Telit Wireless M-Bus Part 4 + Part 5 Mode R2 User Guide

1vv0300828 Rev.6 – 2013-05-06

APPLICABILITY TABLE

PRODUCT
ME50-868

SW Version
U00.01.03

SPECIFICATIONS SUBJECT TO CHANGE WITHOUT NOTICE

Notice

While reasonable efforts have been made to assure the accuracy of this document, Telit assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. The information in this document has been carefully checked and is believed to be entirely reliable. However, no responsibility is assumed for inaccuracies or omissions. Telit reserves the right to make changes to any products described herein and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Telit does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others.

It is possible that this publication may contain references to, or information about Telit products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Telit intends to announce such Telit products, programming, or services in your country.

Copyrights

This instruction manual and the Telit products described in this instruction manual may be, include or describe copyrighted Telit material, such as computer programs stored in semiconductor memories or other media. Laws in the Italy and other countries preserve for Telit and its licensors certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Telit and its licensors contained herein or in the Telit products described in this instruction manual may not be copied, reproduced, distributed, merged or modified in any manner without the express written permission of Telit. Furthermore, the purchase of Telit products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Telit, as arises by operation of law in the sale of a product.

Computer Software Copyrights

The Telit and 3rd Party supplied Software (SW) products described in this instruction manual may include copyrighted Telit and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the Italy and other countries preserve for Telit and other 3rd Party supplied SW certain exclusive rights for copyrighted computer programs, including the exclusive right to copy or reproduce in any form the copyrighted computer program. Accordingly, any copyrighted Telit or other 3rd Party supplied SW computer programs contained in the Telit products described in this instruction manual may not be copied (reverse engineered) or reproduced in any manner without the express written permission of Telit or the 3rd Party SW supplier. Furthermore, the purchase of Telit products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Telit or other 3rd Party supplied SW, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Usage and Disclosure Restrictions

License Agreements

The software described in this document is the property of Telit and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

Copyrighted Materials

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Telit

High Risk Materials

Components, units, or third-party products used in the product described herein are NOT fault-tolerant and are NOT designed, manufactured, or intended for use as on-line control equipment in the following hazardous environments requiring fail-safe controls: the operation of Nuclear Facilities, Aircraft Navigation or Aircraft Communication Systems, Air Traffic Control, Life Support, or Weapons Systems (High Risk Activities"). Telit and its supplier(s) specifically disclaim any expressed or implied warranty of fitness for such High Risk Activities.

Trademarks

TELIT and the Stylized T Logo are registered in Trademark Office. All other product or service names are the property of their respective owners.

Contents

1. Introduction 7
1.1. Scope 7
1.2. Audience 7
1.3. Contact Information, Support 7
1.4. Document Organization 8
1.5. Text Conventions 8
1.6. Related Documents 8
2. Wireless M-Bus Overview 9
2.1. Definition of Wireless M-Bus 9
2.2. Wireless M-Bus Presentation 9
2.2.1. Mode T 9
2.2.2. Mode R2 10
2.2.3. Mode S 10
2.3. Physical Link 10
2.4. Data Format on RF Link 10
2.5. Summary 12
2.6. Wireless M-Bus Part 5 (Mode R2) 12
2.6.1. Downstream Transmission 13
2.6.2. Upstream Transmission 14
3. Hardware Characteristics 16
3.1. Pinout 17
4. Software Operation 19
4.1. Configuration Mode 19
4.2. Register List 21
4.3. Operating Mode 25
4.3.1. Serial Frame on Transmission 26
4.3.2. Serial Frame on Reception 28
4.4. Stand-by Mode 29
4.4.1. Wakeup of the Module 29

4.4.2. Wakeup of External User Equipment 30
4.5. Advanced Features 31
4.5.1. Hardware Flow Control 31
4.5.2. Duty Cycle Management....31
4.5.3. Listen Before Talk 31
4.5.4. Date and Time 32
4.5.5. Registered Meters 32
4.5.6. Frame Filtering 32
4.5.7. Encryption 33
4.5.8. Remote AT Commands....35
5. Wireless M-Bus Part 5 Operation 36
5.1. Basic Operation 36
5.2. Network Management Protocol 39
5.2.1. Time Synchronization 40
5.2.2. Clear Relaying List....40
5.2.3. End Node Relaying List 40
5.2.4. Gateway Relaying List....40
5.2.5. Known Node List....41
5.2.6. Clear Known Nodes 41
5.2.7. Downstream Relaying Error 42
5.2.8. Upstream Relaying Error 42
5.3. Network Management in Gateways 42
5.4. Network Management in Concentrators 43
6. Power Consumption 45
6.1. S1 Mode 45
6.2. R2 Mode 46
7. Acronyms and Abbreviations 48
8. Document History 49

1. Introduction

1.1. Scope

Scope of this document is to present the features and the application of the Wireless M-Bus embedded stack available on ME50-868.

1.2. Audience

This document is intended for software developers and system integrators using ME50-868 with Wireless M-Bus firmware.

1.3. Contact Information, Support

For general contact, technical support, to report documentation errors and to order manuals, contact Telit Technical Support Center (TTSC) at:

TS-EMEA@telit.com
TS-NORTHAMERICA@telit.com
TS-LATINAMERICA@telit.com
TS-APAC@telit.com

Alternatively, use:

http://www.telit.com/en/products/technical-support-center/contact.php

For detailed information about where you can buy the Telit modules or for recommendations on accessories and components visit:

http://www.telit.com

To register for product news and announcements or for product questions contact Telit Technical Support Center (TTSC).

Our aim is to make this guide as helpful as possible. Keep us informed of your comments and suggestions for improvements.

Telit appreciates feedback from the users of our information.

1.4. Document Organization

This document contains the following chapters:

"Chapter 1: "Introduction" provides a scope for this document, target audience, contact and support information, and text conventions.

"Chapter 2: "Wireless M-Bus Overview" gives an overview of the Wireless M-Bus protocol.

"Chapter 3: "Hardware Characteristics" lists the radio frequency specifications of ME50-868 and describes the pinout of the module.

"Chapter 4: "Software Operation" describes the operation of the Wireless M-Bus firmware and how it interfaces with an external host.

"Chapter 5: "Wireless M-Bus Part 5 Operation" describes the firmware operation when EN 13757-5 Mode R2" is enabled.

"Chapter 6: "Power Consumption" provides information on the module power consumption in different operating conditions.

1.5. Text Conventions

Danger – This information MUST be followed or catastrophic equipment failure or bodily injury may occur.

Caution or Warning – Alerts the user to important points about integrating the module, if these points are not followed, the module and end user equipment may fail or malfunction.

Tip or Information – Provides advice and suggestions that may be useful when integrating the module.

1.6. Related Documents

- EN 300 220-2 v2.3.1
- ERC Recommendation 70-03
- IEC 60870-5-2
- EN 13757 part 1 to 5
- DSMR – P2 Companion Standard
- Telit ME50-868 RF Module User Guide, 1vv0300892

2. Wireless M-Bus Overview

2.1. Definition of Wireless M-Bus

M-Bus (Meter-Bus) is a European Standard for the remote reading of gas, water or electricity meters. M-Bus is also usable for other types of consumption meters. The M-Bus interface is made for communication on two wires, making it very cost effective.

This protocol exists with several physical layers such as paired wires, optical fiber or radio link.

The radio variant of M-Bus is called Wireless M-Bus and is specified in EN 13757-4. It is dedicated to the European ISM frequency band at 868 MHz. It means that modules embedding the Wireless M-bus stack must comply with the general SRD standard EN 300-220.

2.2. Wireless M-Bus Presentation

Devices communicating with Wireless M-Bus technology are classified as either meters or 'other' devices: the role of meters is to transmit utility consumption data, while 'other' devices (also referred to as concentrators) are in charge of collecting those data and can optionally send commands to meters.

The Wireless M Bus specification defines 3 different ways to exchange data with remote meters:

- Mode S 'Stationary'
- Mode T 'frequent Transmit'
- Mode R 'frequent Receive'

2.2.1. Mode T

In mode T, the meter sends spontaneously data, either periodically or stochastically.

- In Mode T1 the meter doesn't care if any receiver is present or not. The meter sends data and returns immediately in IDLE without waiting for an ACK. This is a unidirectional communication.
- In Mode T2 the meter sends its data and stays awake during a short time immediately after transmission to listen to a possible ACK. If no ACK is received, the meter returns in IDLE. If an ACK is received, then a bidirectional communication link is opened between meter and concentrator.

2.2.2. Mode R2

In Mode R2 the meter doesn't send spontaneously data. The meter wakes up periodically in Rx mode and waits for a wakeup frame received from concentrator. If no frame is received, the meter returns in IDLE. If a valid wakeup frame is received, a bidirectional link is then opened between meter and concentrator.

2.2.3. Mode S

- Mode S1 operates exactly as Mode T1 (unidirectional spontaneous transmission) but uses a different radio link described below.
- Mode S2 has the same behavior as Mode R2 (periodic wake up and wait for a wakeup frame before transmitting) but also with a different physical link.

2.3. Physical Link

Wireless M-Bus can use 3 different radio links, depending on baud rate and coding format. Moreover short or long preamble can be used depending of used mode.

- Radio link A operates at 868.3 MHz, the radio baud rate is 32.768 kcps and data coding is Manchester.
- Radio link B operates at 868.95 MHz, the baud rate is 100 kcps and data coding is "3 out of 6".
- Radio link C operates at 868.03 MHz, the baud rate is 4.8 kcps and data coding is Manchester.

This paper is software oriented to describe the stack behavior and features, for details about radio such as modulation, deviation etc. please refer to EN13757-4 documentation.

2.4. Data Format on RF Link

For all modes and whatever is the radio link used, the packet format is always the same:

Preamble	Block 1	Block 2	Block n	Postamble

Block 1 format:

L-Field	C-Field	M-Field	A-Field	CRC-Field
1 byte	1 byte	2 bytes	6 bytes	2 bytes

Block 2 format:

CI-Field	Data-Field	CRC-Field
1 byte	15 bytes or (((L – 9) mod 16) – 1) bytes	2 bytes

Block n format:

Data-Field	CRC-Field
16 bytes or ((L – 9) mod 16) bytes	2 bytes

- **L-Field** is the length indication
- **C-Field** is the communication indication (request, send, response expected, ACK…)
- **M-Field** is the Manufacturer ID
- **A-Field** is the unique address of the device
- **CI-Field** is the Control Information to indicate the protocol used to the upper layer
- **CRC-Field** is the Cyclic Redundancy Check

Wireless M-Bus uses an unbalanced transmission as described in IEC 60870-5-2; the format of the C-Field (or control field) is described below:

RES	PRM	FCB	FCV	Function			
		ACD	DFC				
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0

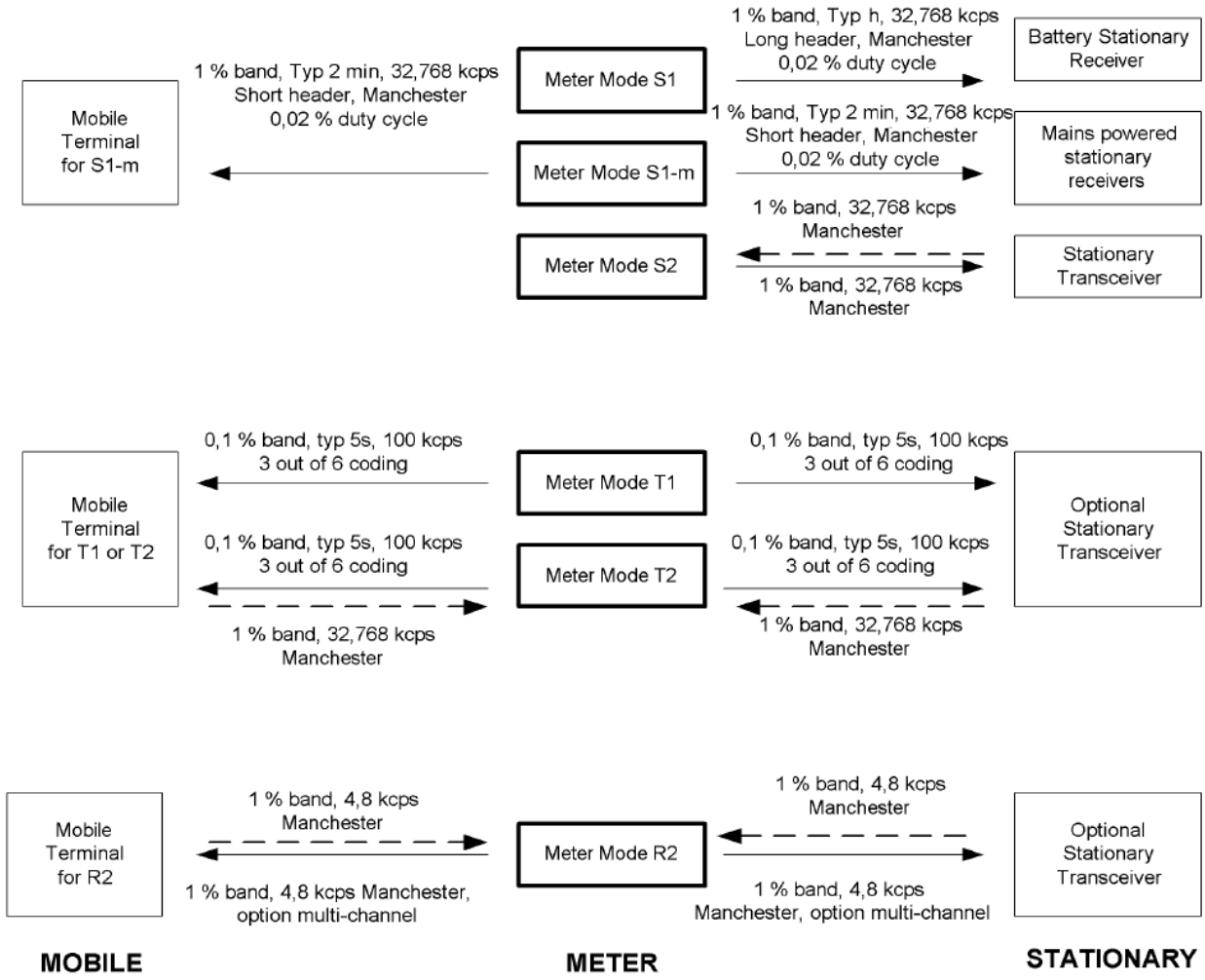
The meaning of bits 5 and 4 depends on the value of bit 6 (**PRM**): when **PRM** is set to 1, bits 5 and 4 are interpreted as **FCB** and **FCV** fields respectively, otherwise the same bits carry **ACD** and **DFC** fields.

- **RES** is a reserved bit and should be set to 0
- **PRM** indicates if the frame is being sent from a primary to a secondary station (when set to 1) or vice versa (when set to 0); the role of meters and concentrators as primary or secondary stations is defined by the application
- **FCB** (Frame Count Bit) is used to detect frame duplication: its value should alternate between 0 and 1 for successive frames sent from a primary station to the same secondary station; in order to set a common starting value of this bit for a given pair of stations, a link reset frame is defined (function code 0) which indicates to the receiving secondary station that the next frame from the primary station will have **FCB** set to 1
- **FCV** (Frame Count Valid) in frames sent from a primary station indicates whether the duplication detection mechanism of the frame count bit is used (when set to 1) or not (when set to 0)
- **ACD** (ACcess Demand), if set to 1, indicates that the sending secondary station has high priority data available, which should be requested by the primary station
- **DFC** (Data Flow Control), if set to 1, indicates that the sending secondary station may not be able to process further frames sent by the primary station; it can be used as a flow control mechanism to prevent data overflow at the secondary station

- **Function** is a numeric code indicating the type of frame being sent; its meaning depends on the direction of communication (primary to secondary or vice versa)

2.5. Summary

This drawing from EN13757-4 clearly summarizes the different Wireless M-Bus modes and



the link details used in each case.

2.6. Wireless M-Bus Part 5 (Mode R2)

The first specification of the Wireless M-Bus standard in EN 13757-4 allows communication between a meter and a concentrator only if radio frames sent from a device can reach directly the other device.

EN 13757-5 (also referred to as Wireless M-Bus part 5) describes different approaches to achieve multi-hop communication in which data packets between source and destination are relayed through one or more intermediate network nodes. According to EN 13757-5 terminology, data frames transferred from the concentrator to a meter are said to travel in downstream direction, while frames generated by a meter are called upstream frames. One of the methods described in EN 13737-5 to implement wireless relaying uses Mode R2 defined in EN 13757-4 and adds the concept of gateways, i.e. devices that can behave alternatively as meter or 'other' devices. The Wireless M-Bus firmware for ME50-868, in addition to the basic Wireless M-Bus modes described in EN 13757-4, implements relaying using Mode R2 with gateways.

With the gateway approach, at each hop in a multi-hop communication a device acting as meter communicates with another device acting as 'other': if the receiving device is not the end destination of a frame, it switches from 'other' to meter or vice versa and relays the frame to the subsequent node in the path to the destination. Network topology is hierarchical: the concentrator has the role of root node and each meter is either a leaf node or an intermediate node (gateway). Leaf nodes are meter devices according to EN 13757-4 notation, and communicate either with a gateway or directly with the concentrator. Gateways appear as 'other' devices to a group of neighboring nodes down the tree (downstream nodes), and as meter devices to another node (upstream node).

Only the concentrator must know the topology of the entire network, with the address of every node and the downstream path to communicate with it. Gateways have a more limited knowledge of the network, since they must know only the address of the downstream nodes with which they communicate directly. Finally, leaf nodes do not need any knowledge of the network, because they communicate exclusively with their upstream node.

The Wireless M-Bus frame format described in Section 2.4 allows specifying only one device address, and thus is not suitable for frame relaying: in a multi-hop communication, network information must be inserted at the application layer in transmitted frames. The presence of network information in a Wireless M-Bus frame is indicated by the CI-Field value 0x81: when this value is present, the first part of the Data-Field contains information related to the transmission path of the frame, followed by another (application-specific) CI-Field and then the application data.

2.6.1. Downstream Transmission

When the concentrator needs to send data downstream to a destination meter, if the two devices are able to communicate directly (i.e. they are in the radio communication range of each other) the frame transmitted by the concentrator has the standard format as described in Section 2 .4, with the M-Field and A-Field containing the manufacturer ID and address of the receiving meter. If one ore more gateways are needed to reach the meter, then the frame is transmitted to the first gateway in the path to the meter (the M-Field and A-Field identify the gateway), and the remaining path to the destination is specified in the transmitted frame, as described below:

CI-Field	Data-Field						
0x81	Hop count	Current hop	Address 1	...	Address n	CI-Field	Application data

The first part of the Data-Field contains the network information needed to reach the destination node, and is followed by the application data:

- Hop count (1 byte, with values from 1 to 10) is the number of gateways through which the frame must travel in the path to the meter
- Current hop (1 byte) is the remaining number of hops necessary, and corresponds to the number of Address fields in the frame format
- Address 1 to Address n (8 bytes) are the manufacturer ID and address (in this order) of the nodes through which the frame must travel, starting from the second gateway and including the destination meter
- CI-Field (1 byte) is the "real" CI-Field indicating the type of the following application data
- Application data is the data to deliver to the meter application

For example, if there are two gateways between the concentrator and the meter (indicated by GW1 and GW2), the format of the frame transmitted by the concentrator (ignoring CRC fields) is as follows.

First block:

L-Field	C-Field	M-Field	A-Field
		M-Field GW1	A-Field GW1

Second and subsequent blocks:

CI-Field	Data-Field							
0x81	0x02	0x02	M-Field GW2	A-Field GW2	M-Field meter	A-Field meter	CI-Field	Application data

The gateways involved to forward the frame modify the network information of the received frame before forwarding it; in the hop from the last gateway to the destination meter the transmitted frame does not contain any network information, and the meter receives it as if it came directly from the concentrator (network topology is transparent to the meters).

2.6.2. Upstream Transmission

When a meter sends data to the concentrator, it uses the frame format described in Section 2.4 and inserts its manufacturer ID and address in the M-Field and A-Field. If the distance between meter and concentrator is such that the concentrator is able to receive directly frames transmitted from the meter, communication between the two devices is carried out as in standard Mode R2; otherwise, one or more gateways are needed in order to relay the frame from meter to concentrator. At each hop toward the concentrator, the sending gateway inserts its own manufacturer ID and address in the M-Field and A-Field. When the first gateway receives the frame from the meter, it forwards the frame upstream after inserting the information needed to keep track of the original sender. The frame transmitted by the gateway may be received either directly by the concentrator or by another gateway; in the latter case, the second gateway forwards the frame upstream as it is (apart from the M-Field and the A-

Field), and this process continues until the concentrator is reached. Since any given node in the network (except the concentrator) is connected to exactly one upstream node, the communication path in upstream direction is unambiguous, and network information in an upstream frame does not have to contain the path from source to destination: instead, only the address of the source meter is reported, as described below:

CI-Field	Data-Field			
0x81	Hop info	Meter address	CI-Field	Application data

- Hop info (2 bytes) always contains the fixed value 0x0101
- Meter address (8 bytes) is the manufacturer ID and address (in this order) of the sending meter
- CI-Field (1 byte) is the "real" CI-Field indicating the type of the following application data
- Application data is the data to deliver to the concentrator application

Considering the example in which meter and concentrator communicate via two gateways (indicated by GW2 and GW1, in this order from meter to concentrator), the frame received by the concentrator has the following format (ignoring the CRC fields).

First block:

L-Field	C-Field	M-Field	A-Field
		M-Field GW1	A-Field GW1

Second and subsequent blocks:

CI-Field	Data-Field					
0x81	0x01	0x01	M-Field meter	A-Field meter	CI-Field	Application data

3. Hardware Characteristics

As specified earlier, the Wireless M-Bus stack is available on ME50-868.

Within this chapter, we will focus on hardware description of the RF module and necessary specification for integration in a final application. For more detailed information, please refer to the module user guide.

Below is a summary of ME50-868 RF module specifications for Wireless M-Bus:

		Min	Typ	Max	Unit	Note
Center frequency	Mode S	868.278	868.3	868.322	MHz	~ 25 ppm
	Mode T	868.90	868.95	869.00		~ 60 ppm
	Mode R	868.313	868.330	868.347		~ 20 ppm
Radio channel	Mode S	-	1	-	-	-
	Mode T	-	1	-		-
	Mode R	-	10	-		868.03 + (n x 0.06) (868.03 to 868.57 MHz)
Output power	Mode S	-	+13	+14	dBm	• EN 300 220-2 v2.3.1 • Selectable by software from 0 to +14 dBm
	Mode T					
	Mode R					
Radio chip rate	Mode S	-	32.768	-	kcps	± 1.5%
	Mode T	90	100	110		-
	Mode R	-	4.8	-		± 1.5%
FSK deviation	Mode S	± 40	± 50	± 80	kHz	EN 13757-4
	Mode T	± 40	± 50	± 80		
	Mode R	± 4.8	± 6	± 7.2		
Duty cycle	Mode S	-	0.02	1	%	• EN 300 220-2 v2.3.1 • EN 13757-4
	Mode T	-	-	0.1		
	Mode R	-	-	1		

Sensitivity	Mode S	-	-100	-	dBm	• EN 13757-4
	Mode T	-	-101	-		
	Mode R	-106	-107	-108		
Rx bandwidth	Mode S	-	80	-	kHz	-
	Mode T	-	200	-		
	Mode R	-	10	-		
Blocking	Mode S	28 min @ ± 2 MHz 53 min @ ± 10 MHz			dB	• EN 300 220-2 v2.3.1 • EN 13757-4
	Mode T	24 min @ ± 2 MHz 49 min @ ± 10 MHz				
	Mode R	37 min @ ± 2 MHz 62 min @ ± 10 MHz				

3.1. Pinout

Pin	Name	Type	Signal level	Function
J30	GND	Gnd		RF Ground connection for external antenna
J29	Ext_Antenna	RF		RF I/O connection to external antenna
J28	GND	Gnd		RF Ground connection for external antenna
J27	GND	Gnd		Ground
J26	GND	Gnd		Ground
J25	VDD	Power		Digital and Radio part power supply pin
J24	CTS	I	TTL	Clear To Send
J23	RESET	I	TTL	µC reset (Active low with internal pull-up)
J22	RTS	O	TTL	Request To Send
J21	RXD	I	TTL	RxD UART – Serial Data Reception
J20	GND	Gnd		Ground
J19	TXD	O	TTL	TxD UART – Serial Data Transmission

J18	WAKEUP	I	TTL	Signal to wake-up the module in stand-by mode (Active high with internal pull-down)
J17	GND	Gnd		Ground
J16	Prog	I	TTL	Signal for serial µC flashing (Active high with internal pull-down)
J15	GND	Gnd		Ground
J14	PDI_DATA	I/O	TTL	Program and Debug Interface Data
J13	GND	Gnd		Ground
J12	GND	Gnd		Ground
J11	GND	Gnd		Ground
J10	PDI_CLK	I	TTL	Program and Debug Interface Clock
J9	IO9 (*)	I/O	-	Digital I/O N°9 with interrupt
J8	IO8_AD_DA (*)	I/O	-	A to D and D to A I/O N°8 with interrupt (Logic I/O capability)
J7	IO7_A	I/O	Analog	Analog Input 7 (Logic I/O capability)
J6	IO6_A	I/O	Analog	Analog Input 6 (Logic I/O capability)
J5	IO5_A	I/O	Analog	Analog Input 5 (Logic I/O capability)
J4	IO4_A	I/O	Analog	Analog Input 4 (Logic I/O capability)
J3	IO3_A	I/O	Analog	Analog Input 3 (Logic I/O capability)
J2	STANDBY STATUS	O	TTL	Signal indicating stand-by status
J1	RADIO STATUS	O	TTL	Signal indicating reception or transmission of radio frame

(*) In case you want to use in the same application Telit ZE51 or ZE61 modules J9 and J8 should not be connected, since reserved on these modules.

4. Software Operation

There are 2 different modes:

- The configuration mode which allows to parameter the module. It is set through the use of Hayes commands sent on the serial link.
- The operating mode which is the functional mode for data transmission.

4.1. Configuration Mode

Hayes or 'AT' commands comply with Hayes protocol used in PSTN modem standards. This ‘AT’ protocol or Hayes mode is used to configure the modem parameters, based on the following principles:

- A data frame always begins with the two ASCII ’AT’ characters, standing for ‘ATtention’
- Commands are coded over one or several characters and may include additional data
- A given command always ends with a <CR> Carriage Return

A	T	Command	Additional data	<CR>

The only exception to this data-framing rule is the switching command from the operating/communication mode to ‘AT Mode’. In this case only, the escape code (‘+++’) must be started and followed by a silent time at least equal to the serial time out. In this case only <AT> and <CR> shall not be used.

Commands are parsed by the module only after <CR> is sent, except for the escape sequence ‘+++’ which is acted upon when the serial timeout expires after the last character of the sequence.

Below is the complete list of the ‘AT’ commands available on the module.

Command	Description
+++	‘+++’ command gives an instant access to the modem’s parameters configuration mode (Hayes or AT mode), whatever the current operating mode in process might be. ‘+++’ command should be entered as one string, i.e. it should not be preceded by ‘AT’ and followed by <CR> but two silent times whose duration is configurable via register 431 (Serial time-out). The time between two ‘+’ must not exceed the time-out value. Hayes mode inactivates radio functions. Answer : OK
ATO	‘ATO’ command gives an instant access to the modem’s operating mode, configured in register 400. ‘ATO’ command is used to get out of Hayes mode. Answer : OK or ERROR if the configuration is not complete

AT/V	'AT/V' command displays the modem's firmware and bootloader version number as follows: pp.UP0.MM.mm-Bbbb<CR>pp.B00.NN.nn With: pp indicating the hardware platform (GC for ME50-868) UP0: U means M-Bus stack, P=0 for OEM boards, P=1 for USB dongle MM: major version number of firmware mm: minor version number of firmware Bbbb: build number of firmware NN: major version number of bootloader nn: minor version number of bootloader Example: GC.U00.01.02-B011<CR>GC.B00.01.10 indicates an M-Bus stack V1.02 (Build 011) for a ME0-868 module in an OEM board, plus a bootloader V1.10
ATSn?	'ATSn?' command displays the content of Hayes register number n (refer to the register description table). Answer : Sn=x or ERROR if syntax problem or invalid register
ATSn=m	'ATSn=m' command configures Hayes register number n with the value m, e.g. ATS400=4<CR> enters the value '4' in the register 400. Answer : OK or ERROR
ATR	'ATR' command resets all modem's parameters to their default values. Answer : OK or ERROR
ATBL	'ATBL' command exits from the main program and runs the bootloader. This command is useful to update the firmware by serial or radio link. Answer : OK or ERROR
ATT	Continuous modulated carrier, simulating transmission of '010101' data. Answer : OK or ERROR This command is stopped by sending a character on the serial link Answer: No answer when exiting ATT
ATDT=MMDDhhmmYYss	Set current date and time. • MM is the month number, from 1 to 12 • DD is the day number, from 1 to 31 • hh is the current hour, from 0 to 23 • mm is the current minute, from 0 to 59 • YY is the current year, from 5 to 99 (corresponding to years from 2005 to 2099) • ss is the current second, from 0 to 59 Answer: OK if command format is correct, ERROR otherwise
ATDT?	Get current date and time. Answer: MMDDhhmmYYss, where: • MM is the month number, from 1 to 12 • DD is the day number, from 1 to 31 • hh is the current hour, from 0 to 23 • mm is the current minute, from 0 to 59 • YY is the current year, from 5 to 99 (corresponding to years from 2005 to 2099) • ss is the current second, from 0 to 59

After an AT command (ended by <CR>), the serial link gives back result code, "OK" or "ERROR"; the response string contains <CR> as trailing character.

"+++" command gives back "OK".

4.2. Register List

Numbers in **bold** indicate the default value

Access	Register	Name	Description
R	192	Serial Number	Serial number of the module, the one present on the sticker. Read-only register. Ex: *GCAJ4400001<CR>*
R/W	400	M-Bus Mode	Indicates the M-Bus mode on which the module works : • **'0': Mode S1-meter (default)** • '1': Mode S1-other • '2': Mode S2-meter • '3': Mode S2-other • '4': Mode T1-meter • '5': Mode T1-other • '6': Mode T2-meter • '7': Mode T2-other • '8': Mode R2-meter • '9': Mode R2-other Note: to activate Mode S1-m, select S1 in this register and then act on preamble length in register 421.
R/W	401	Serial Rx Format	Indicates the serial format options for serial frames sent from user to the RF module **Default value : 0** • Bit 0: indicates if Length Field is activated (1) or not (0) • Bit 1: indicates if C Field is activated (1) or not (0) • Bit 2: indicates if M Field is activated (1) or not (0) • Bit 3: indicates if A Field is activated (1) or not (0) • Bit 4: indicates if CI Field is activated (1) or not (0)

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Reserved (Write 0)	Reserved (Write 0)	Reserved (Write 0)	CI Field	A Field	M Field	C Field	Length

<table>
<tr><td rowspan="2">R/W</td><td rowspan="2">402</td><td>Serial Tx Format</td><td>Indicates the serial format options for serial frames sent from RF module to user</td></tr>
<tr><td colspan="2">
<table>
<tr><td>Bit 7</td><td>Bit 6</td><td>Bit 5</td><td>Bit 4</td><td>Bit 3</td><td>Bit 2</td><td>Bit 1</td><td>Bit 0</td></tr>
<tr><td>RSSI</td><td>Wakeup character</td><td>LQI</td><td>CI Field</td><td>A Field</td><td>M Field</td><td>C Field</td><td>Length</td></tr>
</table>
Default value : 0

• Bit 0: indicates if Length Field is activated (1) or not (0)
• Bit 1: indicates if C Field is activated (1) or not (0)
• Bit 2: indicates if M Field is activated (1) or not (0)
• Bit 3: indicates if A Field is activated (1) or not (0)
• Bit 4: indicates if CI Field is activated (1) or not (0)
• Bit 5: indicates if LQI Field is activated (1) or not (0)
• Bit 6: indicates if Wakeup character is activated (1) or not (0)
• Bit 7: indicates if RSSI Field is activated (1) or not (0)
</td></tr>
<tr><td>R/W</td><td>410</td><td>C Field</td><td>Indicates the C Field value (Byte 0) when not activated on serial format (Bit 1 of register 401). From 0 to 255.
Default : 68</td></tr>
<tr><td>R/W</td><td>411</td><td>M Field_Byte0</td><td>Indicates the M Field value (Byte 0) when not activated on serial format (Bit 2 of register 401). From 0 to 255.
Default : 174</td></tr>
<tr><td>R/W</td><td>412</td><td>M Field_Byte1</td><td>Indicates the M Field value (Byte 1) when not activated on serial format (Bit 2 of register 401). From 0 to 255.
Default : 12</td></tr>
<tr><td>R/W</td><td>413</td><td>A Field Byte0</td><td>Indicates the A Field value (Byte 0) when not activated on serial format (Bit 3 of register 401). From 0 to 255.
Default : 120</td></tr>
<tr><td>R/W</td><td>414</td><td>A Field Byte1</td><td>Indicates the A Field value (Byte 1) when not activated on serial format (Bit 3 of register 401). From 0 to 255.
Default : 86</td></tr>
<tr><td>R/W</td><td>415</td><td>A Field Byte2</td><td>Indicates the A Field value (Byte 2) when not activated on serial format (Bit 3 of register 401). From 0 to 255.
Default : 52</td></tr>
<tr><td>R/W</td><td>416</td><td>A Field Byte3</td><td>Indicates the A Field value (Byte 3) when not activated on serial format (Bit 3 of register 401). From 0 to 255.
Default : 18</td></tr>
<tr><td>R/W</td><td>417</td><td>A Field Byte4</td><td>Indicates the A Field value (Byte 4) when not activated on serial format (Bit 3 of register 401). From 0 to 255.
Default : 1</td></tr>
<tr><td>R/W</td><td>418</td><td>A Field Byte5</td><td>Indicates the A Field value (Byte 5) when not activated on serial format (Bit 3 of register 401). From 0 to 255.
Default : 7</td></tr>
<tr><td>R/W</td><td>419</td><td>CI Field</td><td>Indicates the CI Field value when not activated on serial format (Bit 4 of register 401). From 0 to 255.
Default : 120</td></tr>
<tr><td>R/W</td><td>420</td><td>Radio Channel</td><td>Indicates the radio channel (for R2 mode only). From 0 to 9
Default : 0</td></tr>
</table>

<table>
<tr><td>R/W</td><td>421</td><td>Preamble Length</td><td>Indicates if the preamble of the radio frame is short or long (for Mode S only) :
'0': short preamble (default)
'1': long preamble
Note: When using Mode S1, this register allows the module to work either in sub-mode S1-m (short preamble) or in normal Mode S1 (long preamble).</td></tr>
<tr><td>R/W</td><td>422</td><td>Radio Output Power</td><td>Indicates the output power of the RF module :
'0': 0 dBm
'1': +5 dBm
'2': +10 dBm (default)
‘3’: +14 dBm</td></tr>
<tr><td>R/W</td><td>430</td><td>Serial Speed</td><td>Indicates the speed on the serial link :
• ‘1’: 1200 bits/s
• ‘2’: 2400 bits/s
• ‘3’: 4800 bits/s
• ‘4’: 9600 bits/s
• ‘5’: 19200 bits/s (default)
• ‘6’: 38400 bits/s
• ‘7’: 57600 bits/s
• ‘8’: 115200 bits/s</td></tr>
<tr><td>R/W</td><td>431</td><td>Serial Time-Out</td><td>Indicates the value of the time-out on the serial link when Length Field is not activated.
Between 2 and 100 milliseconds
Default : 5
The time out value must be compatible with the serial speed.
<table>
<tr><td>Min. timeout</td><td>Serial speed</td></tr>
<tr><td>17 ms</td><td>1200 bits/s</td></tr>
<tr><td>9 ms</td><td>2400 bits/s</td></tr>
<tr><td>5 ms</td><td>4800 bits/s</td></tr>
<tr><td>3 ms</td><td>9600 bits/s</td></tr>
<tr><td>2 ms</td><td>≥ 19200 bits/s</td></tr>
</table></td></tr>
<tr><td rowspan="2">R/W</td><td rowspan="2">440</td><td>Wake-Up options</td><td>Indicates the different ways to wake-up the RF module.</td></tr>
<tr><td colspan="2">
<table>
<tr><td>Bit 2</td><td>Bit 1</td><td>Bit 0</td></tr>
<tr><td>Timer</td><td>Serial</td><td>Low Power Enable</td></tr>
</table>
Default value : 0 (No stand-by)
• Bit 0: Set this bit to ‘1’ to activate low power
• Bit 1: activates wake-up on serial character
• Bit 2: activates wake-up on timer (period set in register 442)
Note: if bit 0 is set while bits 1 and 2 are both reset to ‘0’, the only way to wake up the module is to use hardware wakeup pin J18. If one of bits 1 and 2 is set, bit 0 must also be set, otherwise an error response is returned.</td></tr>
</table>

R/W	441	Wakeup Time Out	Defines the duration between the end of an event (radio or serial exchange) and the return to stand-by. This is useful to keep the module awake between frames during a bidirectional session as defined in Modes S2, T2, R2. For Modes S1 and T1 this register may set to a low value to save power. Each time a new event happens, the timer is restarted with the specified value. More details in Section 4.4.1. Between 0 and 255 milliseconds. **Default : 0**
R/W	442	Sleep Time	Defines sleep time in seconds between 2 wake-up events when wake-up timer option is activated in register 440. Between 0 and 255. 0 indicates a sleep duration of 500 milliseconds. Other values indicate directly the sleep duration in seconds. **Default : 1**
R/W	452	Rx Filter	Indicates whether received radio frames are filtered based on their M-Field and A-Field. • **'0': Rx filter disabled (default)** • '1': Rx filter enabled
R/W	453	Tx Options	8 bits mask containing options for Wireless M-Bus frame transmission. • Bit 0: enable check on duty cycle limit • Bit 1: enable Listen Before Talk • Bit 2–7: reserved Refer to Section 4.5 for details on transmission options. **Default: 0**
R/W	454	M-Bus part 5	8 bits mask containing options for Wireless M-Bus part 5. • Bit 0: enable Wireless M-Bus part 5 when in Mode R2 • Bit 1: if Wireless M-Bus part 5 is enabled, enable network management in the concentrator • Bit 2: if Wireless M-Bus part 5 is enabled, disable upstream frame forwarding in gateways without downstream nodes • Bit 3–7: reserved Reserved bits should be set to zero for compatibility with future firmware versions. Refer to Chapter 5 for details on the implementation of Wireless M-Bus part 5. **Default: 0**

<table>
<tr><td rowspan="2">W</td><td rowspan="2">460</td><td>Registered Meter Options</td><td>Command options for registered meters (write-only register)</td></tr>
<tr><td colspan="2">
<table>
<tr><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th><th>Bit 0</th></tr>
<tr><td>Reserved (Write 0)</td><td>Reserved (Write 0)</td><td>Reserved (Write 0)</td><td>Reserved (Write 0)</td><td>Reserved (Write 0)</td><td>Enable encryption</td><td>Do not filter</td><td>Add/remove meter</td></tr>
</table>

Bit 0: Set this bit to ‘1’ to add or edit a registered meter, set to ‘0’ to remove a registered meter
Bit 1: Set this bit to ‘1’ to enable sending to the serial port received radio frames with the corresponding M-Field and A-Field
Bit 2: Activates encryption and decryption to frames with the corresponding M-Field and A-Field

</td></tr>
<tr><td>R/W</td><td>461-468</td><td>Meter Address</td><td>Contain the manufacturer ID (registers 461-462) and address (registers 463-468) of a registered meter, corresponding to the M-Field and A-Field of frames sent by that meter. Both fields are stored least significant byte first.
Values from 0 to 255</td></tr>
<tr><td>R/W</td><td>470-485</td><td>Meter Key</td><td>Contain the encryption key for communication with a registered meter, stored most significant byte first. If DES is used, the key is 8 bytes long and is stored in the first 8 registers (470 to 477), while the remaining registers are unused; if AES-128 is used, the key is 16 bytes long and is stored in registers 470 to 485.
Values from 0 to 255</td></tr>
</table>

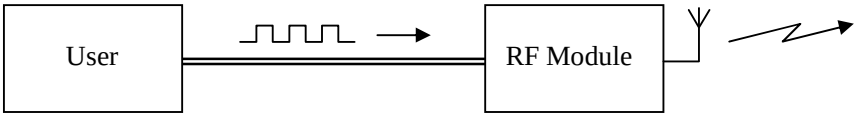
4.3. Operating Mode

When the module is in operating mode, each frame arriving on the serial link is sent on the radio link, and each valid wireless M-Bus frame received on the radio link is sent on the serial link.

These serial data (Tx or Rx) will have a specific format depending on the module configuration defined through the different registers. It allows a high flexibility in the use of our module in a wireless M-Bus application.

A module configured as either S1-meter or T1-meter (register 400 set to 0 or 4, respectively) does not activate frame reception on the radio interface, since S1 and T1 are unidirectional modes. As a result, no frames will be sent to the serial link by modules with these configuration settings.

4.3.1. Serial Frame on Transmission



Serial frames arriving on the serial link of the RF module can have the following fields:

Wakeup	Length	C	M	A	CI	Data

with:

Field	Length	Description
Wakeup	1	**Wakeup character** If wakeup on serial character is activated, the RF module can be triggered by starting the serial frame with a 0xFF or 0x00 character.
Length	1	**Length of frame** Giving the serial frame length to the RF module shortcuts the serial time out at the end of RX, leading in a very short wake up duration and very low power results. Using this field allow to save at least 2 ms for each wake up cycle. The RF module considers that the serial frame is complete as soon as the specified length is reached or until the serial time out is spent. Length value should count all subsequent bytes, including other serial options fields if any. Only Wake-up and Length bytes don't enter in the calculation of Length.
C	1	**C field** It specifies the role of the frame (Request, ACK, ...).
M	2	**Manufacturer and Address fields** Use this option to simplify the maintenance: in case of radio module replacement, the ID is already specified in the host and doesn't need to be set through registers. However this option makes the serial frame longer and increases the work duration (more power consumption). M and A can be activated separately.
A	6	
CI	1	**Control Information field.** Option to be used if several applicative layers use the wireless M-Bus link. If only one application is running, the CI field can be fixed and specified in the corresponding register.

The optional header depends on the different settings of module registers:

- **Wakeup** is necessary if bit 1 of register 440 is set to 1
- **Length** is necessary if bit 0 of register 401 is set to 1
- **C** is necessary if bit 1 of register 401 is set to 1
- **M** is necessary if bit 2 of register 401 is set to 1
- **A** is necessary if bit 3 of register 401 is set to 1
- **CI** is necessary if bit 4 of register 401 is set to 1

Examples:

S401 = 31 and S440 = 3 or 7
Serial frame must have this format:

Wakeup	Length	C	M	A	CI	Data

S401 = 30 and S440 = 3 or 7
Serial frame must have this format:

Wakeup	C	M	A	CI	Data

S401 = 17 and S440 = 3 or 7
Serial frame must have this format:

Wakeup	Length	CI	Data

S401 = 31 and S440 = 1 or 5
Serial frame must have this format:

Length	C	M	A	CI	Data

Whatever is the serial frame format, data on RF link will always have the same format, described in Section 2.4. In case of one or several fields (except Wakeup) is not activated on the serial frame, the RF module will use the value defined in the corresponding register.

Example:

If serial frame has this format:

Length	Data (10 bytes)

On the RF link, data will have the following format:

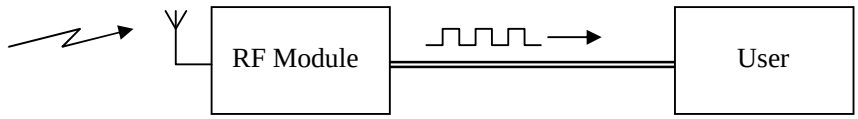
Preamble

L-Field	C-Field	M-Field	A-Field	CRC-Field
Length	Register 410	Registers 411 - 412	Registers 413 - 418	2 bytes

CI-Field	Data-Field	CRC-Field
Register 419	Data (10 bytes)	2 bytes

Postamble

4.3.2. Serial Frame on Reception



Serial frames sent on the serial link by the RF module can have the following fields:

0xFF	Length	C	M	A	CI	Data	LQI	RSSI

with:

Field	Length	Description
0xFF	1	**Wakeup character** Very useful especially in Modes S2 and R2 to work as "Wake On Radio" way. In these modes the user can be woken up by serial if a valid radio frame is received. This option comes in addition to the STANDBY STATUS signal.
Length	1	**Length of frame** Indicates to the user the length of serial frame he is receiving. Length value takes into account all subsequent bytes, including other serial options fields if any. Only Wakeup (0xFF) and Length bytes don't enter in the calculation of Length.
C	1	**C field** Specifies the role of the frame (Request, ACK, ...).
M	2	**Manufacturer and Address fields** Indicate the sender or receiver ID of the received frame. M and A can be activated separately.
A	6	
CI	1	**Control Information field.** Option to be used if several applicative layers use the wireless M-Bus link. If only one application is running, the CI field can be fixed and specified in the corresponding register.
LQI	1	**LQI** This byte indicates the level of radio reception, from 0 (poor) to 3 (excellent).
RSSI	1	**RSSI** Received Signal Strength Indicator, containing the input power of the received radio frame expressed in dBm as a signed 8 bit number.

The optional header and footer depend on the different settings of module registers:

- **Wake-up** will be added if bit 6 of register 402 is set to 1
- **Length** will be added if bit 0 of register 402 is set to 1
- **C** will be added if bit 1 of register 402 is set to 1

- **M** will be added if bit 2 of register 402 is set to 1
- **A** will be added if bit 3 of register 402 is set to 1
- **CI** will be added if bit 4 of register 402 is set to 1
- **LQI** will be added if bit 5 of register 402 is set to 1
- **RSSI** will be added if bit 7 of register 402 is set to 1

Examples:

S402 = 127
Serial frame will have this format:

Wakeup	Length	C	M	A	CI	Data	LQI

S402 = 126
Serial frame will have this format:

Wakeup	C	M	A	CI	Data	LQI

S402 = 209
Serial frame will have this format:

Wakeup	Length	CI	Data	RSSI

S402 = 31
Serial frame will have this format:

Length	C	M	A	CI	Data

4.4. Stand-by Mode

A key functionality available into the Wireless M-Bus stack is the ability to have RF modules in stand-by mode. During this mode, the RF module has a very low power consumption.

4.4.1. Wakeup of the Module

There are 3 different ways to wake up the module, defined by value of register 440.

- Wakeup on hardware, using wakeup signal J18: it is always possible to wake up the module by applying a logical ‘1’ to the ‘WAKEUP’ signal. When serial transmission is finished, ‘WAKEUP’ signal must be put back to a logical ‘0’ to allow the module returning in stand-by; else the module is kept awake while the WAKEUP pin is

maintained to '1'. When wakeup on serial character is not activated, there must be at least a 90 µs delay between the positive edge of the WAKEUP pin and the first character sent on the serial port.

- Wakeup on serial character: it is possible to wake up the module by sending a wakeup character at the beginning of the serial frame to send (refer to Section 4.3.1); although any character can awaken the module, either 0xFF or 0x00 must be used as wakeup character, otherwise the module serial port might receive corrupted bytes. After sending this frame on the air, the module will stay awake until a new radio or serial event occurs or until timeout defined by register 441 is reached.
- Wakeup on timer: it is possible to force the module to wake up periodically. This cyclic wakeup option is activated by bit 2 of register 440 and the time between 2 wakeup events is defined by the value of register 442. When waking up, the module will check the radio link for a valid frame preamble. If nothing is detected on the air, the module returns immediately to stand-by. Otherwise, it will wait for a valid frame and then automatically go back to stand-by after an interval defined by the value of register 441.

When timer is enabled, the stand-by consumption of the RF module is higher (refer to consumption data in Chapter 6).

These different wakeup and stand-by modes are strongly related to the Wireless M-Bus mode chosen. So that, the user has to correctly set the different registers in accordance with the usage. The following truth table can help for configuration:

	S1	S2	T1	T2	R2
Register 440 bit 1	✓	✗	✓	✓	✗
Register 440 bit 2	✗	✓	✗	✗	✓
Register 441	✓	✓	✓	✓	✓
Register 442	✗	✓	✗	✗	✓

✓ : to be configured

✗ : not used

4.4.2. Wakeup of External User Equipment

There are 2 different ways to wake up the external user equipment:

- Through 'STANDBY STATUS' output signal (J2): this signal is set to logical '1' while the module is operating and return to '0' during stand-by periods.
- Through serial character: when the module receives a valid RF frame, it can add a 0xFF character at the beginning of the serial frame to wake up the external user equipment. This type of functioning is so called "Wake on Radio".

4.5. Advanced Features

4.5.1. Hardware Flow Control

In both configuration mode and data mode, flow control on the serial port is operated via the RTS pin, which is de-asserted (logic level 1) when the module is unable to receive bytes (e.g. when processing an AT command or a serial frame) and re-asserted (logic level 0) when new bytes can be received.

4.5.2. Duty Cycle Management

Configuration register 453 allows using the duty cycle management feature of ME50-868. When enabled (bit 0 of register 453 set to 1), this feature ensures that a single module does not occupy the radio channel more than allowed by the Wireless M-Bus standard. The duty cycle is defined as the total time a device transmits in the wireless medium over a 60 minutes period. It is expressed in percentage relative to 60 minutes, and its maximum allowed value varies between 0.02% and 1%, depending on M-Bus mode and device type.

When a frame is received from the serial port and the duty cycle limit has been reached, the module discards the received frame instead of sending it to the radio interface.

The Wireless M-Bus firmware of ME50-868 implements duty cycle management by filling an internal log containing data on the radio frames transmitted in the last hour. Since memory resources of the module are limited, the transmission log cannot host more than 255 entries, and each entry cannot account for more than 255 milliseconds of transmission time (if a single frame lasts more than 255 milliseconds, its transmission time is split in different entries). If at a given time the internal log is full, no further frames can be sent by the module (even if the duty cycle limit has not been reached) until sufficient time has passed such that some log entries become older than one hour; this limitation should be taken into account when enabling duty cycle management in the module.

Records of past transmissions used for duty cycle management are cleared when the module is put in configuration mode and receives either the ATR command or a command that sets register 400 to a valid value.

4.5.3. Listen Before Talk

When bit 1 of configuration register 453 is set to 1, the Listen Before Talk (LBT) feature of ME50-868 is enabled. LBT operation allows decreasing the probability of collision between different modules trying to transmit radio frames at the same time. When this feature is enabled, ME50-868 listens to the wireless medium before transmitting a radio frame (except for frames sent with function codes ACK, NACK and RACK, which are used as acknowledgement frames in Wireless M-Bus Part 5; refer to Section 5.1 for details). The minimum listen time is 5 ms; if during this time no activity is detected on the radio link, frame transmission starts immediately, otherwise ME50-868 waits until the link becomes free and then listens again for another 5 ms interval, after which an additional listen interval of random duration between 0 and 5 ms is added before frame transmission finally starts. If the

radio link becomes busy during the listen time, ME50-868 waits for the channel to become free and then restarts the listen procedure.

4.5.4. Date and Time

ME50-868 is able to keep track of current date and time, with a supported calendar covering the years from 2005 to 2099. The internal clock runs also with low power mode enabled. The current date and time can be set and retrieved in configuration mode with the ATDT command (see Section 4.1 for details). If Wireless M-Bus part 5 operation is enabled and ME50-868 is configured as meter device, the current date and time can also be set in operating mode, by sending to the module a specific time synchronization frame as described in Section 5.2.1.

4.5.5. Registered Meters

A ME50-868 module can register up to 32 meters, to be used for filtering received M-Bus frames and encrypting radio communication. Data for registered meters is stored in EEPROM memory, which is accessed through configuration registers 460, 461-468 and 470-485.

To add, edit or delete an entry in the list of registered meters, the manufacturer ID and address of the meter must be inserted in registers 461 to 468, the encryption key (if used) must be inserted in registers 470 to 485, and the appropriate flags must be set in register 460. When bit 0 of register 460 is set to 1, if no meter corresponding to the contents of registers 461 to 468 is present in the list, a new entry is added with the option flags specified in register 460; if the meter is already present, no entry is added, but the option flags of the existing entry are updated. When bit 0 of register 460 is set to 0, the registered meter corresponding to the contents of registers 461 to 468 is removed from the list. An error response is returned by ME50-868 when trying to add a new entry if the list is full. Register 460 is write-only, and an error response is returned when trying to read the register value. After exiting configuration mode, contents of registers 461 to 468 and 470 to 485 are not guaranteed to remain the same when re-entering configuration mode, thus the user should always set the register contents (at least manufacturer ID and address, if no encryption is needed) before setting a value in register 460. Issuing the ATR command clears the list of registered meters. Refer to the description of frame filtering and encryption in the rest of this section for details on how to use registered meters.

4.5.6. Frame Filtering

An optional filter on received M-Bus frames can be activated, which allows transmitting to the serial port only frames whose M-Field and A-Field match one or more specific values. Frame filtering is enabled by setting register 452 to 1. The addresses used to filter incoming frames differ depending on whether the module is configured as ‘meter’ or ‘other’ device.

Meter devices use the manufacturer ID and address defined by the content of registers 411 to 418 to filter incoming frames. Regardless of the frame filtering option being activated or not, meter devices never filter out received frames containing the broadcast address (i.e. with all bits of manufacturer ID and address set to 1).

Concentrators can use the frame filtering feature of ME50-868 by registering the meters from which they want to receive data, i.e. putting their manufacturer ID and address in the list of registered meters. When registering a given meter (or changing the options of a registered meter), bit 1 in the value of register 460 must be set to 1 in order to enable sending to the serial port M-Bus frames received from that meter.

A Wireless M-Bus application can define an installation mode in which a meter looks for a concentrator to bind to. Frames sent by meters in installation mode use typically a C-Field with function code set to 6 (refer to Section 2.4 for a description of C-Field format). In order to be able to receive frames from meters in installation mode, when ME50-868 is configured to act as concentrator, filtering does not apply to received frames with function code set to 6, which are always sent to the serial port, regardless of the frame filtering option.

When Wireless M-Bus part 5 operation is enabled (see Chapter 5), different filtering rules are applied to frames received from the radio interface, thus the frame filtering option in register 452 has no effect.

4.5.7. Encryption

ME50-868 can encrypt and decrypt Wireless M-Bus frames to provide secure communication between nodes. Two encryption algorithms are supported, namely DES and AES-128; for both algorithms, Cipher Block Chaining is used as mode of operation.

Encryption and decryption are implemented following the guidelines in EN 13757-3 and adding some extensions from the Dutch Smart Meter Requirements. In order to use encrypted communication, one of the following CI-Field values must be used in sent frames: 0x72, 0x7A, 0x5A and 0x5B. In addition, a specific header must be inserted as first part of the Data-Field; this data header is used by the firmware to determine the encryption type. The encrypted part of a frame is the portion of the Data-Field following the data header, while the data header itself is always sent unencrypted.

There are two types of data header. The first is 4 bytes long and must be used with CI-Field values 0x7A and 0x5A; its format is the following:

Access number	Status	Signature
1 byte	1 byte	2 bytes

The second type of data header is 12 bytes long and must be used with CI-Field values 0x72 and 0x5B; its format is the following:

Identification number	Manufacturer ID	Version	Device Type	Access number	Status	Signature
4 bytes	2 bytes	1 byte	1 byte	1 byte	1 byte	2 bytes

- **Identification Number** is a unique device identifier coded as 8 BCD digits.
- **Manufacturer ID** is the identifier of the device manufacturer.
- **Version** specifies the version number of the device and depends on the manufacturer.
- **Device Type** specifies the functionality of the device (for example, electricity meter).

- **Access Number** is an unsigned number from 0 to 255 that should be incremented by one at each sent frame.
- **Status** indicates the operating status of the device and can be used to signal the presence of an error condition.
- **Signature** is a 2 bytes word containing the length of encrypted content (in the first byte) and the encryption method code (in the 4 least significant bits of the second byte). Since encryption and decryption can only be performed in blocks, the number of encrypted bytes is a multiple of the block size (8 for DES and 16 for AES-128). Therefore, the 3 or 4 least significant bits of the first byte of the signature word do not enter in the count of encrypted bytes, and can be used for other purposes.

The supported encryption methods are identified by codes 2, 3, 4 and 5. Methods 2 and 3 use DES encryption, while methods 4 and 5 use AES-128. Methods 3 and 5 need the long data header (12 bytes) to initialize the CBC algorithm, therefore they can be used only with CI field values 0x72 and 0x5B; methods 2 and 4 can be used with any of the four CI-Field values. Method 3 needs the current date to initialize the CBC algorithm, therefore in order to communicate with this encryption method a meter must have the same date as set in the concentrator.

Concentrator devices can send encrypted frames to (and receive encrypted frames from) any of the registered meters; to enable encryption for communication with a given meter, manufacturer ID, address and key (DES or AES-128) of the meter must be inserted in the relevant registers and bit 1 must be set to 1 in the option register 460. Since the M-Field and A-Field values of frames sent or received by a given meter correspond to the meter manufacturer ID and address, encryption is enabled in a meter device by inserting its own manufacturer ID and address in an entry of the registered meter list and setting bit 1 of the options register 460 to 1.

Once all the relevant configuration registers for encryption have been set, when a frame with a data header specifying one of the supported encryption methods is received from the serial port, ME50-868 encrypts the frame using the key corresponding to manufacturer ID and address and the encryption method contained in the signature word. If the signature contains an encryption method code incompatible with the CI-Field, the frame is discarded. If the signature contains an unsupported encryption method (or method 0, which means no encryption), the frame is sent unencrypted. Before encrypting a frame, filler bytes with value 0x2F are added at the end of the Data-Field, if necessary, to make the length of the encrypted payload a multiple of the block size (8 bytes for DES and 16 bytes for AES-128). The number of encrypted blocks contained in the signature word provided by the user is ignored, and the value corresponding to the length of the encrypted content is inserted in the signature before sending the frame (sent frames cannot be partially encrypted).

When receiving from the radio interface an encrypted Wireless M-Bus frame, if M-Field and A-Field correspond to a registered meter with encryption enabled, ME50-868 decrypts the frame before sending it to the serial port, provided the frame contains a valid data header and a supported encryption method code. Received frames that cannot be decrypted because of invalid contents (such as Data-Field length incompatible with signature, or encryption method incompatible with CI-Field) are discarded, and frames with unsupported encryption methods are sent unaltered to the serial port. Decryption of partially encrypted frames is supported. ME50-868 does not modify the signature word of a received M-Bus frame after decryption, so that user applications are able to verify which encryption method has been used and how many blocks of the frame have been sent encrypted.

If Wireless M-Bus part 5 operation is enabled, in order to support encrypted communication with multi-hop paths, the key used to encrypt and decrypt frames in a concentrator may be selected based on the network layer information instead of the M-Field and A-Field; refer to Section 5.4 for further information.

4.5.8. Remote AT Commands

ME50-868 is able to accept and execute AT commands sent over the radio link as Wireless M-Bus frames; this feature is particularly useful to update the firmware of ME50-868 from a remote host. Only modules configured as meters can accept remote AT commands.

A Wireless M-Bus frame containing an AT command for a given module must have the C-Field set to 0x4B, the M-Field and A-Field set to the contents of configuration registers 411 to 418 of the module and the CI-Field set to 0xA0 (this is the first value in the range reserved for manufacturer-specific applications according to EN 13757-4). The Data-Field must contain the AT command with the format described in Section 4.1, without the trailing <CR> character. Upon receiving a remote AT command, ME50-868, instead of sending the received frame to the serial port, executes the command and replies with a Wireless M-Bus frame containing the response to the command. The response frame has the C-Field set to 0x08 and the M-Field, A-Field and CI-Field identical to those of the command frame; the Data-Field contains the response with the format described in Section 4.1, without the trailing <CR> character.

If the module receives a remote AT command including a <CR> character, this character and all subsequent bytes in the command string are ignored.

The '+++' escape sequence and the ATT command cannot be sent remotely, and an ERROR response is sent by the module if these command strings are received. Since registers 461 to 468 and 470 to 485 are not guaranteed to keep their content when the module is in operating mode, it is not recommended to use remote AT commands to update the list of registered meters of a given module.

In order to avoid conflict with the execution of remote AT commands, external applications should not use the CI-Field value 0xA0 for other purposes than sending AT commands.

5. Wireless M-Bus Part 5 Operation

An important feature of ME50-868 is the implementation of the protocol described in Section 6 of EN 13757-5 (refer to Section 2.6 for basic information on the protocol). This chapter contains more detailed information on firmware operation when Wireless M-Bus part 5 is enabled.

5.1. Basic Operation

In order to enable Wireless M-Bus part 5 operation, configuration register 400 must be set to either 8 (R2-meter) or 9 (R2-other), and bit 0 of register 454 must be set to 1. When a module is configured as concentrator ("other" device), it acts as the root node of the network tree, while modules configured as meter devices can be either leaf nodes or gateways.

Each device has a manufacturer ID and address, which are used to determine whether frames received in downstream direction are for the local node, and can be used (depending on the serial Rx format options) as M-Field and A-Field of frames sent upstream. In the remainder of this chapter, the concatenation of manufacturer ID and address of a specific node will be referred to simply as the node address. Each module retrieves its local address from configuration registers 411 to 418.

When its M-Bus mode is configured as R2-meter, a module is able to operate as a gateway in a tree network as defined in Wireless M-Bus part 5. Upon receiving a radio frame, a gateway parses the frame fields to determine whether the frame must be forwarded to another node, handled internally by the firmware, transmitted on the serial port to the user application or ignored; broadcast frames (containing the M-Field and A-Field with all bits set to 1) are also supported. A concentrator (M-Bus mode set to R2-other), upon reception of an M-Bus frame, either discards it, handles it internally or passes it to the serial port.

The concentrator, as root node of the tree, decides the network topology by means of two mechanisms. For downstream transmissions, each frame sent by the concentrator contains the full path to reach the destination; for upstream transmissions, the concentrator assigns to each gateway two lists of nodes for which the gateway will relay frames: one is the list of end-nodes and the other is the list of gateways. As described in Section 2.6.2, the first gateway in the path from a meter to the concentrator adds network information to frames received from the meter, using the CI-Field value 0x81; this makes it possible to distinguish frames forwarded by gateways from frames sent directly by meters. A gateway forwards upstream a frame sent directly by a meter if that meter is in its list of end-nodes; likewise, a frame forwarded by a gateway is forwarded again by a second gateway if the first node is in the list of gateways of the second node. Two exceptions apply to this rule. The first exception is that received frames are always forwarded by a gateway if its relevant list is empty. The second exception is represented by frames sent (directly or indirectly) by nodes in installation mode, i.e. with the function code of the C-Field set to 6: these frames are forwarded by all gateways receiving them, regardless of the presence and contents of the relaying lists.

ME50-868 modules configured as gateways implement the rules described above to determine whether a received frame must be forwarded, retrieving the transfer direction of the frame from the PRM bit in its C-Field (which is set to 1 in downstream transmissions and to 0

in upstream transmissions). Downstream frames are forwarded by a gateway if their M-Field and A-Field correspond to the local address of the gateway and there is valid network information to determine the next hop. Upstream frames are forwarded if they come from nodes belonging to the local list of nodes to relay data from (if the list is not empty), or if they are installation frames (i.e. the function code sub-field of the C-Field has value 6). See Section 5.3 for further information on the management of relaying lists.

Depending on the network topology, having gateways without downstream nodes in their lists can cause unnecessary network traffic and in some cases collisions between frames from different nodes, because according to EN 13757-5 a gateway receiving an upstream frame shall forward it if the relevant list of nodes to relay data from is empty. Since the additional network traffic due to the above rule could cause a degradation of network performance, a configuration option is provided which allows disabling under certain conditions frame forwarding by gateways. This configuration option is represented by bit 2 of register 454 (see Section 4.2): if this bit is set to 1 in a module configured as gateway, the module does not forward an upstream frame received from a node which is not in the appropriate relaying list, regardless of the list being empty. This option does not affect frames sent from nodes in installation mode, (function code set to 6), which are always forwarded.

As explained in Section 2.6.2, the first gateway in the upstream path from a meter to the concentrator inserts network information before forwarding a received frame; this network information is 11 bytes long, thus the maximum length of frames sent by meters which are not in direct communication with the concentrator is 11 bytes less than the normal maximum length of a Wireless M-Bus frame. If a gateway cannot forward an upstream frame because its Data-Field is too long to insert network information, the frame is discarded.

The communication flow between concentrator and meters is usually initiated by the concentrator, which can send data to meters and request data from them; however, meters are allowed to send unsolicited frames upstream, for example when in installation mode. If a multi-hop path separates the concentrator from a meter, the travelling frames are acknowledged at each hop by the receiving node (unless the function code indicates an acknowledgement is not needed), both in downstream and upstream direction. If a sending node fails to receive an acknowledgement, it re-sends the frame up to two times.

The function codes to be used for downstream frames are listed below:

Function code	Name	Description
0x0	LRESET	Link reset, used to set the FCB bit for a pair of nodes to a common starting value (see Section 2.4); a link reset frame does not carry CI-Field and Data-Field and is not acknowledged
0x3	SEND	Send data downstream
0x4	BCAST	Send data downstream, without acknowledgement
0x6	INSTALL	Send data to a node in installation mode
0x7	RACK	Reverse acknowledge, used to acknowledge frames received from downstream
0x8	S-REQUEST	Status request
0xA	P-REQUEST	Priority request
0xB	REQUEST	Request

The following table lists function codes to be used for upstream frames:

Function code	Name	Description
0x0	ACK	Positive acknowledge, used to acknowledge frames received from upstream
0x1	NACK	Negative acknowledge, used to reject frames received from upstream
0x6	INSTALL	Send data, used in installation mode; not acknowledged
0x8	RESPONSE	Response, used to respond to P-REQUEST or REQUEST frames
0x9	N-RESPONSE	Negative response, used when a response to a request cannot be provided; not acknowledged
0xB	S-RESPONSE	Status response, used to respond to a status request

A request frame, which usually requires acknowledgement, may not be followed by an ACK when the receiving node is the end destination meter, because the response frame of the meter is an implicit acknowledgement of the received request.

When Wireless M-Bus part 5 operation is enabled in ME50-868, for each frame sent or received by a module on the radio link, acknowledgement and retransmissions are handled automatically by the firmware according to EN 13757-5, without any interaction with the serial interface. Acknowledge frames sent by the module do not carry CI-Field and Data-Field. Acknowledge frames are not sent for request frames received from upstream at an end node, since a response frame is expected to be sent shortly via the user application. After sending a frame, any acknowledge frame received is considered valid if it carries the same M-Field and A-Field as the frame just sent. If a frame with the FCV bit of the C-Field set is being sent downstream, the frame count bit is automatically adjusted based on frames previously sent to the same downstream node. When sending the first frame with FCV set to a given node, a LRESET frame is sent first to ensure the following frame will not be discarded

by the receiving node. In frames sent by the concentrator, which are necessarily downstream frames, the PRM bit in the C-Field is automatically set if not set by the user. Frames sent by user applications should not carry a function code LRESET, because this could cause a misalignment between the FCB bit of network nodes and thus prevent further communication between the nodes. With the exception above, user applications can exchange frames with any function code: if an unknown function code is being sent or received, the module does not expect or send any acknowledgement. Any CI-Field value can be used in application frames, even values marked as reserved for future use in EN 13757-5; however, special values such as 0x81 and 0x83 should only be used for the specific purpose for which they are intended, because frames with these CI-Field values might be handled internally by the firmware.

When a frame is being sent to another node, ME50-868 is unable to send or receive frames other than those related to the current transmission, until it completes either successfully or with errors. If the receiving node does not respond, several seconds might pass before a new transmission can be initiated (for instance a 11 seconds timeout is mandated by EN 13757-5 for frames sent to end nodes); during this time, a new frame can be received on the serial port, but after that the RTS pin is de-asserted until the bytes received from the serial port have been processed and the new frame is ready to be sent. When stand-by mode is enabled (see Section 4.4), the module does not enter stand-by as long as the current transmission is ongoing.

5.2. Network Management Protocol

In order for the concentrator to establish the transmission path to any given network node in the tree, EN 13757-5 defines a network management protocol which allows the concentrator to discover the path to nodes not directly reachable and instructs the gateways to relay frames from specific nodes. The ME50-868 firmware is able to generate and parse internally network management frames, allowing setup and management of the network topology without user intervention.

Network management is implemented by an application layer protocol using the CI-Field value 0x83. The first byte of the application data of a network management frame is called function field (F-Field); the length and format of subsequent data depends on the F-Field value. The following sections describe the different types of network management frames, specifying the F-Field value and the format of application data. Frames used to send data from the concentrator to other network nodes (time synchronization, clear relaying list, end-node relaying list, gateway relaying list and clear known list) have a C-Field with function code set to SEND, BCAST or INSTALL. Frames used to request data from network nodes (such as to retrieve the known node list and the upstream errors) have a function code set to S-REQUEST, P-REQUEST or REQUEST, and corresponding responses from network nodes have a function code set to S-RESPONSE, P-RESPONSE or RESPONSE. Last, frames used to report a downstream relaying error are sent as unsolicited responses from gateway to concentrator and have a function code set to S-RESPONSE or RESPONSE.

5.2.1. Time Synchronization

The concentrator sends time synchronization frames to gateways and meters to set a common time reference for the network nodes. The format of the application data is the following:

F-Field	Year	Month	Day	Hour	Minutes	Seconds	Time zone
0x00	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte

Year can range from 5 to 99, **Month** is the month number (ranging from 1 to 12) and **Time zone** is the time offset relative to UTC, ranging from -12 to 12.

5.2.2. Clear Relaying List

The concentrator uses this frame type to empty the relaying lists of one or more gateways. The format of the application data is the following:

F-Field	Modifier
0x10	1 byte

Modifier is a bitmask indicating which lists should be cleared, with bit 7 (most significant bit) for the list of gateways and bit 6 for the list of end-nodes.

5.2.3. End Node Relaying List

The concentrator uses this frame type to add elements to the lists of end-nodes of a gateway. The format of the application data is the following:

F-Field	Node count	Address 1	…	Address n
0x11	1 byte	8 bytes		8 bytes

Node count is the number of end-nodes to add to the list and **Address 1** to **Address n** are the addresses of the end-nodes.

5.2.4. Gateway Relaying List

The concentrator uses this frame type to add elements to the lists of gateways of a gateway. The format of the application data is the following:

F-Field	Node count	Address 1	…	Address n
0x12	1 byte	8 bytes		8 bytes

Node count is the number of gateways to add to the list and **Address 1** to **Address n** are the addresses of the gateways.

5.2.5. Known Node List

The concentrator uses this frame type to request the list of known nodes to a given device, i.e. the nodes with which the device is able to communicate directly. The format of the application data of the request frame is the following:

F-Field	Modifier
0x14	1 byte

Modifier is a bitmask, with bit 7 (most significant bit) indicating whether the first (value 0) or the next (value 1) block from the list of known nodes should be returned, and bit 6 indicating whether information for the link quality of each known node should be returned (value 1 means quality information should be returned).

The format of the application data of the response frame is the following:

F-Field	Count/Modifier	Address 1	Quality indicator 1	…	Address n	Quality indicator n
0x14	1 byte	8 bytes	1 byte		8 bytes	1 byte

Count/Modifier is a bitmask, with the following bit fields:

- bit 7 (most significant bit) indicates whether the first (value 0) or the next (value 1) block from the list of known nodes is being returned
- bit 6 indicates whether quality information is being returned (value 1 means quality information is present)
- bit 5 indicates whether this is the last block from the list (value 1) or there are more known nodes to be reported (value 0)
- bits 4 to 0 contain the number of nodes present in the frame

Address 1 to **Address n** contain the address of known nodes.

Quality indicator 1 to **Quality indicator n** (present only if bit 6 of **Count/Modifier** is set to 1) represent the link quality with the known nodes, expressed as unsigned number, with larger values indicating better quality.

5.2.6. Clear Known Nodes

The concentrator uses this frame type to empty the list of known nodes of a gateway. The application data contains only the F-Field, with value 0x15.

5.2.7. Downstream Relaying Error

When a gateway is unable to forward a downstream frame, it sends to the concentrator an unsolicited response frame containing information on the error. The format of the application data is the following:

F-Field	Condition	Address
0x20	1 byte	8 bytes

Condition is a bitmask, with bit 7 (most significant bit) set to 1 if the downstream frame was rejected by the recipient with NACK responses, and bit 6 set to 1 if there has been no acknowledge from the recipient.

Address is the address of the downstream node to which the frame could not be relayed.

5.2.8. Upstream Relaying Error

When a gateway is unable to forward an upstream frame, it stores internally the error condition so that when the link with the upstream node is re-established the concentrator can retrieve information on the error. The application data of the request frame from the concentrator contains only the F-Field, with value 0x21, while the format of the application data of the response frame is the following:

F-Field	Count/Modifier	Time tag 1	Application data 1	…	Time tag n	Application data n
0x21	1 byte	7 bytes	n bytes		7 bytes	n bytes

Count/Modifier is a bitmask, with the following bit fields:

- bit 7 (most significant bit) is set to 1 if time tag is being returned for each error
- bit 6 is set to 1 if application data is being returned for each error
- bit 5 indicates whether this is the last block from the list of downstream errors (value 1) or there are more errors to be reported (value 0)
- bits 2 to 0 contain the number of error entries present in the frame

Time tag 1 to **Time tag n** (present only if bit 7 of **Count/Modifier** is set to 1) contain the timestamp at which the errors occurred; the timestamp format is the same as that used in time synchronization frames sent by the concentrator.

Application data 1 to **Application data n** (present only if bit 6 of **Count/Modifier** is set to 1) contain the application data that could not be relayed when the errors occurred.

5.3. Network Management in Gateways

Gateway operation is enabled in ME50-868 setting configuration register 400 to R2-meter (value 8). If a gateway receives a frame from upstream whose end destination is the local node and whose CI-field indicates that it contains network management information (value 0x83), the frame is handled internally by the firmware instead of being sent to the serial interface. A gateway always handles internally network management frames, regardless of the value set in bit 1 of register 454.

ME50-868 supports all types of network management frames, with the following features and limitations:

- The lists of relaying nodes and known nodes cannot host more than 64 entries overall; if a node is present in more than one list, it counts as one single entry. The lists are cleared when the module is put in configuration mode and receives either the ATR command or a command that sets register 400 to a valid value; moreover, the lists are cleared when the module is powered off.
- Each node in the list of known nodes is associated to a quality indicator corresponding to the signal strength of the last received frame from that node, expressed in dBm and increased by 128.
- A maximum number of 4 upstream errors with associated timestamps are stored for later retrieval by the concentrator; no application data is stored for upstream errors. If 4 upstream errors are accumulated in a node without being requested by the concentrator, at every subsequent error the last stored error entry is overwritten.

5.4. Network Management in Concentrators

Concentrator operation is enabled in ME50-868 by setting configuration register 400 to R2-other (value 9). Network management services in a concentrator can be implemented by either the user application (if bit 1 of register 454 is cleared) or the firmware of ME50-868 (if bit 1 of register 454 is set). This flexibility allows users to adapt module operation to their needs: if network management is enabled in the firmware, user applications can be very simple and do not need to know anything about network topology, nor have to implement a network layer; on the other hand, by disabling network management in the firmware users can have a greater degree of flexibility in managing the network topology.

A concentrator handles received network management frames internally only if network management is enabled (i.e. bit 1 of register 454 is set), otherwise these frames are sent to the serial interface, to be processed by the user application.

If bit 1 of register 454 is cleared, each frame received from the serial port is sent as is to the radio interface (except for the PRM bit in the C-field, which is set if not set by the user); this means that if a frame must travel a multi-hop path to reach the end destination, this path must be set up by the user application and inserted in the network information of the frame as described in Section 2.6. Likewise, upstream frames received by the concentrator are sent unmodified to the serial interface, and the user application must parse the network information (if present) to determine the address of the originating node. For frames transmitted and received via the serial port containing network information, the CI-field of the serial frame format refers to the network layer CI-field (which has the value 0x81), while the Data field is the concatenation of network information, application layer CI-field and application data. The user application is fully responsible for building and managing the network tree; for this purpose, it can use the different network management frames described in Section 5.2.

If network management is enabled, network layer data (including its CI-field) is automatically added to frames sent to the radio interface and removed from frames received, and the address fields are adjusted so that user applications can handle frames transferred on the serial port as if the concentrator communicated directly with the end node. The network tree is set up and managed internally by the firmware, and is updated whenever a frame needs to be sent to a

node which is not present in the current tree. If the concentrator knows the destination node as directly reachable (i.e. it has received at least one upstream frame carrying the node address), the node is added to the network tree as direct child of the concentrator. If the destination node cannot be reached directly, known nodes are requested to send their list of known nodes and if necessary their relaying lists are updated; this process continues with the concentrator contacting all the nodes down the tree until a path can be established for the frame to be sent. If a path cannot be established or network information cannot be inserted because the Data-Field supplied by the user is too long, the frame is discarded. During path discovery, the RTS pin of the module is de-asserted, to indicate that no further serial frames can be processed until the current frame is ready to be sent. If a network management frame is received by the concentrator indicating a downstream error, the faulty node is removed from the network tree, along with all the nodes in the tree using that node as an intermediate hop. Broadcast frames received from the serial port are always sent without network information.

Regardless of network management being enabled or not, M-Bus frames received by the concentrator are discarded if they are sent by nodes for which no direct link with the concentrator is set up, unless they are installation frames (function code 6). The list of direct link nodes is built automatically based on frames sent by the concentrator: whenever a frame is being sent directly to a node (either as end destination, or as an intermediate hop toward the end destination), that node is inserted in the list of direct link nodes. If communication with a node fails (i.e. no acknowledgement or response is received when expected) and network management is enabled, the node is removed from the tree, together with all the nodes depending on it to communicate with the concentrator. The maximum number of nodes that a concentrator can handle is 64; if network management is enabled this is the limit on the total number of nodes in the tree, otherwise this limit applies only to direct link nodes. Every node entry is deleted when the module is put in configuration mode and receives either the ATR command or a command that sets register 400 to a valid value; moreover, node entries are deleted when the module is powered off.

When encryption is used to protect transmitted data, decryption of frames traveling in a multi-hop path is performed by the end nodes (meters or concentrator), while intermediate gateways relay the frames unaltered in their application data. When network management is disabled in the concentrator, frames sent by the user application to the serial port have the full path from source to destination in their network layer, and frames sent by the module have the address of the original sender in the network layer. In order to encrypt frames with the correct key, a concentrator with network management disabled parses each frame received from the serial port to determine whether a multi-hop path is used to reach the destination node, and selects the encryption key accordingly. Likewise, before sending to the serial port frames received from the radio interface, the network layer of the frames, if present, is parsed to determine the address of the original sender and consequently the key used to decrypt the frame.

When network management is enabled in the concentrator, having nodes in stand-by mode can influence network tree management, because when a node is unresponsive it is deleted from the tree, along with its downstream nodes.

6. Power Consumption

The table below lists ME50-868 power consumption values in different conditions, with 3.0 V power supply.

Mode	Current Consumption
Tx at 25 mW	39 mA
Rx	28 mA
Stand-by without wakeup on timer	1.4 µA
Stand-by with wakeup on timer	1.9 µA

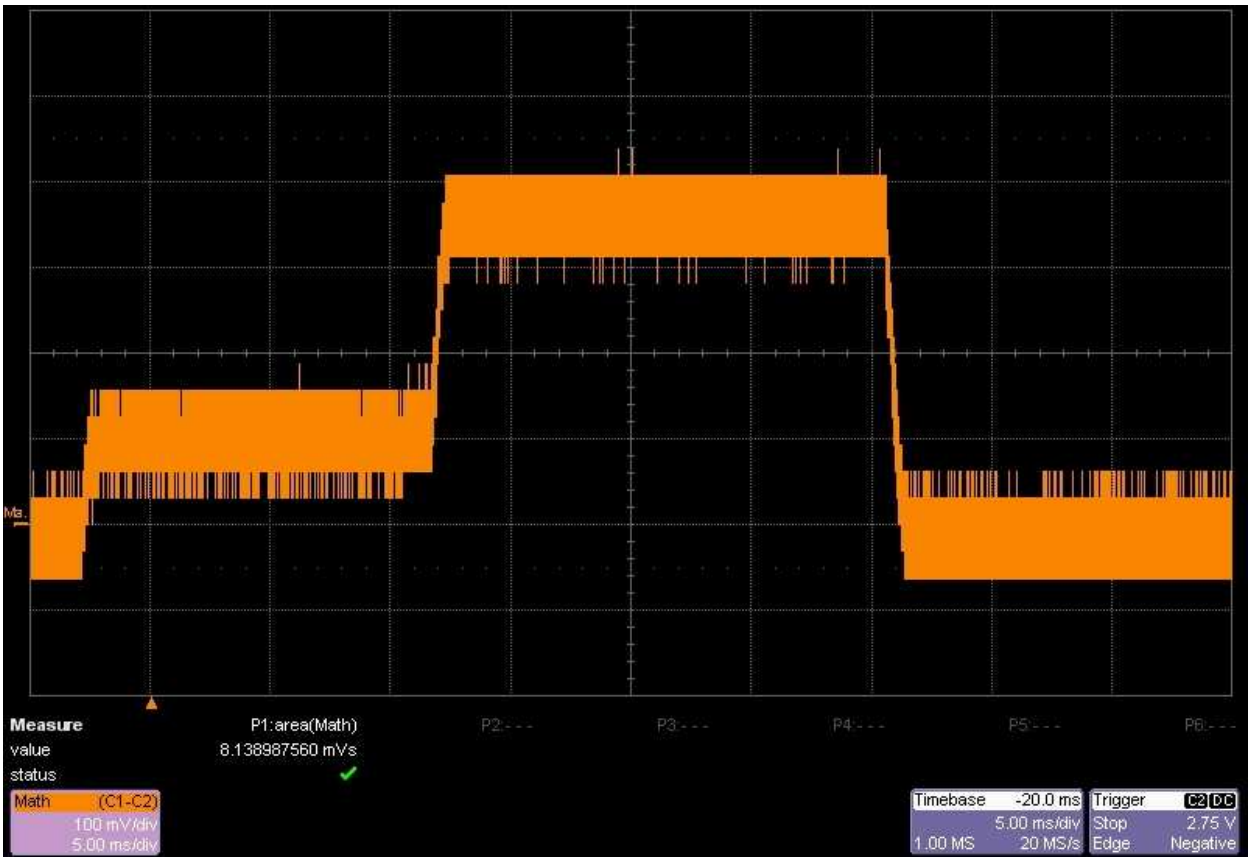
The remainder of this chapter reports a few examples showing power consumption values in typical operating conditions.

6.1. S1 Mode

The following example is using Mode S1 (stationary) of Wireless M-Bus. The stand-by mode is activated, with serial wake-up.

Let us suppose that user equipment wakes-up the module to send a 30 bytes frame with serial data rate at 19200 bps.

Here is a picture of current consumption during a transmission cycle. The power supply voltage is 3 V and the output power is 25 mW. Each such transmission cycle spends typically 814 µAs.



Here is a table of average consumption versus the period of transmission cycles.

Sleep Time	Equivalent Consumption (µA)
1 second	815.4
10 seconds	82.8
1 minute	15
1 hour	1.6
1 day	1.4

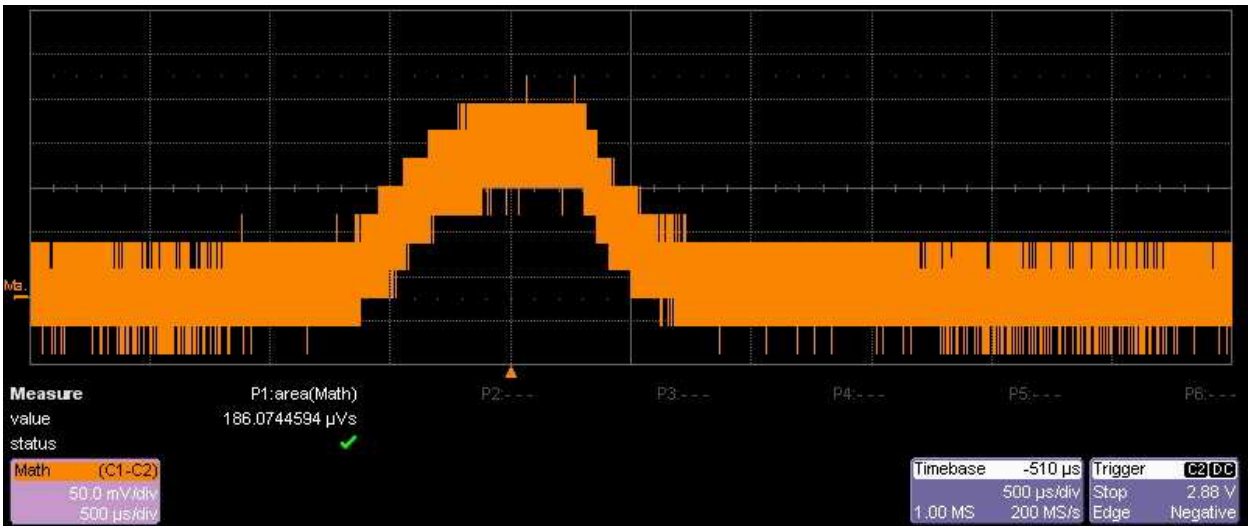
6.2. R2 Mode

The following example is using the R2 mode (frequent receive) of Wireless M-Bus. The stand-by mode is activated, with cyclic wake-up.

With this functioning mode, the meter module wakes up periodically to listen to the radio channel during a very short time. If some activity is detected, the module stays awake to receive the frame, else returns quickly in stand-by mode.

Assuming that the concentrator is rarely present and considering that this band is clear (duty cycle < 1% as requested by ETSI rules in EN 300 220-2), the main current consumption is due to wake up cycles without detection of energy.

Here is a picture of a typical current consumption pattern during a wake-up cycle. The power supply voltage is 3 V. In this case, Wakeup Time Out register 441 has no influence since no event is detected.



Here is a table of average consumption versus wake-up period (register 442) when no exchanges are done and no radio perturbation occurs.

Sleep Time	Equivalent Consumption (µA)
1 second	20.5
5 seconds	5.6
10 seconds	3.8
20 seconds	2.8
30 seconds	2.5
1 minute	2.3
2 minutes	2.1

7. Acronyms and Abbreviations

ACP	Adjacent Channel Power
AES	Advanced Encryption Standard
BCD	Binary Coded Decimal
BER	Bit Error Rate
CBC	Cipher Block Chaining
CER	Character Error Rate
dBm	Power level in decibel milliwatt (10 log (P/1mW))
DES	Data Encryption Standard
EMC	Electro Magnetic Compatibility
EEPROM	Electrically Erasable Programmable Read-Only Memory
ETR	ETSI Technical Report
ETSI	European Telecommunications Standards Institute
FSK	Frequency Shift Keying
GFSK	Gaussian Frequency Shift Keying
GMSK	Gaussian Minimum Shift Keying
IF	Intermediate Frequency
ISM	Industrial, Scientific and Medical
kbps	kilobits per second
kcps	kilochips per second
LBT	Listen Before Talk
LNA	Low Noise Amplifier
LQI	Link Quality Indication
M-Bus	Meter Bus
MHz	Mega Hertz
PLL	Phase Lock Loop
NRZ	Non Return to Zero
RF	Radio Frequency
RoHS	Restriction of Hazardous Substances
RSSI	Received Signal Strength Indicator
Rx	Reception
SRD	Short Range Device
Tx	Transmission
SMD	Surface Mounted Device
VCO	Voltage Controlled Oscillator
VCTCXO	Voltage Controlled and Temperature Compensated Crystal Oscillator

8. Document History

Revision	Date	Changes
0	2009-05-04	First issue
1	2009-09-17	• Updated product applicability • Updated graphics in Chapter V
2	2010-03-30	• Added information on activation of Mode S1-m • Updated format of firmware version string • Updated register 440 description
3	2010-11-18	• Added new Wireless M-Bus product (ME50-868)
4	2011-01-31	• Removed TinyOne Lite product • Added ME50-868 additional features
5	2011-06-23	• Renamed RSSI serial frame field to LQI • Added new RSSI serial frame field • Removed Serial Type configuration register • Added LBT transmission option • Added remote AT commands • Added power consumption examples for Mode R2 • Changed endianness of signature field • Changed document template
6	2013-05-06	• Changed software version to U00.01.03