.3.2.4.1. After succeeding the connection with the power analyzer and successfully creating the graph, it is time to connect the modem to the PM130 analyzers which are connected to the PLC. It is very important that the RS485 connection of the PLC itself is disconnected from the analyzers. Otherwise there are two different masters asking data of the analyzer, the PLC and the modem in GECAD through the client in the F-building. If this occurs the data cannot be transmitted to the modem which will indicate ‘remote problems’ on the webpages.

If one of the PM130 analyzers is connected with the modem independently of the PLC and the registers are known, a program is needed equal as the one of the CIRCUTOR. Instead of using a new program, the data can directly be implemented in the SCADA system of GECAD to collect data of all the PM130 analyzers. Thereby the system can fluently extract data of the PM130 over the antennas for a self-chosen amount of time and create a graphical form.

With the different registers, shown in 7.3, of the PM130 in compare to the CIRCUTOR a new request is created to collect the data.

Before the SCADA system can be operational, there needs to be a clear transmission possible therefor the PM130 will be tested with the webpages if there is data available. After adjusting the settings of the previous paragraph, the request can be fabricated and send to the analyzers. In Figure 41 the request and response are visible of the PM130. Using the embedded webpages on the Modbus gateway mode, a response is retrieved. The slave ID of the used PM130 is 4 and the register to retrieve the voltage is 13312-13318 which indicates a quantity of 6 registers that need to be accessed. In Table 5 the voltage of the three phases or recalculated into their decimal value. All three of them give a realistic value of the situation in the electrical installation.



Client 1 Timeout : 200ms Cycle : Disabled

Slave Number: 4 (0 - 255)
Function: 0x03
Start Addr: 13312 (0 - 65535)
Qty of Registers: 6 (0 - 54 words)

Success

```
08D4000
0090000
0009060
000
```

Figure 41 Response of PM130 slave ID 4

The response exists of 6 registers which contain the voltage of the three lines in the PM130 analyzer with slave ID number 4. To understand the values of the created response the hexadecimal values are translated into decimal values underneath.

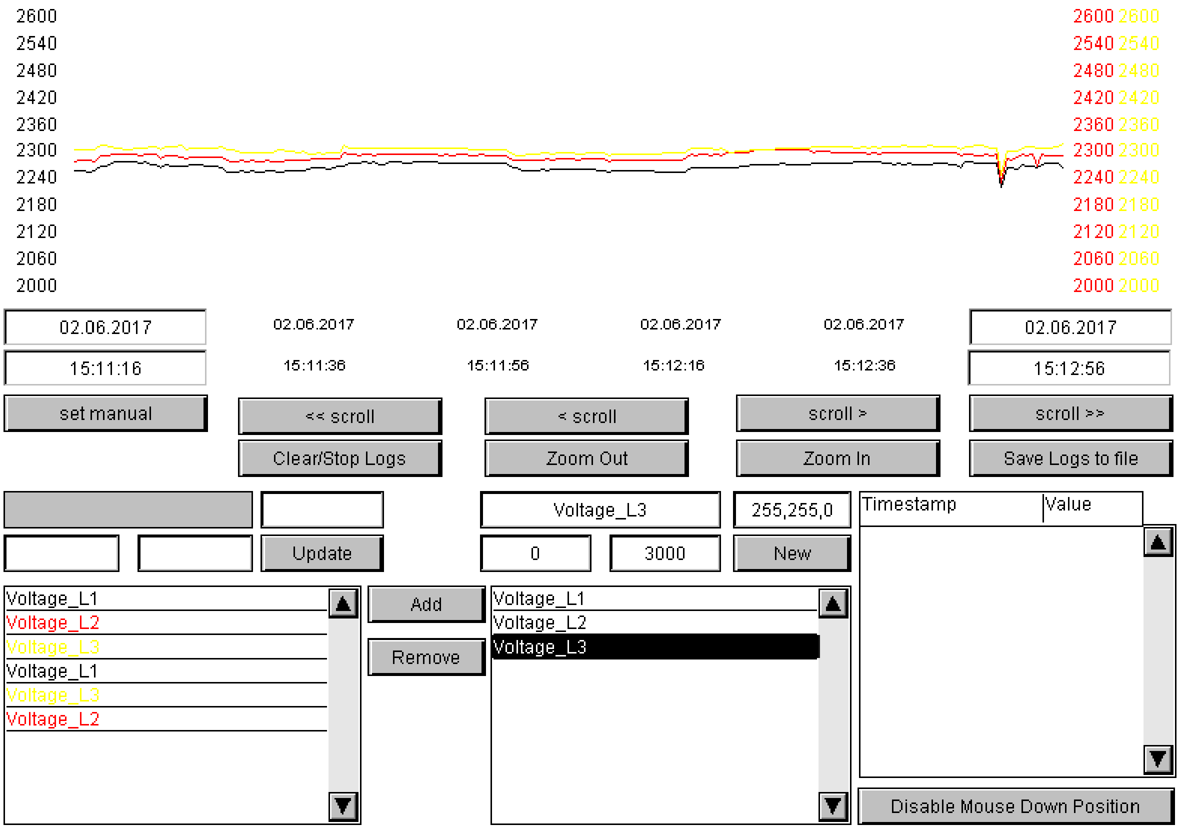
Hexadecimal	*Decimal*	*Voltage*
08D4	2260	226,0V
0900	2304	230,4V
0906	2308	230,8V

Table 5 Response of PM130 slave ID 4

5.6 Converting to SCADA

5.6.1 Results

Paragraph CHAPTER 4: 4.1.1 contains the information about the connection with the SCADA system. After receiving the right data of the PM130 analyzer, the data can be send to the self-created webpage of the PLC. It is shown below in Figure 42 how the voltages can be monitored. On the y-axis the values are between 2000 and 2600 but it needs to be divided by 10 to reach the exact value of the voltages.



Voltage_L3
255,255,0
0
3000

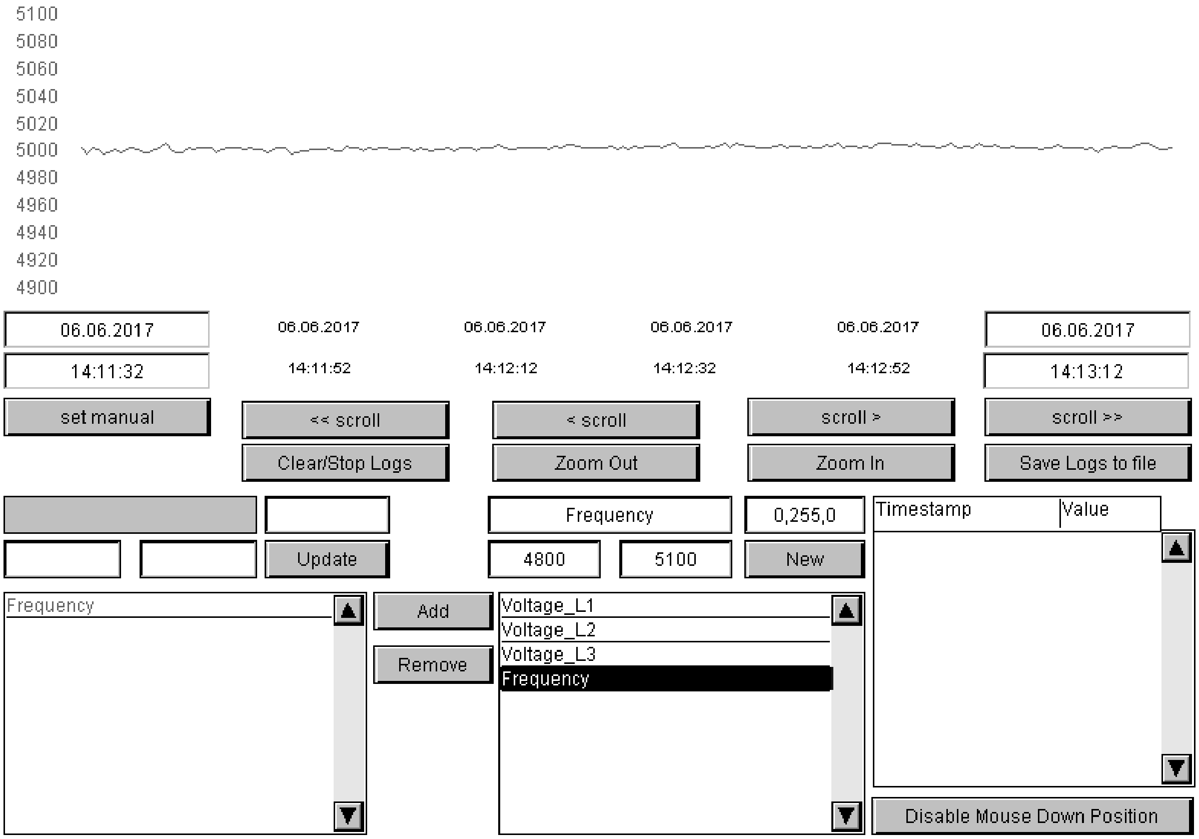
Voltage_L1
Voltage_L2
Voltage_L3
Voltage_L1
Voltage_L3
Voltage_L2

Voltage_L1
Voltage_L2
Voltage_L3

Figure 42 SCADA webpage of the three phase voltages

This graphical form can be created with all the other registers of the PM130. This shows the great purpose of a SCADA system that can access all the data and displays it clearly to make monitoring possible.

Next register that is accessed to receive data is ‘13828’ which describes the frequency of the grid. For this grid the measurement should be 50Hz which is always used in Portugal.



06.06.2017
14:11:32

06.06.2017
14:13:12

Frequency
0,255,0
4800
5100

Frequency

Voltage_L1
Voltage_L2
Voltage_L3
Frequency

Figure 43 SCADA webpage of the frequency

Other measurements cannot be displayed because, at the moment the analyzers only measure the voltage and frequency. The analyzers do not measure any current which indicates in a powerless installation. When they are reconnected to the whole grid of the F-building the SCADA system will be able to display all the parameters of the installation. All the parameters that can be accessed, can be found in the registers in appendix 7.3.

5.6.2 Communication time

The communication time between the SCADA system and the PM 130 analyzers fluctuates between 500ms. This gives an indication that the radio waves can create a small distortion in the data transmission. This was also the case for the communication time of the CIRCUTOR but it does not create a big influence in the received data.

The response time of several data transfers is shown in Figure 44 to indicate the speed of a data transmission between both modems when they connect the GECAD laboratory to the PM 130 analyzers.

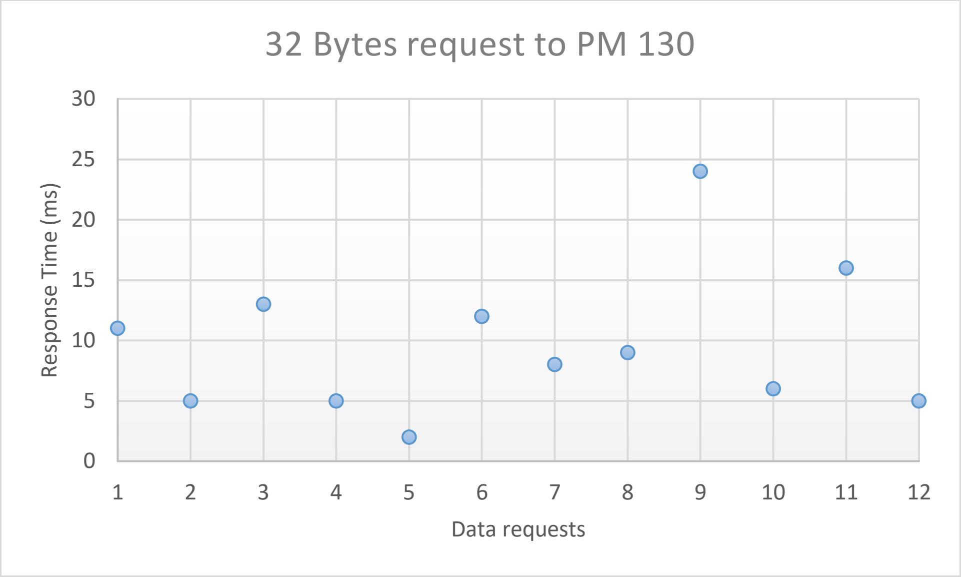


Figure 44 32 Bytes request time PM130

The response time between both modems is very fast which is perfect when integrating in a SCADA system. The fluctuation in the graph is minimum comparing to the amount of time which indicates on a good response time for the transmission.

5.6.3 Lost packages

The number of lost packages can indicate on the quality of the transmission, just like a PING-PONG test. In this case it is impossible to use this parameter to analyze the quality of the transmission because there were only two possible outcomes during this assignment. If the modems could communicate with each other, there were never packages lost. If there was a slight malfunction in the radio communication, all data was lost and communication was impossible.

All tests, for the CIRCUTOR and PM 130, were executed with a perfect signal where no packages were lost. But from time to time, it could occur that the signal got lost and no data could be retrieved.

CHAPTER 6: Conclusion

ATIM, the manufacturer of the ARM-SE modem, created a useful device to execute a data transmission using radio communication with different protocols. They managed to make the modem compatible with many operating systems and developed a system to create a fluent way for usage.

At the start of this assignment the modems were successfully configured and the different operation modes and protocols were tested. The tests of the various possible modes showed that there would be many complexities in the process. The first was to create an interface to display the response of any power analyzer. This was only possible using the mode of the Modbus Gateway because it was integrated in the webpages. The interfaces for other operation modes were established using an Arduino, simply Modbus and Matlab®, which indicates the great variety of the modem. Ethernet was the only operation mode that was not tested with an external system because there were none available. The only way to test this mode was by using the command prompt on the computer for multiple Ping-Pong tests. The use of these different protocols in this research of the ARM-SE has shown all the possibilities of the modem. It created a clear view on how radio transmission and data transfers are realized.

All the various approaches to retrieve data between two modems, enabled to select the best way to connect the network of GECAD to analyzers of a PLC in an extern building. By connecting the networks the PM130 analyzers a SCADA system can monitor the electrical installation. The power analyzer (CIRCUTOR) used during the tests of the different operation modes can connect to the modem the same way a PM130 can be connected. This is why the Matlab® program was designed first for the analyzer so it became clear how to access the PM130 analyzers. The chosen operation modes for the modems have also been selected in function of the Matlab® program and SCADA system. This means that the access point modem located in GECAD uses Modbus gateway and the client in the F-building uses the serial mode with RS485 like paragraph 3.3.2.

The program designed in Matlab® can find the IP-address using the Modbus TCP/IP and generates a request in function of generating a response of the analyzer or PLC. These responses are recalculated and transformed into decimal values that in turn are displayed in a graphical form showing the fluctuation of the measurement over a specific period of time. When the PM130 analyzers were connected to the network of GECAD, the PLC could be configured easily because of the knowledge gained by the Matlab® program. At the end of this assignment the SCADA system was able to reach the data of the PM 130 analyzers to monitor the electrical installation.

During this assignment it became clear that, despite the fact a modem is a multifunctional device designed for this radio transmission, a radio modem is not a fully reliable device. Many errors have occurred during this assignment and the cause was mostly unknown. The biggest issue that occurred was because one of the modems was not able to continuously collect data of the analyzers.

This problem made sure that it was really difficult to prove the reliability of the devices but at the end of the assignment the modems functioned normally and the implementation of the analyzers in the SCADA system was successfully achieved.

6.1 Future perspective

This assignment was the beginning to use the ARM-SE modems to manage and control the electrical installation of an external building by implementing the data in the existing SCADA system of GECAD. In this report is described how to access the different registers by creating the right request. The SCADA system can access all the registers of the analyzers to collect the data that is required to connect the installation to the GECAD network.

It should be possible to control every aspect of more analyzers and make monitoring on a full scale possible. That means, later on there can be several of analyzers or other devices connected to the modem which al can be monitored from the GECAD network. This can reflect on connecting all the buildings of ISEP and implement them to the SCADA system. This creates a lot of possibilities for future assignments because the foundation for intelligent buildings in ISEP and GECAD has been created.

CHAPTER 7: References

[1] E. UCLA, "Phase Change Composite Materials for Energy Efficient Building Envelopes," [Online]. Available: https://www.seas.ucla.edu/~pilon/PCMIntro.html.

[2] K. A. J. J. R.-A. C. R. Milos Manic, "Intelligent Buildings of the Future: Cyberaware, Deep Learning Powered, and Human Interacting," 4 12 2016. [Online]. Available: Intelligent Buildings of the Future: Cyberaware, Deep Learning Powered, and Human Interacting.

[3] Y. W. E. C. ,. B.-H. S. Quang Duy La, "Power Management of Intelligent Buildings Facilitated by Smart Grid: A Market Approach," 03 05 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7313001/.

[4] N. C. Kennis, Voordelen en Nadelen van Wireless Media.

[5] G. ISEP, "GECAD," [Online]. Available: http://www.gecad.isep.ipp.pt/GECAD/Pages/Presentation/Home.aspx.

[6] ATIM, "The company," ATIM, [Online]. Available: http://www.atim.com/en/company/about/.

[7] ATIM, "Series Ethernet Radio Modem ARM-SE," ATIM, [Online]. Available: http://www.atim.com/en/produits/catalogue/arm-range/series-ethernet-radio-modem-arm-se/.

[8] ATIM, "ARM-SE, Documentation and datasheets," ATIM, [Online]. Available: http://www.atim.com/en/produits/catalogue/arm-range/series-ethernet-radio-modem-arm-se/.

[9] ATIM, "ANT868-BZ," ATIM, [Online]. Available: http://www.atim.com/IMG/pdf/FRDS_ANT868-BZ.pdf.

[10] Zytrax, "Fresnel Zones and their Effect," [Online]. Available: http://www.zytrax.com/tech/wireless/fresnel.htm.

[11] DataWeb, "Wat is Ethernet?," [Online]. Available: http://www.ethernet.nl/wat-is-ethernet/.

[12] E. D. Penton, "What’s The Difference Between The RS-232 And RS-485 Serial Interfaces?," [Online]. Available: http://www.electronicdesign.com/what-s-difference-between/what-s-difference-between-rs-232-and-rs-485-serial-interfaces.

[13] I. I. A. S. MODICON, "Modicon Modbus Protocol Reference Guide," Modicon, [Online]. Available: http://modbus.org/docs/PI_MBUS_300.pdf.

[14] S. Modbus, "TCP/IP," [Online]. Available: http://www.simplymodbus.ca/TCP.htm.

[15] APG, "Modbus RTU vs Modbus TCP/IP: What's the Difference?," [Online]. Available: https://www.apgsensors.com/about-us/blog/modbus-rtu-vs-modbus-tcp-ip.

[16] M. S. Ltd, "How to Fix Data Error (Cyclic Redundancy Check)!," [Online]. Available: https://www.powerdatarecovery.com/data-recovery-resources/data-error-crc.html.

[17] C. S.A., "Circutor CVM-MINI Series," [Online]. Available: http://www.samey.is/_pdf/_circutor/CVM_MINI_Maelistod_Manual.pdf.

[18] PowerMeters, "SATEC PM130 PLUS High Performance Powermeter," PowerMeters 'A division of powerpoint engineering LTD', [Online]. Available: http://www.powermeters.ie/power-meter/satec-pm130-plus-high-performance-powermeter/.

[19] I. Automation, "What is SCADA?," [Online]. Available: https://inductiveautomation.com/what-is-scada.

[20] Mathworks, "The Language of Technical Computing," MATLAB, [Online]. Available: https://nl.mathworks.com/products/matlab.html.

[21] L. Bies, "On-line CRC berekening en routines," 12 2016. [Online]. Available: https://www.lammertbies.nl/comm/info/nl_crc-calculation.html.

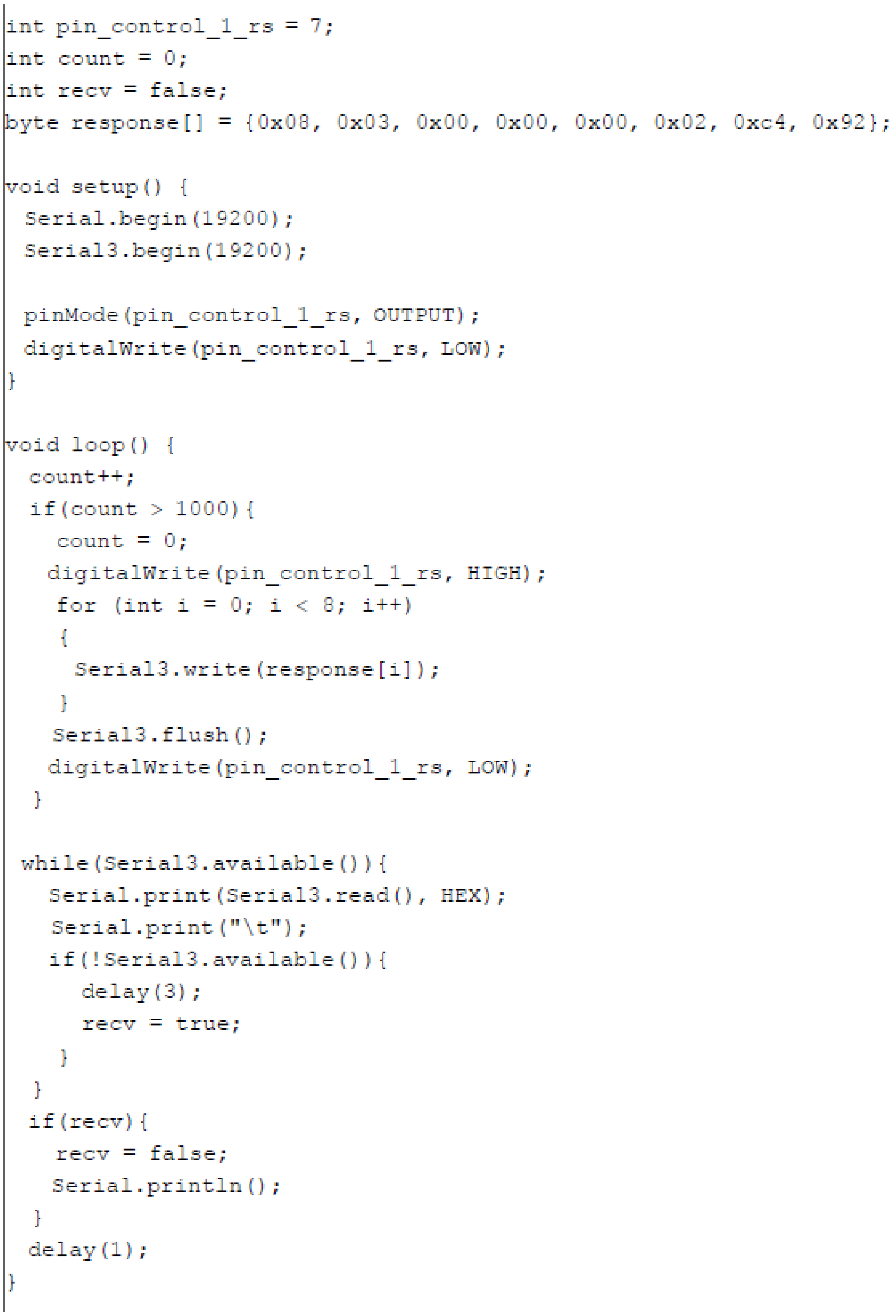
[22] LSIS, "PLC XGB Series," LSIS Co., 2012. [Online]. Available: http://www.lsis.com/product/product.aspx?d1=CCC&c=P00139.

[23] NLDIT, "Voordelen & Nadelen van Wireless Media," [Online]. Available: http://www.nldit.com/netwerken/internet-networking/201309/67675.html#.WSf_Tevytph.

[24] SATEC, "Series PM130 PLUS Powermeters," SATEC Powerful solutions, [Online]. Available: http://satec-global.com.au/documentation/PM130%20PLUS%20Modbus%20-%20Copy.pdf.

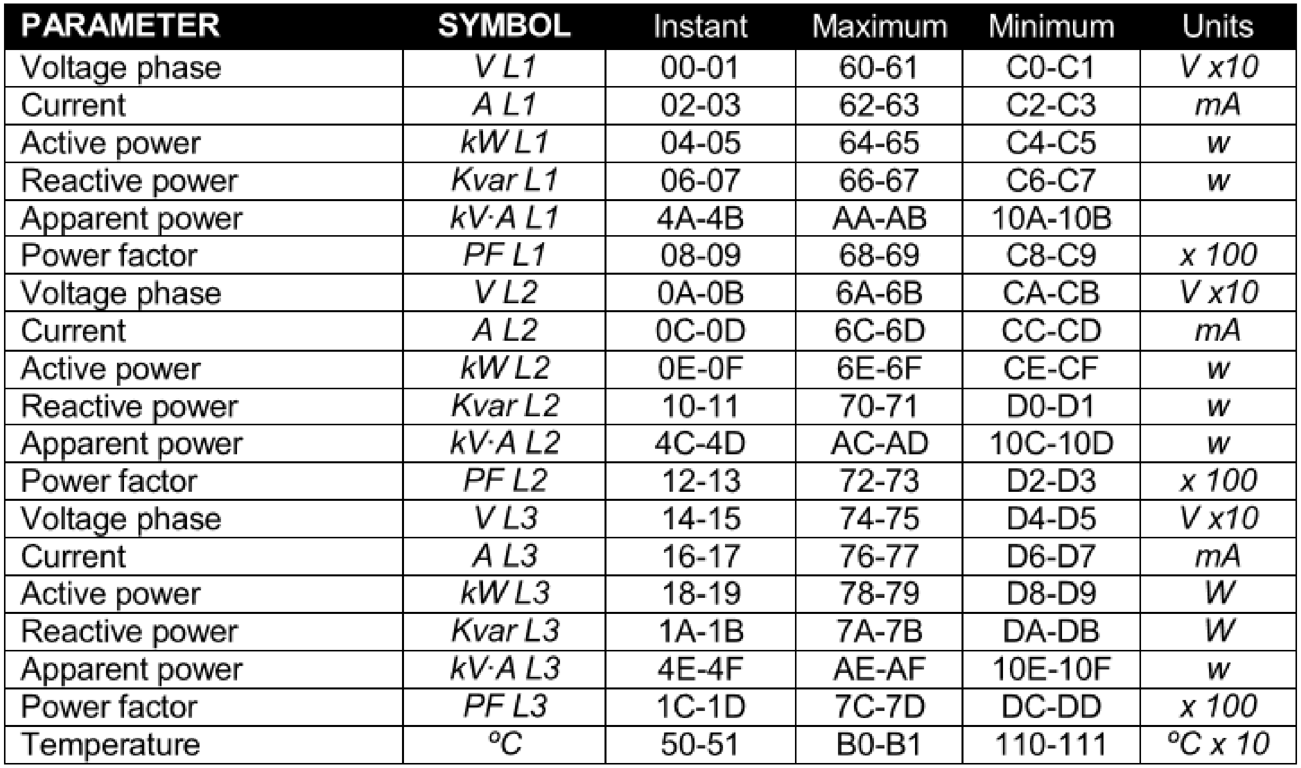
Appendix

7.1 Program to access with Arduino



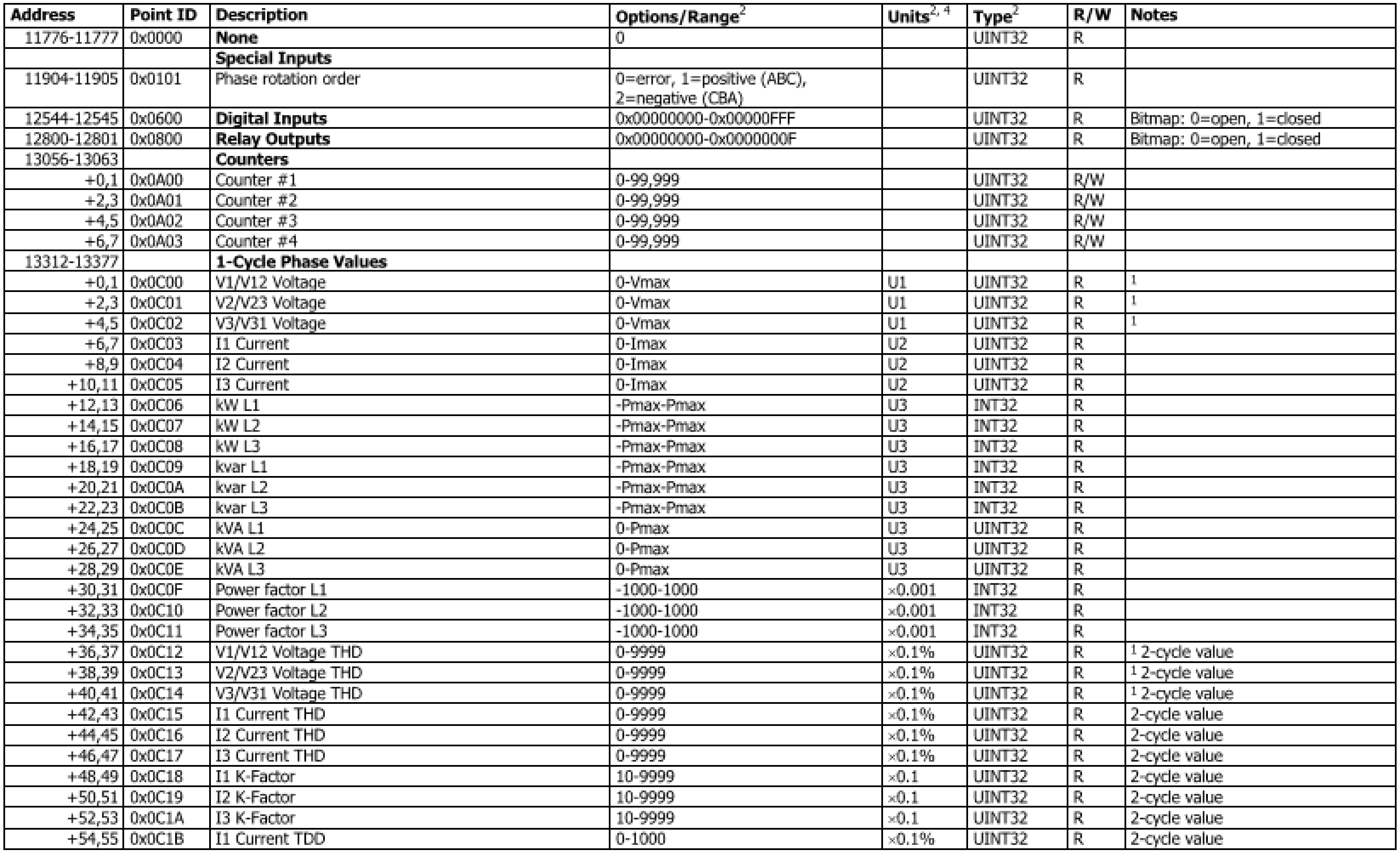
```
int pin_control_1_rs = 7;
int count = 0;
int recv = false;
byte response[] = {0x08, 0x03, 0x00, 0x00, 0x00, 0x02, 0xc4, 0x92};

void setup() {
  Serial.begin(19200);
  Serial3.begin(19200);

  pinMode(pin_control_1_rs, OUTPUT);
  digitalWrite(pin_control_1_rs, LOW);
}

void loop() {
  count++;
  if(count > 1000){
    count = 0;
   digitalWrite(pin_control_1_rs, HIGH);
    for (int i = 0; i < 8; i++)
    {
     Serial3.write(response[i]);
    }
    Serial3.flush();
   digitalWrite(pin_control_1_rs, LOW);
  }

 while(Serial3.available()){
   Serial.print(Serial3.read(), HEX);
    Serial.print("\t");
   if(!Serial3.available()){
      delay(3);
      recv = true;
    }
  }
  if(recv){
    recv = false;
    Serial.println();
  }
  delay(1);
}
```

7.2 Registers of the CIRCUTOR

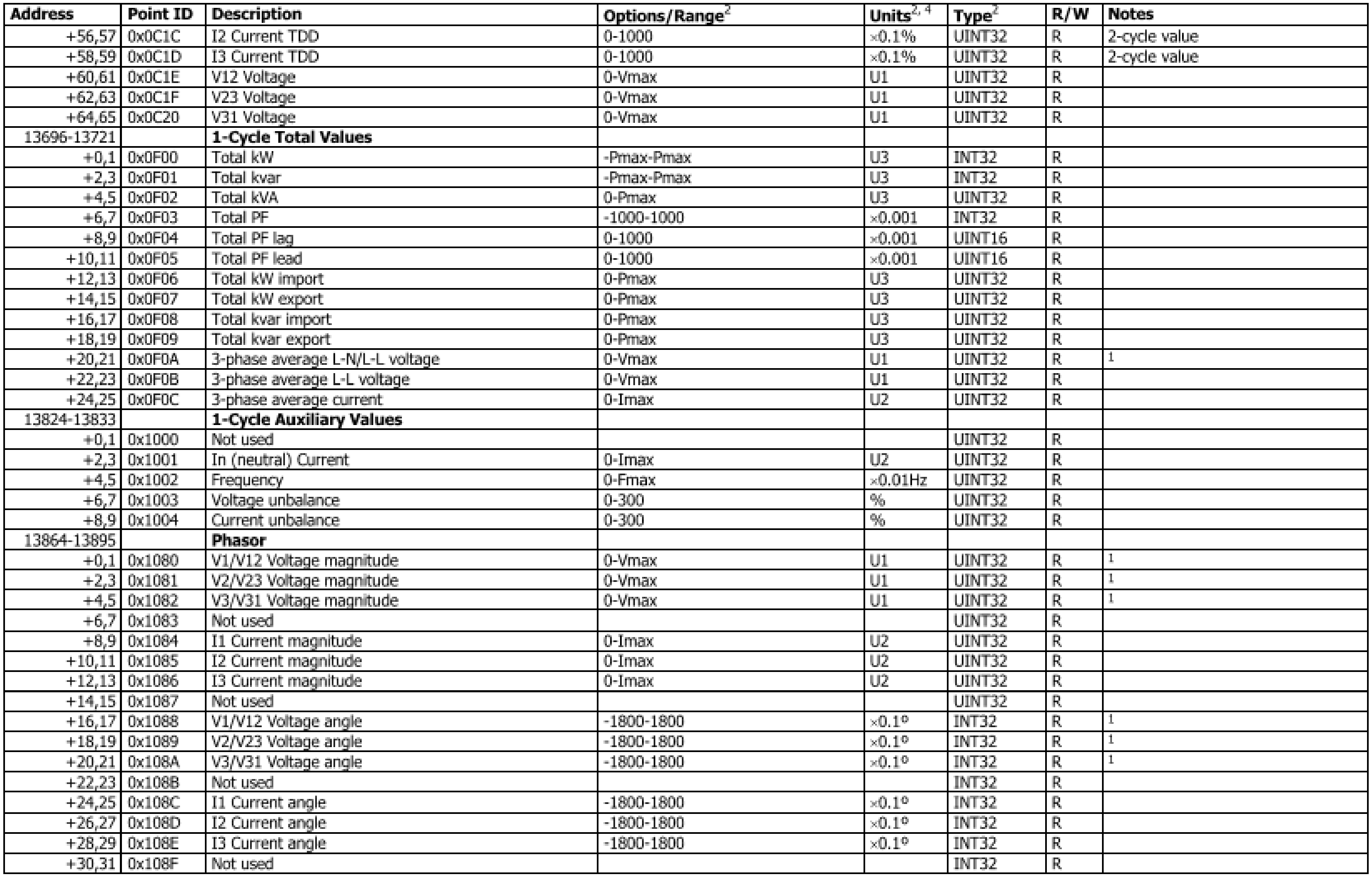


PARAMETER	SYMBOL	Instant	Maximum	Minimum	Units
Voltage phase	*V L1*	00-01	60-61	C0-C1	*V x10*
Current	*A L1*	02-03	62-63	C2-C3	*mA*
Active power	*kW L1*	04-05	64-65	C4-C5	*w*
Reactive power	*Kvar L1*	06-07	66-67	C6-C7	*w*
Apparent power	*kV·A L1*	4A-4B	AA-AB	10A-10B	
Power factor	*PF L1*	08-09	68-69	C8-C9	*x 100*
Voltage phase	*V L2*	0A-0B	6A-6B	CA-CB	*V x10*
Current	*A L2*	0C-0D	6C-6D	CC-CD	*mA*
Active power	*kW L2*	0E-0F	6E-6F	CE-CF	*w*
Reactive power	*Kvar L2*	10-11	70-71	D0-D1	*w*
Apparent power	*kV·A L2*	4C-4D	AC-AD	10C-10D	*w*
Power factor	*PF L2*	12-13	72-73	D2-D3	*x 100*
Voltage phase	*V L3*	14-15	74-75	D4-D5	*V x10*
Current	*A L3*	16-17	76-77	D6-D7	*mA*
Active power	*kW L3*	18-19	78-79	D8-D9	*W*
Reactive power	*Kvar L3*	1A-1B	7A-7B	DA-DB	*W*
Apparent power	*kV·A L3*	4E-4F	AE-AF	10E-10F	*w*
Power factor	*PF L3*	1C-1D	7C-7D	DC-DD	*x 100*
Temperature	*ºC*	50-51	B0-B1	110-111	*ºC x 10*

7.3 Registers of the PM 130



Address	Point ID	Description	Options/Range[2]	Units[2, 4]	Type[2]	R/W	Notes
11776-11777	0x0000	**None**	0		UINT32	R	
		Special Inputs					
11904-11905	0x0101	Phase rotation order	0=error, 1=positive (ABC), 2=negative (CBA)		UINT32	R	
12544-12545	0x0600	**Digital Inputs**	0x00000000-0x00000FFF		UINT32	R	Bitmap: 0=open, 1=closed
12800-12801	0x0800	**Relay Outputs**	0x00000000-0x0000000F		UINT32	R	Bitmap: 0=open, 1=closed
13056-13063		**Counters**					
+0,1	0x0A00	Counter #1	0-99,999		UINT32	R/W	
+2,3	0x0A01	Counter #2	0-99,999		UINT32	R/W	
+4,5	0x0A02	Counter #3	0-99,999		UINT32	R/W	
+6,7	0x0A03	Counter #4	0-99,999		UINT32	R/W	
13312-13377		**1-Cycle Phase Values**					
+0,1	0x0C00	V1/V12 Voltage	0-Vmax	U1	UINT32	R	[1]
+2,3	0x0C01	V2/V23 Voltage	0-Vmax	U1	UINT32	R	[1]
+4,5	0x0C02	V3/V31 Voltage	0-Vmax	U1	UINT32	R	[1]
+6,7	0x0C03	I1 Current	0-Imax	U2	UINT32	R	
+8,9	0x0C04	I2 Current	0-Imax	U2	UINT32	R	
+10,11	0x0C05	I3 Current	0-Imax	U2	UINT32	R	
+12,13	0x0C06	kW L1	-Pmax-Pmax	U3	INT32	R	
+14,15	0x0C07	kW L2	-Pmax-Pmax	U3	INT32	R	
+16,17	0x0C08	kW L3	-Pmax-Pmax	U3	INT32	R	
+18,19	0x0C09	kvar L1	-Pmax-Pmax	U3	INT32	R	
+20,21	0x0C0A	kvar L2	-Pmax-Pmax	U3	INT32	R	
+22,23	0x0C0B	kvar L3	-Pmax-Pmax	U3	INT32	R	
+24,25	0x0C0C	kVA L1	0-Pmax	U3	UINT32	R	
+26,27	0x0C0D	kVA L2	0-Pmax	U3	UINT32	R	
+28,29	0x0C0E	kVA L3	0-Pmax	U3	UINT32	R	
+30,31	0x0C0F	Power factor L1	-1000-1000	×0.001	INT32	R	
+32,33	0x0C10	Power factor L2	-1000-1000	×0.001	INT32	R	
+34,35	0x0C11	Power factor L3	-1000-1000	×0.001	INT32	R	
+36,37	0x0C12	V1/V12 Voltage THD	0-9999	×0.1%	UINT32	R	[1] 2-cycle value
+38,39	0x0C13	V2/V23 Voltage THD	0-9999	×0.1%	UINT32	R	[1] 2-cycle value
+40,41	0x0C14	V3/V31 Voltage THD	0-9999	×0.1%	UINT32	R	[1] 2-cycle value
+42,43	0x0C15	I1 Current THD	0-9999	×0.1%	UINT32	R	2-cycle value
+44,45	0x0C16	I2 Current THD	0-9999	×0.1%	UINT32	R	2-cycle value
+46,47	0x0C17	I3 Current THD	0-9999	×0.1%	UINT32	R	2-cycle value
+48,49	0x0C18	I1 K-Factor	10-9999	×0.1	UINT32	R	2-cycle value
+50,51	0x0C19	I2 K-Factor	10-9999	×0.1	UINT32	R	2-cycle value
+52,53	0x0C1A	I3 K-Factor	10-9999	×0.1	UINT32	R	2-cycle value
+54,55	0x0C1B	I1 Current TDD	0-1000	×0.1%	UINT32	R	2-cycle value



Address	Point ID	Description	Options/Range[2]	Units[2, 4]	Type[2]	R/W	Notes
+56,57	0x0C1C	I2 Current TDD	0-1000	×0.1%	UINT32	R	2-cycle value
+58,59	0x0C1D	I3 Current TDD	0-1000	×0.1%	UINT32	R	2-cycle value
+60,61	0x0C1E	V12 Voltage	0-Vmax	U1	UINT32	R	
+62,63	0x0C1F	V23 Voltage	0-Vmax	U1	UINT32	R	
+64,65	0x0C20	V31 Voltage	0-Vmax	U1	UINT32	R	
13696-13721		**1-Cycle Total Values**					
+0,1	0x0F00	Total kW	-Pmax-Pmax	U3	INT32	R	
+2,3	0x0F01	Total kvar	-Pmax-Pmax	U3	INT32	R	
+4,5	0x0F02	Total kVA	0-Pmax	U3	UINT32	R	
+6,7	0x0F03	Total PF	-1000-1000	×0.001	INT32	R	
+8,9	0x0F04	Total PF lag	0-1000	×0.001	UINT16	R	
+10,11	0x0F05	Total PF lead	0-1000	×0.001	UINT16	R	
+12,13	0x0F06	Total kW import	0-Pmax	U3	UINT32	R	
+14,15	0x0F07	Total kW export	0-Pmax	U3	UINT32	R	
+16,17	0x0F08	Total kvar import	0-Pmax	U3	UINT32	R	
+18,19	0x0F09	Total kvar export	0-Pmax	U3	UINT32	R	
+20,21	0x0F0A	3-phase average L-N/L-L voltage	0-Vmax	U1	UINT32	R	[1]
+22,23	0x0F0B	3-phase average L-L voltage	0-Vmax	U1	UINT32	R	
+24,25	0x0F0C	3-phase average current	0-Imax	U2	UINT32	R	
13824-13833		**1-Cycle Auxiliary Values**					
+0,1	0x1000	Not used			UINT32	R	
+2,3	0x1001	In (neutral) Current	0-Imax	U2	UINT32	R	
+4,5	0x1002	Frequency	0-Fmax	×0.01Hz	UINT32	R	
+6,7	0x1003	Voltage unbalance	0-300	%	UINT32	R	
+8,9	0x1004	Current unbalance	0-300	%	UINT32	R	
13864-13895		**Phasor**					
+0,1	0x1080	V1/V12 Voltage magnitude	0-Vmax	U1	UINT32	R	[1]
+2,3	0x1081	V2/V23 Voltage magnitude	0-Vmax	U1	UINT32	R	[1]
+4,5	0x1082	V3/V31 Voltage magnitude	0-Vmax	U1	UINT32	R	[1]
+6,7	0x1083	Not used			UINT32	R	
+8,9	0x1084	I1 Current magnitude	0-Imax	U2	UINT32	R	
+10,11	0x1085	I2 Current magnitude	0-Imax	U2	UINT32	R	
+12,13	0x1086	I3 Current magnitude	0-Imax	U2	UINT32	R	
+14,15	0x1087	Not used			UINT32	R	
+16,17	0x1088	V1/V12 Voltage angle	-1800-1800	×0.1º	INT32	R	[1]
+18,19	0x1089	V2/V23 Voltage angle	-1800-1800	×0.1º	INT32	R	[1]
+20,21	0x108A	V3/V31 Voltage angle	-1800-1800	×0.1º	INT32	R	[1]
+22,23	0x108B	Not used			INT32	R	
+24,25	0x108C	I1 Current angle	-1800-1800	×0.1º	INT32	R	
+26,27	0x108D	I2 Current angle	-1800-1800	×0.1º	INT32	R	
+28,29	0x108E	I3 Current angle	-1800-1800	×0.1º	INT32	R	
+30,31	0x108F	Not used			INT32	R	

7.4 Realtime meter of the CIRCUTOR

```
%Blank M-file cretaed with variable number of inputs and some fixed inputs
%Fixed inputs: Time, step_time and adresses. Extra adresses can be added by varargin
%Input 'adresses' is [00]

close all;
temp = 0;

time = 30
step_time = 0.5
adresses = [00]
varargin = 0

%Convert the input array 'adresses' to a cellarray
celladresses = num2cell(adresses);

%Concatenate the input variables adresses and varargin
arguments = [celladresses,varargin];

%Count the number of elements in the array
num = numel(arguments);

%Initiate a variable with all zeros where data will be in stored
r = time/step_time;
R = zeros(num, r);

%Configuration of TCP/IP channel
IPADDR_ = '192.168.2.119';%IP adress is adjustable in the menu of the Janitza
PORT=502; %The port should be 502 for TCP/IP

%Open the connection
t = tcpip(IPADDR_, PORT); %Set IP and Port of Janitza
set(t, 'InputBufferSize', 512);
t.ByteOrder='bigEndian';

tic;

t1 = 0;

%Run the code as long as the given time
while t1 <= time
t2 = toc;

%Try to open connection and display status of connection
try
if ~strcmp(t.Status,'open')
fopen(t);
end
if temp == 0, disp('TCP/IP Open'), end;
catch
disp('Error: Can''t open TCP/IP');
```

```
end

a1 = 0;
A = cell(num,1);
B = cell(num,1);
while a1 < num;
a1 = a1 + 1;

message = [...
%*** TRANSACTION ID ***%
uint8(0); ... %
uint8(3); ... % Two byte transaction ID
%*** PROTOCOL ***%
uint8(0); ... %
uint8(0); ... % Two byte protocol ID - all zeros means Modbus TCP
%*** BYTES REMAINING ***%
uint8(0); ... %
uint8(6); ... % Two byte number of bytes for everything after this
%*** SLAVE ID ***%
uint8(8); ... % Slave ID - use if end device is after a modbus tcp/rtu router, otherwise use 255
%*** FUNCTION ID ***%
uint8(3); ... % 4 - read input registers
%*** DATA ***%
%***** Starting Register *****%
uint8(0); ... %
uint8(0); ... % Two byte number that gives the starting register to read
%***** Number of Registers to Read *****%
uint8(0); ... %
uint8(2)] % Two byte number that gives how many registers to read

fwrite(t, message,'int8');
while ~t.BytesAvailable,end
response = fread(t,t.BytesAvailable)
result = bitshift(response(10),8*3) + bitshift(response(11),8*2) + bitshift(response(12),8*1) + response(13)

G=result/10;
varargout{a1} = G;
A{a1} = arguments{a1};
B{a1} = varargout{a1};
end

C = [A, B];

%Make arrays out of the cellarrays
C = cell2mat(C);
B = cell2mat(B);

fclose(t);
temp = temp + 1;

```

```
%Store B in a column of R (column number depends on value of temp)
R(1:num,temp) = B;

t1 = toc;

%Open a figure window, but only at the beginning of the first loop
if temp == 1;
gcf = figure('Name','Real-Time Meters','NumberTitle','off','Color',...
[1 1 1],'MenuBar','none');
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
end

%%Draw the plots of the meters
%Plot of L-N Voltage
subplot(2,3,1);
drawnow
hold on
scatter(t1,R(1,temp),'b');


title('Voltage L-N (V)','FontSize',16);
ylabel('Voltage (V)','FontSize',14);
xlabel('Time (s)','FontSize',14);
legend({'L1'});

t3 = toc;

%Pause to respect step_time (step_time can not be smaller than 0.5s)
pause(step_time-(t3-t2));

end

hold off
```