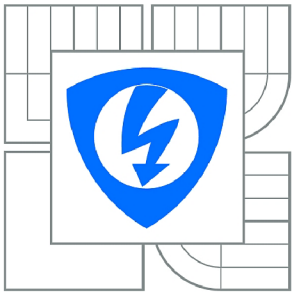
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV JAZYKŮ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF FOREIGN LANGUAGES

ANALYSIS OF COMMUNICATION PROTOCOLS AND MODULES IN WIRELESS M-BUS

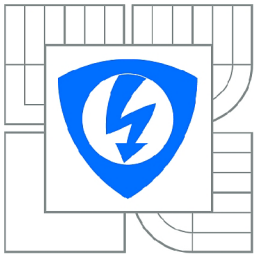
ANALÝZA KOMUNIKAČNÍCH PROTOKOLŮ A MODULŮ PRO WIRELESS M-BUS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — ANNA HOLYSZEWSKÁ
AUTHOR

VEDOUCÍ PRÁCE — Mgr. ŠÁRKA RUJBROVÁ
SUPERVISOR

BRNO 2015



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav jazyků

Bakalářská práce

bakalářský studijní obor
Angličtina v elektrotechnice a informatice

Studentka: Anna Holyszewská ***ID:*** 154652
Ročník: 3 ***Akademický rok:*** 2014/2015

NÁZEV TÉMATU:

Analýza komunikačních protokolů a modulů pro Wireless M-Bus

POKYNY PRO VYPRACOVÁNÍ:

1 Úvod
2 Metody odečtu dat
3 Typy měřičů
4 Budoucnost - užití bezdrátových měřičů
5 Parametry bezdrátových komunikačních modulů
6 Analýza datových telegramů
7 Závěr

DOPORUČENÁ LITERATURA:

[1] EN 13757-4. EUROPEAN STANDARD: Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands). European Committee for Standardization: Management Centre, 2013.
[2] OMS: Open Metering System. [online], 2015. URL http://oms-group.org

Termín zadání: 9.2.2015 ***Termín odevzdání:*** 22.5.2015

Vedoucí práce: Mgr. Šárka Rujbrová
Konzultanti bakalářské práce: doc. Ing. Jiří Šebesta, Ph.D.

doc. PhDr. Milena Krhutová, Ph.D.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Cílem této bakalářské práce je nahlédnout do problematiky spojené s rozúčtováním nákladů na teplo a vodu pro jednotlivé bytové i průmyslové objekty. Data jsou nejprve zpracována teoreticky s postupným dělením podle typů měřičů a typů odečtů. Okrajově se text věnuje i bezpečnostním prvkům měřičů, které zajišťují ochranu proti úmyslnému poškození ze strany zákazníka i neúmyslnému poškození jako takovému. Dále se práce zabývá základními parametry čtyř konkrétních bezdrátových komunikačních modulů podporující Wireless M-Bus. Srovnání těchto parametrů je znázorněno v tabulce. V neposlední řadě se bakalářská práce prakticky věnuje analýze datových telegramů, které konkrétní měřiče vysílají. Analýza je provedena dle standardů. Hlavním přínosem této práce je lepší porozumění bezdrátovým, dálkovým odečtům měřičů tepla, vodoměrů a rozdělovačů topných nákladů.

KLÍČOVÁ SLOVA

Měřič tepla, vodoměr, průtokoměr, rozdělovač topných nákladů, Wireless M-Bus, Wired M-Bus, bezdrátový komunikační modul, datový telegram

ABSTRACT

The thesis aims to present the topic of allocating costs of heating and water in individual flats and industrial buildings. Firstly, data are elaborated theoretically and divided according to the type of meter and the type of reading of values on the meters. In addition to that, this part of the thesis also deals with security features against possible damage to the meters which can be caused by customers. Secondly, basic parameters of four embedded modules supporting Wireless M-Bus are explained and then compared in a table. The last part of the thesis focuses on the introduction to analysis of data telegrams transmitted by the meters according to the standards. The main contribution of this work is a better comprehension of wireless remote reading of heat, water meters and heat cost allocators.

KEYWORDS

Heat meter, water meter, flow meter, heat cost allocator, Wireless M-Bus, Wired M-Bus, embedded module, data telegram

HOLYSZEWSKÁ, A. *Analýza komunikačních protokolů a modulů pro Wireless M-Bus*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav jazyků, 2015. 56 s., 4 s. příloh. Bakalářská práce. Vedoucí práce: Mgr. Šárka Rujbrová.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma Analýza komunikačních protokolů a modulů pro Wireless M-Bus jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Ráda bych poděkovala vedoucí mé bakalářské práce paní Mgr. Šárce Rujbrové a panu doc. Ing. Jiřímu Šebestovi, Ph.D. za jejich odborné vedení, cenné rady a připomínky, které mi pomohly zpracovat tuto bakalářskou práci. Dále bych ráda poděkovala mému tátovi, který je pro mne vždy inspirací, a který tu je pro mě pokaždé, když potřebuji. Děkuji Ti, tati.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

Nowadays, there are many types of heat meters, water meters, flow meters, gas meters, heat cost allocators and other meters which are installed in factories, apartment blocks and flats all over Europe. They help us allocate the common cost of heat, hot and cold water, gas consumption, etc. to several cost objects. In my thesis I would like to present a basic division of the meters which are commonly used by customers. The customer could be an occupant of a particular flat, an owner of a family house, or an owner of a company. I have also included a basic division of reading methods of data which the meters transmit. The reason why I have chosen the topic of various consumption meters and mainly their wireless communication is the fact that nowadays people try to do everything as uncomplicated as possible. It is obvious that wired technologies will be replaced by wireless technologies – this includes reading the values on meters. I worked with the assumption that people would more often select meters with wireless communication rather than devices which have to be read using visual reading, for example. Therefore, my thesis tries to explain the basic principles of wireless data reading. I introduce radio parts placed in the meters or in the reading devices which are called “embedded modules”. Their fundamental parameters have been compared in a clearly arranged table. These embedded modules support Wireless M-Bus. Wireless Meter-Bus, in short Wireless M-bus, is a new European standard for wireless remote reading of various consumption meter types. The practical part of my thesis deals with the analysis of data telegrams from the heat meter Kamstrup Multical 402 and the heat cost allocator Techem. It is supposed that both data telegrams can be decrypted according to the European Standard 13757-4: Communication systems for meters and remote reading of meters, see Part 4, The M-Bus: A Documentation Rev. 4 and Open Metering System Specification: Volume 2, Primary Communication.

1 METHODS OF READING THE DATA

In this chapter I will focus on the methods which are used for reading data from the meters. Inside this data there is encoded not only the consumption of heat or water, but also many other parameters which will be discussed later. Firstly, the Visual reading and its main disadvantage will be explained. Secondly, the Wired M-Bus reading will be clarified, and its developer will be mentioned, too. I will also describe the basic types of connection topology which includes Star Topology, Bus Topology and Ring Topology. The main facts about the Wireless M-Bus are summarized in the following subchapter titled Radio reading. This part contains a division of radio reading methods (Walk-by method, Drive-by method) as well as the different types of communication. (Unidirectional data transfer and Bidirectional data transfer). Finally, I will explain the Automatic Meter Reading (AMR) as a technology which collects automatically values from the meters.

1.1 Visual reading

The reading of meters is realized by an employee of a specific company at regular intervals – mostly once a year. This person has to enter the building and read the values on the display of each heat cost allocator and other meters. The necessity of entrance is the main disadvantage of the visual reading. Therefore, other reading methods have been developed.

1.2 Wired M-Bus reading

This type of reading is commonly used for meters which are located outside the flats, usually in large factories. It is a cable that ensures the connection. The Meter Bus (in short M-Bus) was developed for remote reading by Prof. Dr. Horst Ziegler, a member of the M-Bus Usergroup, at the Department of Physics at the University of Paderborn in Germany. This invention has helped to *fill the need for a system for the networking and*

remote reading of utility meters, for example to measure the consumption of gas or water in the home [1]. The M-Bus interface is made of wires. The speed of communication is not as important as resistance to interference and cost efficiency. One of the following methods is used for linking the components in a system.

1.2.1 Topology of connection

Network nodes can be interconnected into various topologies. Common network topologies include the star topology, bus and ring topology. All of these topologies are described below.

Star topology

The central processor unit has a connection with each component through an individual transmission line. These components can transmit data to the central unit either simultaneously or sequentially. One of the disadvantages of this arrangement is the necessity of a large amount of cables.

Bus topology

In this case, there is one common transmission line and the components are linked to it. This topology is cost-effective but at one instant only one component can transmit data. Nevertheless, if any of them failed, the network would not be disturbed.

Ring topology

In the case of ring topology, one component is linked exactly to two other components and the data are transferred from one point to another. It provides only one pathway between them and if one of the components failed, the whole network would be out of order. For this reason it is used very rarely.

A combination of two types of topology can also be used.

1.2.2 OSI model

The Open Systems Interconnection (OSI) model, which was devised by the International Organization for Standardization (ISO), describes communication functions and servicing in seven layers: Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer and Application Layer. Their basic functions are explained in more detail below.

Physical Layer: The Physical Layer is the lowest layer. It provides data transmission between communicating partners using a physical connection. It is a transport oriented layer.

Data Link Layer: The Data Link Layer ensures the connection between nodes connected by a physical connection. The layer protocol determines the telegram structure, transmission protection methods, addressing of participants, methods of accessing the transmission medium and their synchronization. It is a transport oriented layer.

Network Layer: The Network layer provides packet routing for the Transport Layer. It also chooses the most convenient transmission route in the network between the nodes. It is a transport oriented layer.

Transport Layer: The Transport Layer leads the information through the network, controls the information flow and clusters information into individual packets. It is a transport oriented layer.

Session Layer: The Session Layer controls dialogues between application systems. It is an application oriented layer.

Presentation Layer: The Presentation Layer determines the exchange data format which is common for different kinds of data. It is an application oriented layer.

Application Layer: The Application Layer is the highest layer representing the interface between the user and the open system. It is an application oriented layer.

The M-Bus includes one master (Central Allocation Logic) and several slaves (end-equipment meters). All data are transmitted through the cables. The whole communication is controlled by the Central Allocation Logic.

1.3 Radio reading – wireless M-Bus

Walk-by method: Modern types of meters support radio reading, however, in a limited distance from the transmitter. The employee of the company has to catch data using the receiver in front of each flat or in front of the building. This method is most frequently used for heat cost allocators and domestic water meters. The advantage is that it is not

necessary to enter into the flat. All meters work at the frequency band of 868 MHz. Two years ago the Czech Telecommunication Office gave permission to use also the frequency band of 169 MHz (169.400 MHz). This frequency band is endowed with higher radiated power and magnetic field intensity.

Drive-by method: This method is also used for meters placed in flats but the employee can stay inside his car, go through the whole street and do the radio reading. Some day in the future it could be possible to fix the receiver into a refuse collection car and collect the data without direct human intervention. The refuse collection car is convenient because of its speed and periodicity.

The basic documents for Wireless M-Bus are the European Standard 13757-4 (ES 13757-4) [1] and the Open Metering System (OMS) [7]. They describe modes of operations for the communication with the meter and also the layers. Many of the physical and link layer parameters of these different modes are identical, allowing the use of common software and hardware. Nevertheless, technical requirements cause that some parameters are different.

1.3.1 Types of communication

In general, there are two types of communication according to the direction of the data transfer. The first one is unidirectional data transfer and the second one is bidirectional data transfer.

Unidirectional data transfer

Unidirectional data transfer is used very frequently. The meter contains only one transmitter and transmits data at regular intervals. For the meter it is not important if there is a receiver which would collect the data. The following operating modes are used: T1, S1, C1, and others.

Bidirectional data transfer

Bidirectional data transfer is rarely used. The meter contains a transmitter and a receiver. The situation can be as follows: When a superior system needs values (a stationary device – such as a gateway or mobile devices – for example, a person with the reading system), it sends a requirement to the meter, using its address. The requirement is called “a wake-up message”. The meter analyses it and makes a decision

whether the message is for it or not, and then, in case that the message is for it, sends the data. The following operating modes are used: T2, S2, C2, R2, N2, and F2.

1.4 Automatic Meter Reading

Automatic Meter Reading (AMR) is a technology which automatically collects values from meters inside the flats. The radio gateways are located outside the rooms but inside the buildings – they communicate with the meters which are inside the flats. These gateways later transfer the data to the central database of a company via the Internet, for example. For this reason, it is not used on a regular basis.

2 TYPES OF METERS

In this chapter the meters will be divided into four categories. Firstly, I will speak about heat meters and then about water and flow meters. As it will be mentioned, the water meters can be subdivided into domestic water meters and industrial water meters. I will also focus on the most convenient position for water meters, its input protection sieve and protection against customer induced damage. The typical damages will be explained on several examples. Finally, heat cost allocators will be discussed and divided according to the number of sensors, the method of allocation, the ability of programming, the load of data, the method of reading, and other standards.

2.1 Heat meters

They measure the amount of heat energy which is supplied in the form of hot water. They are used for measuring of the heating and the cooling. They consist of four parts: two temperature sensors, a flow meter and an energy calculator (integrator). The energy calculator either has or has not a radio segment. They can be located in cellars because of measuring the consumption of heat in the whole building or in each flat for measuring the consumption of heat in one particular flat. The units which are commonly used are the following: watt-hour (symbolized by Wh) or joule (symbolized by J).

2.2 Water meters and flow meters

Flow meters include all devices which are able to measure liquids. The following text is mainly about one type of them: water meters.

Domestic water meters: There are two types of domestic meters. One type is used for measuring hot water and the other type for cool water. Both of these types can be divided to electronic meters, mechanical meters and meters with a pulse transmitter or an open collector interface.

Electrical meters: Fully electric with a radio part inside the meter.

Mechanical meters: single-jet meters, the radio module can be added.

Meters with a pulse transmitter or an open collector interface: It is the external radio module (radio pulse adapter) that is connected to the output. These meters are usable for optimum reading with a difficult access.

Industrial water meters: There are two types of meters which are mainly used in the industrial field. Equally to the domestic meters, there is one type for hot water and other type for cool water. Another division could be as follows: multi-jet water meters, ultrasonic water meters, Woltmann water meters, electromagnetic flow meters, and other meters.

2.2.1 The position for installing the water meter

The water meter is usually installed in the horizontal position – the most suitable position for reading. A meter which is installed in the horizontal position and which has its dial located upwards will measure accurately. Whereas a meter which is installed in the vertical position will not measure as accurately as the meter in the previous position. The same situation can occur with a meter installed in the horizontal position but with the dial located on the side.

2.2.2 The input protection sieve

Manufacturers of water meters commonly install the protection sieve into the input part of meters. They do this because of protection against any large particles. These large particles may damage the water meter. Shortly afterwards, this water meter completely or partially stops working and it has to be replaced.

2.2.3 Protection against customer induced damage

Customers very often aim to damage the meters on purpose, because they want to reduce their water costs. Each water meter has a number of protection devices against these attempts to do damage. The first of these protections is a plastic lid fixed to the meter which should protect the dial. Nevertheless, if any person wanted to squeeze something in the dial and block it up, the person would probably manage to do it. The person usually drills a small hole into the lid, puts something inside, which causes the damage and the meter stops working. Because of this reason, the use of non-transparent

lids (they are also used by some companies) is meaningless. The other elements which protect the meter are lead seals and sticky seals. The sticker or the lead seal are usually placed in an appropriate position for protecting the register and the input fitting. If the seal was impaired, the customer would be inquired why it is so. Customers also try to influence water meters with a strong permanent magnet. However, modern meters are able to notice that they are located in a magnetic field. In addition to that, a customer may influence the devices to his own disadvantage. The meter starts showing a larger number of water consumption which does not correspond to the real consumption, or the other way around, it starts showing negative number of water consumption. Last but not least, we should mention the small plastic cylinder. This protection element protrudes from the dial under a cap. The small plastic cylinder is not used very frequently but it functions as a good indication of attempts to press the water meter with great strength, which can cause its discontinuation.

2.3 Heat cost allocators

In the thesis the heat cost allocators are named “meters”, even though in reality they are not meters. Heat coast allocators are used for allocating the common cost of heat among specific consumers. These devices are installed on every radiator. In the past mostly evaporative heat cost allocators with a calibrated liquid in a capillary tube were used. They recorded the total heat consumption. Evaporative heat cost allocators were invented by Max Gehre in Westerwald in 1921. These heat cost allocators had a very simple design (with a pointer indicator). Naturally, a simple design means a low price meanwhile a complicated design may mean higher price. Because of this attribute, they were very popular and companies used them very frequently. During the eighteen twenties, a new type of heat cost allocators, the electronic allocators, were introduced. Nowadays, they are always electronic with an LCD display.

2.3.1 The division of electronic heat cost allocators

According to the number of sensors

One-sensor allocators: The sensor measures separately the temperature of the radiator and the temperature inside the room. It means that these parameters are not able to be

measured simultaneously – one of them is always neglected. They are convenient for the places where the temperature is fairly stable.

Two-sensor allocators: The first of the sensors measures the ambient temperature and the other sensor measures the temperature of the radiator. Due to the sensors, the heat cost allocator with two sensors is able to measure the total heat output of the individual radiator. This means better accuracy and an advantage in low-temperature heating systems. It can also distinguish other heat sources such as sun radiation.

Three-sensor allocators: They work with middle logarithmic difference. Nevertheless, they are not commonly used.

According to the method of allocation

One-sensor method: a heat cost allocator with one sensor.

Two-sensor method: a heat cost allocator with two sensors.

Three-sensor method: a heat cost allocator with three sensors.

According to the abilities of programming

Heat cost allocators which cannot be programmed: it is not possible to program them at all. They measure the values, and after that a person reads the values.

Partially programed heat cost allocators: people are able to program some parameters such as the date when the meter regularly saves the values.

Completely programmed heat cost allocators: people are able to program all parameters.

According to the load of data

Incremental heat cost allocators: the increment of the consumption is permanent. The meter measures constantly and never sets a zero, never starts measuring anew.

With zero: The meter deletes the values on the date which is set and starts counting again.

According to the method of reading

Apart from visual reading the heat cost allocators allow reading using one of these technologies.

Optical port: one-way or two-way communication

Radio reading: Wireless M-Bus, one-way or two-way communication

Memory: saving the data in memory

According to other criteria

Division according to other standards.

3 RADIO READING AS THE FUTURE

In spite of the fact that nowadays many meters are read visually or, for example, through a cable, the only auspicious method is radio reading, hence from this part of my thesis on I will be interested only in this type of reading. It is believed that radio reading is the sole method which will be used for the foreseeable future. One of the main advantages is the fact that this method is very convenient for the final customer. Last but not least, radio reading is more convenient for the companies which are concerned with meters and their reading, too. Nevertheless, meters allowing radio reading are available at a higher cost than meters without the ability of radio reading – meters without the radio module. Therefore, costumers' input costs are higher than if they buy a meter without the radio module. For this reason, many customers choose the "old way" of reading the meters. It is a common practice that a block of flats has to decide which type of meters ought to be used. But it is true that not every company offers radio reading. In this chapter, I will focus on the application of the radio module in meters and reading devices, and then more information about basic standards of the wireless M-Bus will be discussed as well as the design of the radio part. Finally, I will deal with basic information about Advanced Encryption Standard (AES) [12].

3.1 Radio module

As it has been already mentioned, each meter allowing radio reading has to contain a radio module. The radio module is also installed in the reading devices. The reading device often looks as though it was a flash disc but it is actually not. Thanks to the presence of a USB (Universal Serial Bus) connector, the reading device can be simply connected to a computer. This type of reading device is called a USB Stick. The data which are transmitted from the meter to the reading devices and then to the computer are later processed using an appropriate software. Nevertheless, other types of reading devices with the radio module exist. It can have a package shape with an antenna. This type of reading device communicates with the computer using Bluetooth. Bluetooth is a wireless technology which transmits data over a short distance. The reading devices

with an antenna in the package shape can have the USB connector as well. It means that they can be connected to the computer in the same way as the USB Stick.

In the past, each supplier of water meters or, for example, heat cost allocators allowing radio reading created his separate standard for the radio communication. This used to cause a great deal of confusion and disadvantages. The diverse standard of each supplier meant that customers could not have water meters from one company and heat cost allocators from another company. If a block of flats had had one type of meters from one company and the other type of meters from another company, meters could not been read by one reading device. One supplier of all meters in one block of flats impeded the progress of radio reading in Europe. Therefore, the basic document for the Wireless M-Bus was created. This basic document is the European Standard 13757-4 (ES 13757-4) [1]. Thereafter, a community of interest of associations called the Open Metering System Group (OMS-Group) established other standards which continue according to the European Standard 13757-4 [1]. Thanks to these standards, basic rules for radio reading are established and companies from all over Europe should respect them. The meter park is totally compatible. This results in a free selection of suppliers for customers who want to buy meters, because each supplier can use the OMS meters from various manufacturers and combine them arbitrarily.

3.1.1 European Standard 13757-4 (ES 13757-4)

Although the European Standard 13757 has four parts, I will focus only on its fourth part which describes the wireless meter readout (radio meter reading for operations in SRD bands). This European Standard was approved by the European Committee for Standardization (CEN) on 29 June 2013 and exists only in three official versions – English version, French version and German version. However, the same status as the one of the official version is assigned to a version *in other language made by translation under the responsibility of CEN member into its own language and notified to the CEN-CENELEC Management Centre* (2). CEN members mentioned on the first page of the European Standard 13757-4 [1] have to comply the CEN/CENELEC Internal Regulations. The European Standard 13757-4 [1] *specifies the requirements of parameters for the physical and link layer for systems using radio to read remote meters. The primary focus is to use the Short Range Device (SRD) unlicensed telemetry*

bands. The standard encompasses for walk-by, drive-by and fixed installations. As a broad definitions, this European Standard can be applied to various application layers [3].

3.1.2 Open Metering System Specification

An open, vendor independent standard for communications has been developed by the Open Metering System Group. This standard is based on European norms. *The Open Metering System (OMS) is the only system definition across Europe which integrates all media (electricity, gas, heat and water incl. sub metering) into one system. It was developed by the industry in order to guarantee a future-proof communication standard and interoperability between all the meter products* [4].

3.2 Design of the radio part

As it has been already mentioned, each meter allowing radio reading contains a radio part which communicates with the reading device and afterwards with the computer where a suitable software is installed. But firstly, the radio part has to be designed for a particular type of meter by manufacturers. The producers currently have two possibilities of providing their meters and reading devices with the radio part. The first option is to design the radio part individually. This means that it is necessary to choose suitable components and their position and connection on the motherboard. On the one hand, it can be the right decision for large-scale manufacturers, but on the other hand, it is an expensive solution for smaller manufacturers. Small manufacturers mostly choose one of the six embedded radio modules. These embedded modules are already designed and can be easily installed into the meter or the reading devices. All embedded modules respect the European Standard 13757-4 [1] and the OMS-Group standard [7].

3.3 Advanced Encryption Standard

Because of sensitive data, telegrams from the meters are encrypted according to the Advanced Encryption Standard (AES). This standard was developed by Joan Daemen and Vincent Rijmen, the Belgian cryptographers and then established in 2001 by

National Institute of Standards and Technology. It *specifies a cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext* [5]. This algorithm is able to use 128, 192, and 256 bits cryptographic keys for encrypting and decrypting data blocks of 128 bits.

4 PARAMETERS OF EMBEDDED MODULES

In this chapter, I will deal with four embedded modules and their parameters. Although, all embedded modules respect the European Standard 13757-4 [1] and the OMS-Group standard [7], their parameters are different. Generally speaking, only six basic embedded modules exist, but there are various types of them. Unfortunately, two of them are hardly available in the Czech Republic: the Panasonic M-Bus Modem PAN7550 and the Embit EMB-WMB 169/868 MHz Wireless M-Bus module. Therefore, I will focus on the four remaining types of embedded radio modules, which I have selected according to their suitability for remote control. They are RADIOCRAFTS RC1180-MBUS3, ADEUNIS ARF7751CB, FRIENDCOM FC-703C, and AMBER AMB8426-M. All of them operate at the 868 MHz frequency band. Their basic parameters, such as dimensions, type of mounting, RF, RF sensitivity, operating voltage, output power, presence of LED notification for TX and RX, current consumption, operating voltage, encryption, UART interface data rate and role, will be discussed and also compared in the table below.

Frequency band 868 MHz	**Dimensions [mm]**	**Mounting**	**RF**	**RF sensitivity [dBm]**	**Operating voltage [V]**	**Output power [dBm]**
RADIOCRAFTS RC1180-MBUS3	25.4x12.7x3,3	SMD	R,S,T,C (868 MHz)	R: -106 S: -102 T: -101 C: not defined	2.0-3.9	Up to 9
ADEUNIS ARF7751CB	26.0x16.0x2.0	SMD hand	R,S,T,C (868 MHz) F (433 MHz) N (169MHz)	R: -117 S: -112 T: -110 C: not defined	2.0-3.6	Up to 15
FRIENDCOM FC-703C	25.4x13.7x3.4	SMD	R,S,T,C (868 MHz)	R: -107 S: -102 T: -102 C: not defined	2.0-3.6	Up to 11
AMBER AMB8426-M	27.0x17.0x4.0	SMD hand	R,S,T,C (868 MHz)	R: - 107 S: -103 T: -100 C: not defined	2.2-3.6	Up to 11

Tab. 1 Comparison of parameters 1

Frequency band 868 MHz	**LED notification for TX and RX**	**Current consumption [mA or µA]**	**Operating temperature [°C]**	**Encryption**	**UART interface data rate [Bd]**	**Role**
RADIOCRAFTS RC1180-MBUS3	Yes	TX: 37 mA RX: 24mA Sleep: 0.3 µA Standby: not defined	-40 to +85	AES 128	2400-230400	Slave Master Repeater
ADEUNIS ARF7751CB	No	TX: 35 mA RX: 22 mA Sleep: <0.2 µA Standby: <0.6 µA	-40 to +85	AES 128	115200	Slave Master Repeater?
FRIENDCOM FC-703C	Yes	TX: 38 mA RX: 24 mA Sleep: < 0.6 µA Standby: not defined	-40 to +80	AES 128	2400-230400	Slave Master Repeater
AMBER AMB8426-M	No	TX: 38mA RX: 24 mA Sleep: <0.3 µA Standby: not defined	-30 to +85	AES 128	1200-115200	Slave Master

Tab. 2 Comparison of parameters 2

4.1 Parameters overview

Dimensions: Dimensions are significant for embedded modules. They play an important role for manufacturers who place the embedded module to the meter or to the reading devices. Generally speaking, the smaller, the better.

Type of mounting: The embedded module has to be installed to the meter or to the reading device. The installation can be done using two different methods. The first one is the SMD (Surface Mount Devices). The SMD is automatic component placement, mainly used for production of large amounts of products. The other method is the installation by hand with the aid of a soldering iron, mostly used in small-scale production. Some of the embedded modules enable both installation methods.

RF: The RF (radio frequency) defines the operating modes for data transfer in which the embedded module is able to work. It is important to mention that a particular meter or a particular reading device cannot be set simultaneously in two or more modes. It works in one mode only. The basic features of the modes are mentioned below.

Operating modes

T mode (The Frequent Transmit Mode): Data will be automatically sent by the meter on a regular basis. The T mode is divided into the unidirectional data transfer T1 and the bidirectional data transfer T2. In the T1 one-way communication mode, the meter does not receive any data. It periodically reports the data and after the reporting the meter enters a low-power state. In the T2 two-way communication mode, the meter also reports the data, but after reporting, the data are received only during a short period of time. If the meter does not receive any data in this short time, it enters a low-power state. On the other hand, if the meter receives some data, it starts communicating with a concentrator. A typical example of application of T modes (T1 and T2) is the frequent data transmission (short frame meters).

R mode (The Frequent Receive Mode): A one-way communication R1 does not exist. There is only a two-way communication mode R2 which in the "multi-channel receive mode" *allows the simultaneous readout of several meters, each one operating on a different frequency channel* [6]. In the R2 mode, the data are not periodically sent by the

meter. The meter listens every few seconds if a wakeup message comes from a mobile transceiver. If the message is received, a two-way communication is started. The communication takes a few seconds. If the meter does not receive any wakeup message, it enters a low-power sleep state. A typical example of application of the R2 mode is the frequent data reception (long range).

S mode (The Stationary Mode): A one-way communication mode S1 and a two-way communication mode S2 exist. Both of these communication modes are performed between the meter and a stationary or mobile device. These modes are similar to the T modes, nevertheless, the difference between them could consist in the physical layer. A typical application of the S modes is a stationary readout.

C mode (The Compact Mode): The C mode is similar to the T mode but it is more cost-saving. It enables transmission of more data with the same energy budget. There is a one-way communication mode C1 and a two-way communication mode C2. A typical example of application of the C mode are walk-by and drive-by readout.

RF sensitivity: Generally speaking, the higher number of sensitivity, the weaker signal can be caught by the devices. On the other hand, if the meter is set only as a transmitter (in the R1, S1, T1, or C1 mode), it does not catch any data. Therefore, the RF sensitivity is meaningless in this case, whereas the value of the output power is important.

Operating voltage: The voltage range needed for devices so that they could work correctly. The voltages are usually in the range between two and four volts.

Output power: The value of the output power defines how strongly the device transmits the data. The higher number of output power, the higher power of transmission.

LED notification for TX and RX: The LED notification is a tool enabling an LED notification light. The reading devices notify the moment when they receive (RX) or transmit (TX) data by a light-emitting diode (LED). The meter does not have any notification. The main reason is uselessness. Another reason might be the desirability of energy saving.

Current consumption: The current consumption is different in every state of the

module. The embedded module has the highest electricity consumption when it transmits the data (TX), otherwise, when the module receives the data (RX), the electricity consumption is lower. The sleep mode and the standby mode have the lowest electricity consumption. In this case, the embedded module neither receives nor transmits any data. It sleeps and waits for its moment of activity.

Operating temperature: The operating temperature defines the temperature range measured in degrees Celsius in which the embedded module is able to work. This parameter can be significant if the meter with the embedded module is located in special places – exposed to very high or very low temperatures. Some producers also define the storage temperature of embedded modules.

Encryption: Because of sensitive data, telegrams from the meters are encrypted according to the Advanced Encryption Standard (AES) [12] which is used mainly in information technology. The key for encoding and decoding is the same. The encryption is called the "symmetric encryption".

UART interface data rate: It can be said in a very simple way that the UART interface data rate defines the transfer rate between the circuit and the microprocessor inside the embedded module. The UART interface data rate can usually be set to several rates available on the value scale.

Role: Each embedded module enables more roles. These roles are called: a slave, a master and a repeater. If the embedded module works as a master, it is placed in reading devices. If the embedded module works as a slave, it is placed in the meter. The repeaters listen to the data from one module and then repeat them.

4.2 Evaluation of parameters

4.2.1 From the representatives´ point of view

Before evaluating the embedded module parameters, I decided to ask representatives of RADIOCRAFTS, ADEUNIS, FRIENDCOM and AMBER why products of their company are better than products of other companies. Their full answers are mentioned in the appendix.

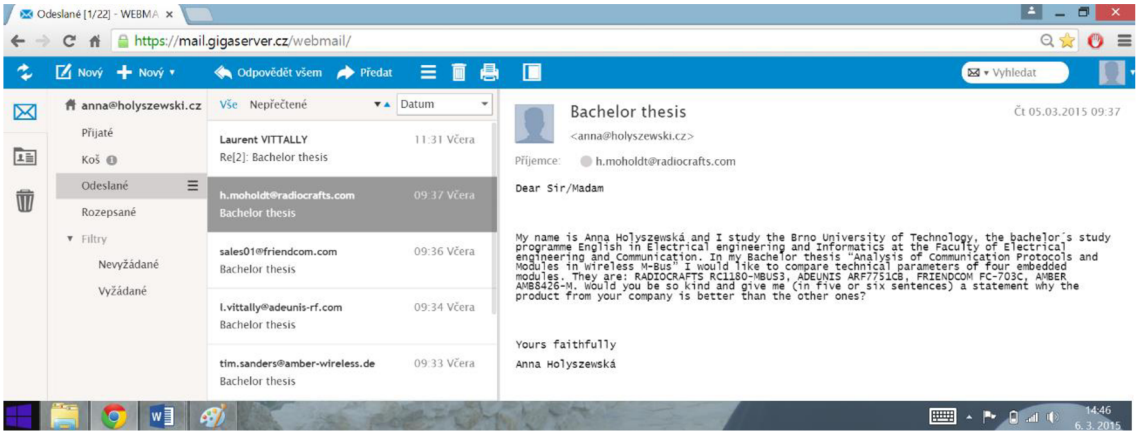


Fig. 1 Email

The first response that I received was from Laurent Vittally, the Customer Service Manager of Adeunis, France. The second response was from Hallvard Moholdt, the Technical Solutions Manager of Radiocrafts, Norway. And the third response was received from Linda Lv, the Sales engineer and the representative of Friendcom, China. Their full answers are included in the appendix. I did not receive any response from the representative of Amber.

I fully agree with Mr. Vittally from Adeunis. Their embedded modules are really very sensitive, especially if they are set on the R operating mode. He also highlighted the fact that Adeunis embedded modules enabled the C mode along with the usual T, S and R modes. That is true but the other three modules enable the C mode, too.

Mr. Moholdt from Radiocrafts mentioned that they had more than three hundred and fifty thousand pieces of embedded modules on the market. I am not able to prove this fact but there is a widespread belief that Radiocrafts is a technological leader in this branch in Europe.

Mrs. Lv, the sales engineer of Friendcom, pointed out that their embedded modules could match the other modules and they were also more cost-effective. This statement is true. Nevertheless, in the table she had provided Mrs. Lv compared parameters of different embedded modules than those I had asked her about. She presented parameters of ADEUNIS ARF7751BB instead of the new model ARF7751BC enabling the C operating mode and RADIOCRAFTS RC1180-MBUS in place of RC1180-MBUS3 with the C operating mode. In addition to that, Linda Lv claims that that AMBER AMB8426-M does not have the C mode at all. This statement is incorrect.

4.2.2 From my point of view

All embedded modules (RADIOCRAFTS RC1180-MBUS3, ADEUNIS ARF7751CB, FRIENDCOM FC-703C, and AMBER AMB8426-M) whose parameters are organized in the table were selected according to their availability in the Czech Republic and their suitability for the wireless M-Bus. It should be noted that all of these embedded modules have similar dimensions, however, the most significant parameter is their thickness. A very flat embedded module is mainly required for the meters. But if the USB Stick is used as a reading device, the thickness is important as well. According to the table, the most flat module is the product of ADEUNIS. ADEUNIS offers a module which is less than two millimetres thick, while the thickness of the other companies' modules is almost double. The rest of dimensions are not so important. Not only are the dimensions similar, but all embedded modules which have been compared enable the SMD mounting. What is more, the products of ADEUNIS and Amber can be installed by hand with the aid of a soldering iron. This type of installation is advantageous for companies that use the embedded module in a lower number of their products. I should mention that all modules could be set on the R, S, T, and C mode. There are no differences among them, while each of them has a different RF sensitivity. According to given parameters, the module of ADEUNIS, model ARF7751CB, has a higher RF sensitivity than other tested products in the R, S, T, and C mode. The RF sensitivity values are as follows: -117 dBm in R mode, -112 dBm in S mode and -110 dBm in T mode. The RF sensitivity in the C mode is not defined. A high sensitivity in modes is a big advantage for such devices where the data have to be received. Despite the fact that ARF7751CB has the highest RF sensitivity and also the largest output power, the electricity consumption is very low during the data transmission as well as the data reception. It is 35 mA for the transmission of telegrams (TX), and 22 mA for the reception of telegrams (RX). If the device sleeps, the electricity consumption is lower than 0.2 μA, which is also the lowest value compared with other modules. The device in the standby mode with the ADEUNIS embedded module needs only less than 0.6 μA. The module of RADIOCRAFTS, type RC1180-MBUS3, has the second lowest electricity consumption. The other modules have a slightly higher electricity consumption when they work and also when they sleep. On the other hand, only ADEUNIS's ARF7751CB is not endowed with the LED notification. The LED

notification consumes electricity but it is quite useful in reading devices for the light notification of transmission or receiving Wireless M-Bus telegrams. It is not mentioned in the table that ADEUNIS´s module enables the telegram filtering according to the producer's code. The operating voltage needed for devices to work correctly is exactly 2.0 to 3.6 V for FRIENDCOM FC-703C as well as for ADEUNIS ARF7751CB, 2.2 to 3.6 V for AMBER AMB8426-M, and 2.0 to 3.9 V for RADIOCRAFTS RC1180-MBUS3. One of the main parameters is how strongly the device transmits the data. It defines the output power. According to the table, ADEUNIS has the strongest output power – up to 15 dBm, and then FRIENDCOM and AMBER – up to 11 dBm. RADIOCRAFTS has the output power only up to 9 dBm. The operating temperature is similar for all modules. The RADIOCRAFTS module and the ADEUNIS module have slightly wider operating temperature range. For this reason, these modules can be installed in places with higher temperatures and a lower temperature, too. Their temperature range is from forty degrees below zero to eighty five degrees above zero. According to the table, FRIENDCOM FC-703C can operate from forty degrees below zero to eighty degrees above zero, and AMBER AMB8426-M from thirty degrees below zero to eighty five degrees above zero. Nevertheless, one can see that the differences are not big. All embedded modules use the Advanced Encryption Standard 128 (AES 128) [12] encryption in order to protect sensitive telegrams. The symmetric encryption provides an identical key for encoding and decoding the data. It is the UART interface data rate that has been mentioned as another parameter in the table. Although three of four embedded modules enable more than one data rate, according to the documentation of the ADEUNIS module, the type ARF7751CB offers only 115200 Bd. In reality, this module can communicate 38400 Bd, too, but it is not written there. Finally, each of the embedded modules is able to play more than one role in a system. AMBER AMB8426-M can be set as a master or a slave, while RADIOCRAFTS RC1180-MBUS3 and FRIENDCOM FC-703C are able to act as repeaters, too. They listen to the data from a module and then repeat the data. For this reason, another distant embedded module can listen to these telegrams. It is not evident if the ARF7751CB can be used as a repeater. This parameter is not clearly defined in its documentation.

5 DATA ANALYSIS

In this chapter data from the heat meter Kamstrup Multical 402 will be analysed in detail. The data analysis will be done mainly according to the European Standard 13757-4: Communication systems for meters and remote reading of meters - Part 4 [1], The M-Bus: A Documentation Rev. 4 [5] and Open Metering System Specification: Volume 2, Primary Communication [7].

Firstly, the data from the meters are read using the embedded module AMBER AMB8426-M set in one particular operating mode. The heat meter sends the data which are displayed in the computer as values in a hexadecimal numeral system. Secondly, the AMBER Commander V1.2 software supplied with AMBER AMB8426-M reads these values in the hexadecimal numeral system and it is able to recognize some of the basic features of the meter e.g. the Manufacturer ID, the Identification number, the Device Type Information and the RSSI (Received Signal Strength Indicator). An example of data reading by this program can be seen in the Fig. 2 (see below). It should be mentioned that the example does not show the values from Kamstrup Multical 402 that will be analysed. Thirdly, an encryption key is written in the manufacturer´s manual. If the encryption key is known this way, the other available program MBT1USB is able to decrypt it using the Advanced Encryption Standard 128 (AES 128) [12]. Some manufacturers of meters use special encryption keys which are not written in their documentations. For this reason, we are not able to decrypt the values and then analyse them.

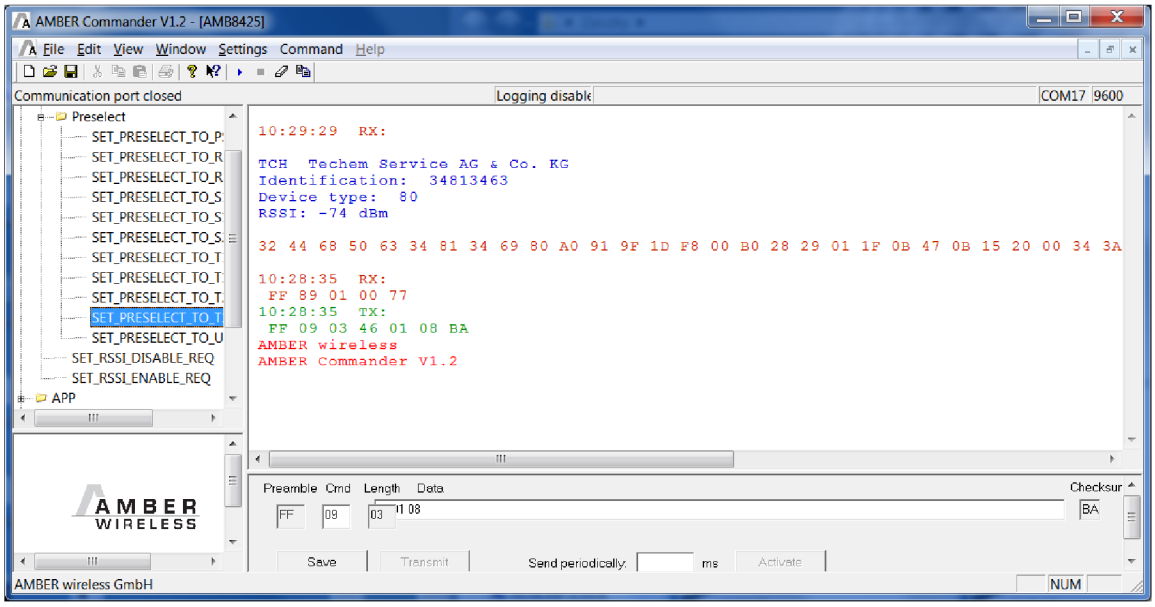


Fig. 2 AMBER Commander V1.2

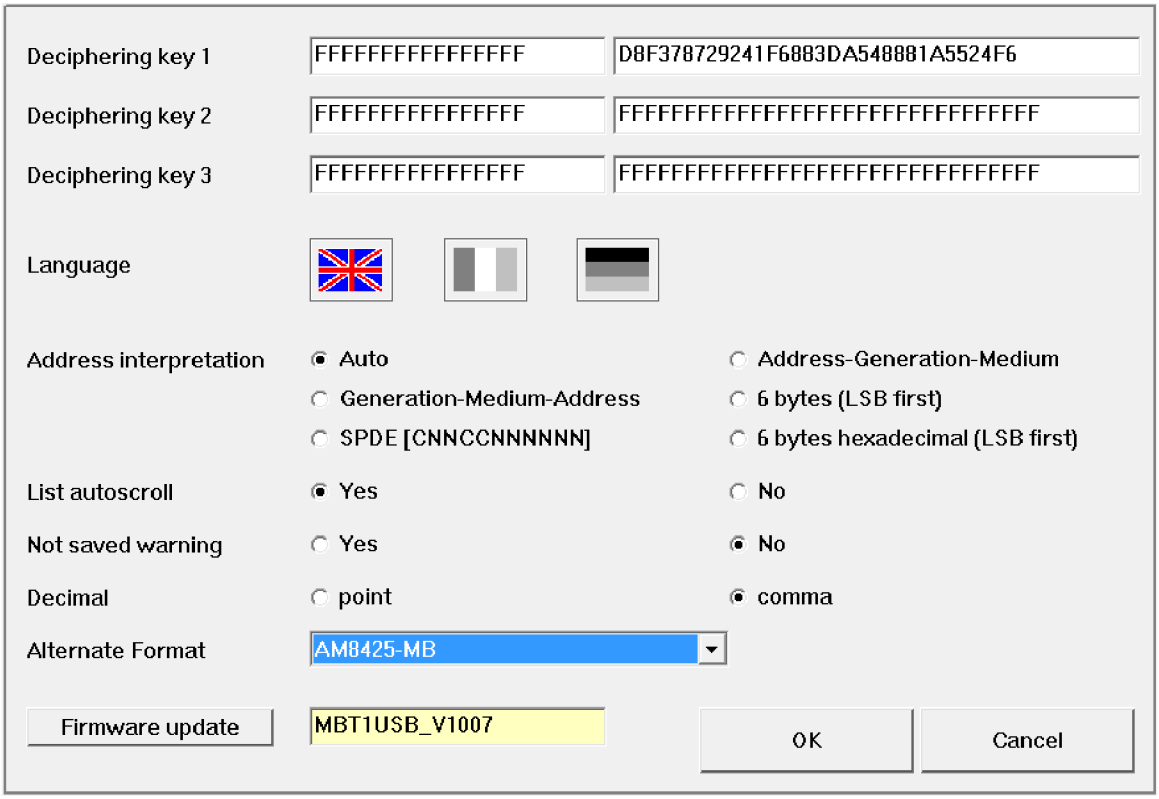


Fig. 3 Encryption key in MBT1USB

5.1 Heat meter Kamstrup Multical 402

The data from Kamstrup Multical 402 were read by AMBER Commander V1.2 set on the operating mode T1. There is the data telegram of this heat meter displayed in the program:

5E442D2C9643636013047AD21050084535BEF5623858243FF4961635B6D30017F
E12743EEC8D5757B0A3EC5E0BB052ABDBF71A75179A1340D01389E144F861F
56780A3F8E1543E2368676A7BDC26214D2330757F0684421A3D5B1E4C781B8

Afterwards, the highlighted values in the data telegram were decrypted in the program MBT1USB according to AES 128 [12]. The encryption key was D8F378729241F6883DA548881A5524F6. We obtained the following values.

5E442D2C9643636013047AD21050052F2F0422BA11000004140F000000043B0000
000002FD1700100259A50A026CB316426CBF1544140F000000040F02000000025D
AF0A04FF070600000004FF0802000000440F020000002F2F2F2F2F2F2F

The first part of the data telegram remained the same because of the regulation in the Open Metering System Specification. The highlighted part was changed.

The whole data telegram is arranged in different blocks according to "Frame format A" which is described in EN 13757-4 [1]. Each block has more than one field. In the data telegram one couple of values represents one byte and the number of bytes has to be multiple of sixteen according to AES 128 [12]. If the number of bytes is not the multiple of sixteen, the program adds extra values "2F". These extra values also verify that the telegram is decrypted correctly. They are described later.

The fields of the first block

Length field (L-field)	**Control field** (C-field)	**Manufacturer ID field** (M-field)	**Address field** (A-field)	**Cyclic redundancy check field** (CRC-field)

The fields of the second block

Control information field (CI-field)	**Data-field**	**Cyclic redundancy check field** (CRC-field)

The fields of the third block

Data-field	**Cyclic redundancy check field** (CRC-field)

Tab. 3 Frame format A

5E 44 2D 2C 96 43 63 60 13 04 7A D2 10 50 05 2F 2F 04 22 BA 11 00 00 04 14 0F 00 00 00 04 3B 00 00 00 00 02 FD 17 00 10 02 59 A5 0A 02 6C B3 16 42 6C BF 15 44 14 0F 00 00 00 04 0F 02 00 00 00 02 5D AF 0A 04 FF 07 06 00 00 00 04 FF 08 02 00 00 00 44 0F 02 00 00 00 **2F 2F 2F 2F 2F 2F 2F**

THE BEGINNING OF THE DATA TELEGRAM

L-field

$5E_{(16)} = 94_{(10)}$

The Length field contains the first byte of the first block. This field determines the number of bytes in the whole data telegram. There are ninety four bytes without the first one (5E). This value is not send by the heat meter but the AMBER AMB8426-M add it to the telegram.

C-field

The Control field contains the second byte of the first block and determines the frame type according to the table below.

RES	PRM	FCB ACD	FCV DFC	Function code			
0	1	0	0	0	1	0	0
0	1	0	0	4			

Tab. 4 Data format of C-field

$4_{(16)} = 0100_{(2)}$

The bit in RES is always zero. If the PRM is one (binary number system), it means that the data go from the meter to the receiver. If the PRM is zero, the data go from the receiver to the meter. In this case, there is number one placed there. Therefore, the transmission takes place from the Kamstrup Multical 402 to the receiver (embedded module AMBER AMB8426-M). FCB, FCV and ACD, DFC bit are coded according to EN 60870-5-2.

$4_{(16)}$ = Function code - Send unsolicited/periodical application data without any request (Send/No Reply). It is compulsory for S2, T2, C2, R2, N2 and F2 operation modes.

M-field

The Manufacturer ID field contains the third and the fourth byte of the first block. This Manufacturer ID, also called User ID is formed from three letters using Ascii table. The values must be read in reverse number but in couples. Therefore, we obtain KAM.

$2D\ 2C_{(16)} = 2C\ 2D_{(16)} = 0\ 01011\ 00001\ 01101_{(2)}$ = Manufacturer ID

$01011_{(2)} = 11_{(10)} + 64_{(10)} = 75_{(10)}$ = **K** according to Ascii table

$00001_{(2)} = 1_{(10)} + 64_{(10)} = 65_{(10)}$ = **A** according to Ascii table

$01101_{(2)} = 13_{(10)} + 64_{(10)} = 77_{(10)}$ = **M** according to Ascii table

A-field

The Address field contains the Identification number (serial number allocated during manufacture), the Version number and the Device type information. The first four bytes of the A-field usually represent the Identification number of the meter. These values must be read from the back but in couples so we obtain 60 63 43 96. Then, the Version number is placed there and the last byte represents the Device type.

96 43 63 60 = 60 63 43 96 = Identification number

$13_{(16)}$ = 0001 0011$_{(2)}$ = Version number

$04_{(16)}$ = 0000 0100$_{(2)}$ = Device type - heat meter (Volume measured at return temperature: outlet)

CRC-field

The CRC shall be computed over the information from the previous block, and shall be generated according to FT3 of EN 60870-5-1. The formula is: $x^{16} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^2 + 1$. *The initial value is 0. The final CRC is complemented* [7]. However, the CRC is not displayed in the data telegram. It is a control value for the module.

CI-field

The Control information field contains the first byte of the second block and determines the type of protocol. For this reason, it is known what information will follow.

7A = Type of following application protocol - Application protocol is M-Bus (EN 13757-3)

Data-field

$D2_{(16)}$ = 1101 0010$_{(2)}$ = Access number

The Access number is increased by one (in binary coding) with each new data transmission from the slave. The next value should be $D3_{(16)}$ = 1101 0011$_{(2)}$.

$10_{(16)}$ = 0001 0000$_{(2)}$ = Status – meter temporary error

If the CI-field is $7A_{(16)}$, the Status is error of the meter. In this case, it is the temporary error according to the Open Metering System Specification: Volume 2, Primary Communication [7].

50 $05_{(16)}$ = 05 $50_{(16)}$ = $0000\ 0101\ 0101\ 0000_{(2)}$ = Signature – Configuration Word according to the Open Metering System Specification: Volume 2, Primary Communication [7]. The Configuration Word mode is five because of the mode bits $0101_{(2)} = 5_{(10)}$. The number of following encryption blocks is five according to $0101_{(2)} = 5_{(10)}$.

Bidirectional communication	accessibility	synchronous	reserved	mode bit3	mode bit2	mode bit1	mode bit0	number of encr. blocks	number of encr. blocks	number of encr. blocks	number of encr. blocks	content of telegram	content of telegram	hop counter	hop counter
0								**0**	**1**	**0**	**1**				

Tab. 5 Configuration Word table

Meter data

The structure of the meter data is given according to the M-BUS Standard because of the value in the CI-field. The highlighted values in the data telegram part have been decrypted (using AES 128) [12] and they will be analysed. Verification of correct decryption in mode five is done using two idle fillers at the beginning of this data telegram part.

Data Information Block (DIB)		**Value Information Block** (VIB)		
Data Information Field (DIF)	**Data Information Field Extension** (DIFE)	**Value Information Field** (VIF)	**Value Information Field Extension** (VIFE)	**Data**

Tab. 6 Structure of Meter data

$2F_{(16)}$ = 0010 $1111_{(2)}$ = Idle Filler (not to be interpreted), DIF is the following byte.

$2F_{(16)}$ = 0010 $1111_{(2)}$ = Idle Filler (not to be interpreted), DIF is the following byte.

04 22 BA 11 00 00

DIF = $04_{(16)}$ = 0000 $0100_{(2)}$ = LSB of storage number 0, Instantaneous value, 32 Bit Integer (Data type B)

Extension Bit	**LSB of storage number**	**Function field**	**Data**
0	0	00	0100

Tab. 7 General coding of DIF

Code	**The next information is contained in:**
0	DIF
1	DIFE

Tab. 8 Coding of Extension Bit in DIF

Code	Description	Code	Description
00b	Instantaneous value	01b	Maximum value
10b	Minimum value	11b	Value during error state

Tab. 9 Coding of Functional field in DIF [8]

Length in Bit	Code	Meaning	Code	Meaning
0	0000	No data	1000	Selection for Readout
8	0001	8 Bit Integer	1001	2 digit BCD
16	0010	16 Bit Integer	1010	4 digit BCD
24	0011	24 Bit Integer	1011	6 digit BCD
32	0100	32 Bit Integer	1100	8 digit BCD
32 / N	0101	32 Bit Real	1101	variable length

Tab. 10 Coding the data in DIF [9]

Extension Bit is 0. Therefore, DIFE is omitted and the next byte is VIF. If the Extension Bit is 1, DIFE will follow. LSB of storage number is 0. In the function field 00 is placed. It means that the meter sends an instantaneous value. Data is 0100. For this reason, the next information is contained in 32 Bit Integer number = 4 bytes (each of them has 8 bits). The Integer number is defined by Data type B (Binary Integer) where the first sign indicates positive (0) or negative (1) value.

VIF = $22_{(16)}$ = $0010\ 0010_{(2)}$ = On Time, hours

Extension Bit	Data
0	010 0010

Tab. 11 General coding of VIF

Code	The next information is contained in:
0	VIF
1	VIFE

Tab. 12 Coding of Extension Bit in VIF

Coding	Description	Range Coding	Range
E000 0nnn	Energy	$10^{(nnn-3)}$ Wh	0.001 Wh to 10000 Wh
E000 1nnn	Energy	$10^{(nnn)}$ J	0.001 kJ to 10000 kJ
E001 0nnn	Volume	$10^{(nnn-6)}$ m3	0.001l to 10000l
E001 1nnn	Mass	$10^{(nnn-3)}$ kg	0.001 kg to 10000 kg
E010 00nn	On Time	nn = 00 seconds nn = 01 minutes nn = 10 hours nn = 11 days	
E010 01nn	Operating Time	coded like OnTime	
E010 1nnn	Power	$10^{(nnn-3)}$ W	0.001 W to 10000 W
E011 0nnn	Power	$10^{(nnn)}$ J/h	0.001 kJ/h to 10000 kJ/h
E011 1nnn	Volume Flow	$10^{(nnn-6)}$ m3/h	0.001 l/h to 10000 l/h
E100 0nnn	Volume Flow ext.	$10^{(nnn-7)}$ m3/min	0.0001 l/min to 1000 l/min
E100 1nnn	Volume Flow ext.	$10^{(nnn-9)}$ m3/s	0.001 ml/s to 10000 ml/s
E101 0nnn	Mass flow	$10^{(nnn-3)}$ kg/h	0.001 kg/h to 10000 kg/h
E101 10nn	Flow Temperature	$10^{(nn-3)}$ °C	0.001 °C to 1 °C

E101 11nn	Return Temperature	$10^{(nn-3)}$ °C	0.001 °C to 1 °C
E110 00nn	Temperature Difference	$10^{(nn-3)}$ K	1 mK to 1000 mK
E110 01nn	External Temperature	$10^{(nn-3)}$ °C	0.001 °C to 1 °C
E110 10nn	Pressure	$10^{(nn-3)}$ bar	1 mbar to 1000 mbar
E110 110n	Time Point	n = 0 date n = 1 time & date	data type G data type F
E110 1110	Units for H.C.A.		dimensionless
E110 1111	Reserved		
E111 00nn	Averaging Duration	coded like OnTime	
E111 01nn	Actuality Duration	coded like OnTime	
E111 1000	Fabrication No		see chapter 6.4.2 §
E111 1001	(Enhanced) Identification		data type C (x=8)
E111 1010	Bus Address		data type C (x=8)

Tab. 13 Coding the data in VIF [10]

BA 11 00 $00_{(16)}$ = 00 00 11 $BA_{(16)}$ = $4538_{(10)}$ hours

The Extension Bit is 0. Therefore, there is not VIFE. LSB of storage number is 0, the meter was switched on 4538 hours ago.

04 14 0F 00 00 00

DIF = $04_{(16)}$ = 0000 $0100_{(2)}$ = LSB of storage number 0, Instantaneous value, 32 Bit Integer (Data type B)

VIF = $14_{(16)}$ = 0001 $0100_{(2)}$ = Volume 10^{4-6} m^2 = 0,01 m^2

0F 00 00 $00_{(16)}$ = 00 00 00 $0F_{(16)}$ = $15_{(10)}$ = 15 x $0.01_{(10)}$ = $0.15_{(10)}$ m^2

04 3B 00 00 00 00

DIF = $04_{(16)}$ = 0000 $0100_{(2)}$ = LSB of storage number 0, Instantaneous value, 32 Bit Integer (Data type B)

VIF = $3B_{(16)}$ = 0011 $1011_{(2)}$ = Volume Flow 10^{3-6} m^3/hod = $l_{(10)}$ /hod

$011_{(2)}$ = $3_{(10)}$

$00000000_{(16)}$ = $00000000_{(16)}$ = $0_{(10)}$ = $0_{(10)}$ m^3/hod

02 FD 17 00 10

DIF = $02_{(16)}$ = 0000 $0010_{(2)}$ = LSB of storage number 0, Instantaneous value, 16 Bit Integer (Data type B)

VIF = $FD_{(16)}$ = 1111 $1101_{(2)}$ = Extension of VIF-codes

Coding	Description
1111 1011	Extension of VIF-codes
E111 1100	VIF in following string (length in first byte)
1111 1101	Extension of VIF-codes
E111 1110	Any VIF
E111 1111	Manufacturer Specific

Tab. 14 VIF-Codes for special purposes [11]

VIFE = $17_{(16)}$ = 0001 $0111_{(2)}$ = Error flags (binary) – this information is written in: The M-Bus: A Documentation Rev. 4, Appendix [12].

$00\ 10_{(16)} = 10\ 00_{(16)} = 4096_{(10)}$

02 59 A5 0A

DIF = $02_{(16)}$ = 0000 $0010_{(2)}$ = LSB of storage number 0, Instantaneous value, 16 Bit Integer (Data type B)

VIF = $59_{(16)}$ = 0101 $1001_{(2)}$ = Flow Temperature $10^{1\text{-}3}$°C = $0{,}01_{(10)}$ °C

$A5\ 05_{(16)} = 0A\ A5_{(16)} = 2725_{(10)} = 2725 \times 0{,}01_{(10)} = 27.25_{(10)}$ °C

02 6C B3 16

DIF = $02_{(16)}$ = 0000 $0010_{(2)}$ = LSB of storage number 0, Instantaneous value, 16 Bit Integer (Data type B)

VIF = $6C_{(16)}$ = 0110 $1100_{(2)}$ = Time Point, date, data type G

$B3\ 16_{(16)} = 16\ B3_{(16)} = $ *0001* 0110 *101* **10011**$_{(2)}$ = 19. 6 2013

Year				**Month**				**Year**			**Day**				
15	*14*	*13*	*12*	11	10	9	8	*7*	*6*	*5*	**4**	**3**	**2**	**1**	**0**

Tab. 15 Data type G

Day **10011**$_{(2)}$ = $19_{(10)}$

Month $0110_{(2)}$ = $6_{(10)}$

Year *0001101*$_{(2)}$ = $13_{(10)}$

42 6C BF 15

DIF = $42_{(16)}$ = 0100 $0010_{(2)}$ = LSB of storage number 1, Instantaneous value, 16 Bit Integer (Data type B)

VIF = $6C_{(16)}$ = 0110 $1100_{(2)}$ = Time Point, date, data type G

15BF = *0001* 0101 *101* **11111**$_{(2)}$ = 31. 5. 2013

Day **11111**$_{(2)}$ = $31_{(10)}$

Month $0101_{(2)}$ = $5_{(10)}$

Year *0001101*$_{(2)}$ = $13_{(10)}$

44 14 0F 00 00 00

DIF = $44_{(16)}$ = 0100 $0100_{(2)}$ = LSB of storage number 1, Instantaneous value, 32 Bit Integer (Data type B)

VIF = $14_{(16)}$ = 0001 $0100_{(2)}$ = Volume 10^{4-6} m^2 = $0{,}01_{(10)}$ m^2

0F 00 00 $00_{(16)}$ = 00 00 00 $0F_{(16)}$ = $15_{(10)}$ = 15 x $0.01_{(10)}$ = $0{,}15_{(10)}$ m^2

04 0F 02 00 00 00

DIF = $04_{(16)}$ = 0000 $0100_{(2)}$ = LSB of storage number 0, Instantaneous value, 32 Bit Integer (Data type B)

VIF = $0F_{(16)}$ = 0000 $1111_{(2)}$ = Energy 10^7 J = $10_{(10)}$ MJ

02 00 00 $00_{(16)}$ = 00 00 00 $02_{(16)}$ = $2_{(10)}$ = 2 x $10_{(10)}$ = $20_{(10)}$ MJ

02 5D AF 0A

DIF = $02_{(16)}$ = 0000 $0010_{(2)}$ = LSB of storage number 0, Instantaneous value, 16 Bit Integer (Data type B)

VIF = $5D_{(16)}$ = 0101 $1101_{(2)}$ = Return Temperature 10^{1-3}°C = $0{,}01_{(10)}$ °C

AF $A0_{(16)}$ = 0A $AF_{(16)}$ = $2735_{(10)}$ = 2735 x $0.01_{(10)}$ = $27{,}35_{(10)}$ °C

04 FF 07 06 00 00 00

DIF = $04_{(16)}$ = 0000 $0100_{(2)}$ = LSB of storage number 0, Instantaneous value, 32 Bit Integer (Data type B)

VIF = $FF_{(16)}$ = 1111 $1111_{(2)}$ = Manufacturer Specific

VIFE = $07_{(16)}$ = 000 $0111_{(2)}$ = VIFE is manufacturer specific

06 00 00 $00_{(16)}$ = 00 00 00 $06_{(16)}$ = $6_{(10)}$

04 FF 08 02 00 00 00

DIF = 04 = 0000 0100 = LSB of storage number 0, Instantaneous value, 32 Bit Integer (Data type B)

VIF = $FF_{(16)}$ = 1111 $1111_{(2)}$ = Manufacturer Specific

VIFE = $08_{(16)}$ = 0000 $1000_{(2)}$ = VIFE is manufacturer specific

02 00 00 $00_{(16)}$ = 00 00 00 $02_{(16)}$ = $2_{(10)}$

44 0F 02 00 00 00

DIF = $44_{(16)}$ = 0100 $0100_{(16)}$ = LSB of storage number 1, Instantaneous value, 32 Bit Integer (Data type B)

VIF = $0F_{(16)}$ = 0000 $1111_{(16)}$ = Energy 10^7 J = $10_{(10)}$ MJ

02 00 00 $00_{(16)}$ = 00 00 00 $02_{(16)}$ = $2_{(10)}$ = 2 x $10_{(10)}$ = $20_{(10)}$ MJ

2F$_{(16)}$ = 0010 $1111_{(2)}$ = Idle Filler (not to be interpreted), DIF is the following byte.

2F$_{(16)}$ = 0010 1111$_{(2)}$ = Idle Filler (not to be interpreted), DIF is the following byte.

2F$_{(16)}$ = 0010 1111$_{(2)}$ = Idle Filler (not to be interpreted), DIF is the following byte.

2F$_{(16)}$ = 0010 1111$_{(2)}$ = Idle Filler (not to be interpreted), DIF is the following byte.

2F$_{(16)}$ = 0010 1111$_{(2)}$ = Idle Filler (not to be interpreted), DIF is the following byte.

2F$_{(16)}$ = 0010 1111$_{(2)}$ = Idle Filler (not to be interpreted), DIF is the following byte.

2F$_{(16)}$ = 0010 1111$_{(2)}$ = Idle Filler (not to be interpreted), DIF is the following byte.

THE END OF THE DATA TELEGRAM

5.2 Heat cost allocator Techem

The data from Techem were read by AMBER Commander V1.2 set on the operating mode T1. There is the data telegram of this heat cost allocator displayed in the program:

32 44 68 50 63 34 81 34 69 80 A0 91 9F 1D F8 00 D0 28 29 01 60 0C AE 0C 15 20 00 34 3A 39 23 28 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

THE BEGINNING OF THE DATA TELEGRAM

L-field

32$_{(16)}$ = 50$_{(10)}$ = The length of data telegram

C-field

4$_{(16)}$ = 0100$_{(2)}$ = Data go from the meter to the receiver

4$_{(16)}$ = Function code – (Send/No Reply)

M-field

68 50$_{(16)}$ = 50 68$_{(16)}$ = 10100 00011 01000$_{(2)}$ = Manufactured ID

10100$_{(2)}$ = 20$_{(10)}$ + 64$_{(10)}$ = 84 $_{(10)}$ = **T** according to Ascii table

00011$_{(2)}$ = 3$_{(10)}$ + 64$_{(10)}$ = 67$_{(10)}$ = **C** according to Ascii table

01000$_{(2)}$ = 8$_{(10)}$ + 64$_{(10)}$ = 72$_{(10)}$ = **H** according to Ascii table

A-field

$63\ 34\ 81\ 34_{(16)}$ = 34 81 34 $63_{(16)}$ = Identification Number

$69_{(16)}$ = 0110 $1001_{(2)}$ = Version number

$80_{(16)}$ = 1000 $0000_{(2)}$ = Device Type – Heat cost allocator

CI-field

A0 = The following data are encoded according to manufacturer specifications

Data-field

91 9F 1D F8 00 D0 28 29 01 60 0C AE 0C 15 20 00 34 3A 39 23 28 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

It is not possible to analyse these values because of A0 in CI-field. The manufacturer has his own cipher for coding the data.

THE END OF THE DATA TELEGRAM

6 CONLUSION

To conclude, I would like to sum up the information I have presented in the thesis. Firstly, types of meters and reading methods of the values on the meters were theoretically elaborated. I presented the basic features of heat meters, water meters and heat cost allocators as well as four methods of data reading from them. They are the following: visual reading, wired M-Bus reading, Radio reading (Wireless M-Bus) and Automatic Meter Reading. My thesis deals mainly with Wireless M-Bus as the only auspicious method that will be used in the future. I introduced the European Standard 13757-4 and the Open Metering System Specification (OMS) as fundamental documents for the radio reading of meters. Different types of embedded modules enabling radio communication between the meters and reading devices were identified. Their parameters were compared in a table and discussed in detail. While it was found that the parameters of RADIOCRAFTS RC1180-MBUS3 embedded module, ADEUNIS ARF7751CB embedded module, FRIENDCOM FC-703C embedded module and AMBER AMB8426-M embedded module are very similar, ADEUNIS ARF7751CB has slightly better features than the other three modules. Its advantage is very high RF sensitivity and high output power. In addition, ARF7751CB has the lowest current consumption. On the other hand, the embedded modules from Radiocrafts are widespread in Europe. I also made an experimental collection of data telegrams from the heat meter Kamstrup Multical 402 and the heat cost allocator Techem using the embedded module AMBER AMB8426-M. These telegrams were analysed. Despite the assumption that it is possible to decrypt all values in the data telegram according to the standards, I realized that this information is not true. Data contents and their encoding can be non-publicly specified by the manufacturer.

WORKS CITED

(1) M-BUS USERGROUP, *The M-Bus: A Documentation Version 4.8*, Introduction, November 11. 1997, Paderborn, [online], accessed 23. 03. 2015, http://www.m-bus.com/mbusdoc/md1.php

(2) EN 13757-4. *EUROPEAN STANDARD: Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands)*, European Committee for Standardization: Management Centre, 2013, p. 1.

(3) EN 13757-4. *EUROPEAN STANDARD: Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands)*, European Committee for Standardization: Management Centre, 2013, p. 4.

(4) OMS: Open Metering System, [online], accessed 08. 02. 2015, http://oms-group.org/en/oms-group/about-oms-group/

(5) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*: Advanced Encryption Standard (AES)*, Federal Information Processing Publications 197, 2001 p. i.

(6) EN 13757-4. *EUROPEAN STANDARD: Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands)*, European Committee for Standardization: Management Centre, 2013 p. 6.

(7) EN 13757-4. *EUROPEAN STANDARD: Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands)*, European Committee for Standardization: Management Centre, 2013, p. 34.

(8) M-BUS USERGROUP, *The M-Bus: A Documentation Version 4.8*, 6 Application Layer, Variable Data Structure, November 11. 1997, Paderborn, [online], accessed 13. 04. 2015 http://www.m-bus.com/mbusdoc/md6.php

(9) M-BUS USERGROUP, *The M-Bus: A Documentation Version 4.8*, 6 Application Layer, Variable Data Structure, November 11. 1997, Paderborn, [online], accessed 13. 04. 2015, http://www.m-bus.com/mbusdoc/md6.php

(10) M-BUS USERGROUP, *The M-Bus: A Documentation Version 4.8*, Appendix, Tables for Variable Data Structure, November 11. 1997, Paderborn, [online], accessed 13. 04. 2015, http://www.m-bus.com/mbusdoc/md8.php

(11) M-BUS USERGROUP, *The M-Bus: A Documentation Version 4.8*, Appendix, Tables for Variable Data Structure, November 11. 1997, Paderborn, [online], accessed 13. 04. 2015, http://www.m-bus.com/mbusdoc/md8.php

(12) M-BUS USERGROUP, *The M-Bus: A Documentation Version 4.8*, Appendix, Tables for Variable Data Structure, November 11. 1997, Paderborn, [online], accessed 13. 04. 2015, http://www.m-bus.com/mbusdoc/md8.php

BIBLIOGRAPHY

[1] EN 13757-4. *EUROPEAN STANDARD: Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands)*, European Committee for Standardization: Management Centre, 2013.

[2] RADIOCRAFTS: *Wireless M-Bus Multi-Mode RF Transceiver Module, RC1180-MBUS Data Sheet*, 2010

[3] HW SERVER S.R.O.: *Automatizace.hw.cz*, [online], accessed 12. 12. 2014, http://automatizace.hw.cz/sbernice-wireless-mbus-jde-i-bezdratove

[4] MIAMI-DADE COUNTY: *Miamidade.gov*, [online], accessed 12. 12. 2014, http://www.miamidade.gov/water/water-meter-read.asp

[5] M-BUS USERGROUP, *The M-Bus: A Documentation Version 4.8*, November 11. 1997, Paderborn, [online], accessed 13. 04. 2015, http://www.m-bus.com

[6] FRIENDCOM: *FC-703 Software User Guide,* Ver. 3.2: Friendcom, 2013

[7] OPEN METERING SYSTEM SPECIFICATION: *Volume 2, Primary Communication,* Issues 3.0.1, 2011

[8] ADEUNIS RF: *Wireless M-Bus, Adeunis RF products, Application note - Frame decoding*, Version V1.1,

[9] ADEUNIS RF: *Wireless M-Bus AES/OMS RF TRX 25mW module – 868MHz*, User guide version V2.3

[10] RADIOCRAFTS: *MBUS User Manual,* 2011

[11] AMBER WIRELESS GMBH: *AMBER WIRELESS*, accessed 10. 4. 2015, https://www.amber-wireless.com/

[12] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*: Advanced Encryption Standard (AES)*, Federal Information Processing Publications 197, 2001

APPENDIX

Representatives of RADIOCRAFTS, ADEUNIS, FRIENDCOM

Laurent Vittally, the Customer Service Manager - ADEUNIS

Dear Anna,

Thank you for your email.

The advantages of our Wireless M-Bus module ARF7751CB in comparison with our competitors are:

- *Very high sensitivity (-117 dBm) + RF output power (14 dBm) = important RF link budget (-131 dB) with a range up to 1000 m*
- *C1 mode embedded along with the usual T/S/R modes*
- *Compatible with OMS Mode 5 standard*
- *RF datarate up to 100 kbps*

Kind regards,

Laurent

Hallvard Moholdt, the Technical Solutions Manager – RADIOCRAFTS

Dear Anna;

Thank you for your email.

Radiocrafts is a member of TC294, OMS and the Wireless M-Bus working groups. We are behind many of the modes in Wireless M-Bus and were first in the market with proven interoperation.

But this does not necessarily mean we are leading right now :-) I think these are our main benefits;

- *Well field proven with > 350k pcs in the field*
- *We do have a patented two-way support solution, with a message mailbox system enabling pre-cooked messages to be stored inside the module, so that the Master can respond to a battery-operated Slave within the limitations of 2-3 ms. We are investigating if some of our competitors violate this patent. But for sure, we do have a very good support for two-way acknowledge to battery operated Slaves*

- *Our modules support C-mode. We are also now together with OMS implementing C mode at 433 MHz. This will do so that customers using 868 MHz can have footprint compatible modules with full 433 MHz support for regions not allowing 868 MHz, or preferring to use 433 MHz due to its better range. We do also support all frequencies and modes in the OMS amendment, see attachment, in footprint compatible modules. This might be more interesting for metering manufacturers to implement Wireless M-Bus as their market gets bigger with the same meter-design.*
- *Our T-mode at 868 MHz supports the wide bit-rate tolerance that is required in the standard. This is a standard requirement which has to be there in order to receive data from old water meters. I am not sure if all competitors actually has implemented this wide RF data rate tolerance*
- *We do have support in the Master support for up to 64 AES128 decryption keys to be installed*
- *Radiocrafts will soon introduce a mesh network backbone for our Wireless M-Bus modules for un-limited range extensions*
- *Finally, we do have footprint compatible modules for 169 MHz Wireless M-Bus (N-mode), 433 MHz (as mentioned above), KNX RF (For home-automation) and Tinymesh, which is ideal for Smart Electricity Meters (more than 400k pcs deployed in the field). We do also have footprint-compatible ZigBee, but it is not so popular for metering in Europe (except for UK)*

I hope the above information can be useful and wish you good luck with your thesis. Please let me know if we can be of any further assistance.

Best regards,

Hallvard Moholdt

Linda Lv, the Sales engineer – FRIENDCOM

Hi Anna,

This is Linda,sales engineer from Friendcom.Wish you suceed on your Bachelor thesis. Sorry to delay your email as we just start to work last week and it was too busy to give you a fully reply. I can give you a comparation file that indicates all the specification about the modules that you are doing the research.Pls check the below picture.

On specification,our module is equally mached with these modules you provided to me. At the same time, our module is more cost-effective.

Are you now on the study of these MBUS module or you will have project that will use these MBUS protocal module?

I have also written thesis and received Best Paper Award level province,if there is anything i can do to help you,just freely contact me.

	Adeunis	Amber	Radiocraft	Friendcom
Serial Number	ARF7751BB	AMB8426-M	RC1180-MBUS	FC-703C
Working Modes	S,T,R	S,T,R	S,T,R	S,T,R,C
Transmission Range	1000m	700m	500～600	600
Output power	14dBm (25mW)	11dBm	10dBm	11dBm
Sensitivity(Payload 20bytes，BER<0.01 or PER<0.8)	S Mode：-112dBm	S Mode：-103dBm	S Mode：-102dBm	S Mode：-102dBm
	T Mode：-110dBm	T Mode：-100dBm	T Mode：-101dBm	T Mode：-102dBm
	R Mode：-117dBm	R Mode：-107dBm	R Mode：-106dBm	R Mode：-107dBm
Operation Voltage (V)	2.0～3.6	2.2～3.6	2.0～3.9	2.0~3.6
Power Consumption	Tx Current：35mA	Tx Current：38mA	Tx Current：37mA	Tx Current：38mA
	Rx Current：22mA	Rx Current：24mA	Rx Current：24mA	Rx Current：24mA
	Standby：<0.6uA	Low Power：<0.3uA	Sleep：typical 0.3uA max 1uA	Sleep：0.6uA
	Sleep: <0.2uA			
Size (mm)	16×26×2	17×27×4	12.7 x 25.4 x 3.3	13.7×25.4×3.4
Operating Temperature (℃)	-40～+80	-30～+85	-40～+85	-40～+80
Weight (g)	N/A	3	N/A	5
Encryption	AES128	AES128	AES128	AES128

Linda Lv Oversales department

Kamstrup Multical 402

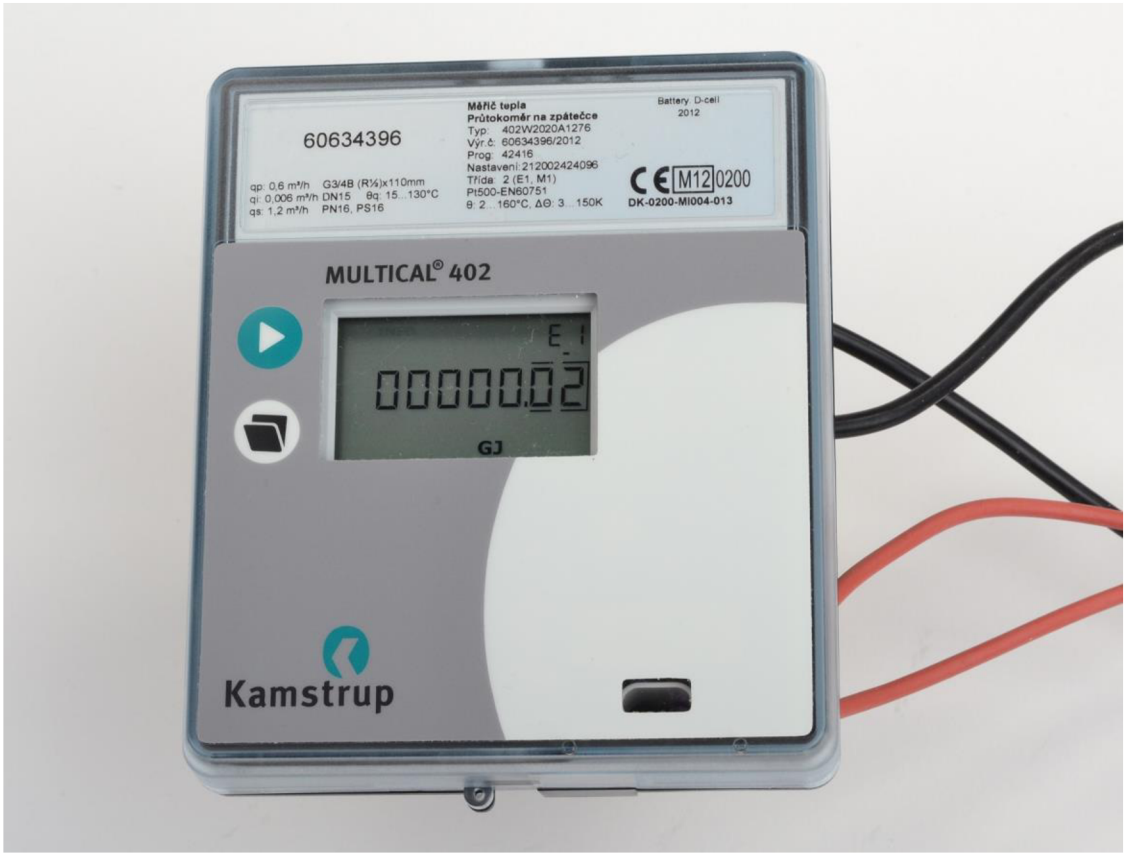


Fig. 4 Kamstrup Multical 402