Telit WMBUS EN 13757-4:2010 User Guide

1VV0300953 Rev.1 – 2011-09-29

Making machines talk.

APPLICABILITY TABLE

PRODUCT
ME50-868
ME50-169

SW Version
U03.01.00

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

1.1. Scope

Scope of this document is to present the features and the application of the Wireless M-Bus EN 13757-4:2010 embedded stack available on ME50-868 and ME50-169.

1.2. Audience

This document is intended for software developers and system integrators using ME50-868 or ME50-169 modules with Wireless M-Bus EN 13757-4:2010 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 ME50-169 and describes the pinout of the modules.

"Chapter 4: "Software Operation" describes the operation of the Wireless M-Bus EN 13757-4:2010 firmware and how it interfaces with an external host.

"Chapter 5: "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 13757-3:2011
- EN 13757-4:2010
- Open Metering System Specification – Primary Communication – Issue 2.0.0
- Dutch Smart Meter Requirements v4.0 – 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 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 bands at 169, 433 and 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 EN 13757-4:2010 defines six different ways to exchange data with remote meters:

- Mode S 'Stationary'
- Mode T 'frequent Transmit'
- Mode R2 'frequent Receive'
- Mode C 'Compact'
- Mode N 'Narrowband VHF'
- Mode F 'Frequent receive and transmit'

ME50-868 with the firmware described in this document supports all the modes designed for the 868 MHz frequency band, namely modes S, T, R2 and C, while ME50-169 supports mode N at 169 MHz.

2.2.1. Mode T

In mode T, the meter sends spontaneously data, either periodically or stochastically. Frame transmission from meters to other devices uses a bit rate of 100 kbps, while communication in the opposite direction is carried out at 32.768 kbps.

- In Mode T1 the meter doesn't care if any receiver is present or not. The meter sends data and returns immediately in power-save mode without waiting for a response. 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 response frame. If no response is received, the meter returns in power-save mode. If a response 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 power-save mode. If a valid wakeup frame is received, a bidirectional link is then opened between meter and concentrator. The bit rate used in this mode is 4.8 kbps.

2.2.3. Mode S

The bit rate for radio communication is 32.768 kbps. The following two sub-modes are defined:

- Mode S1 operates exactly as Mode T1 (unidirectional spontaneous transmission) but uses a different radio link.
- Mode S2 is similar to Mode T2 (meter sends a frame and waits for a response during a short interval) but also with a different physical link.

2.2.4. Mode C

This mode is similar to mode T but uses a different encoding scheme (NRZ); communication from meters to other devices is at 100 kbps, while in the opposite direction a 50 kbps bit rate is used. Two sub-modes are defined, C1 for unidirectional communication from meters to other devices and C2 for bidirectional communication.

2.2.5. Mode N

It uses narrowband communication in the 169 MHz frequency band; the two sub-modes C1 and C2 are for unidirectional and bidirectional communication, respectively. Different channels are defined, with different bit rates and modulation types, as listed below:

- Channel 1a: 4.8 kbps, GMSK modulation
- Channel 1b: 4.8 kbps, GMSK modulation
- Channel 2a: 2.4 kbps, GFSK modulation
- Channel 2b: 2.4 kbps, GFSK modulation
- Channel 3a: 4.8 kbps, GMSK modulation

- Channel 3b: 4.8 kbps, GMSK modulation
- Channel 0: 38.48 kbps, 4-GFSK modulation

2.2.6. Mode F

It is a bidirectional mode operating at 2.4 kbps in the 433 MHz frequency band; communication can be initiated by either the meter (similar to Mode T2) or the concentrator (using a wakeup frame as is done in Mode R2).

2.3. Data Format on RF Link

EN 13757-4:2010 defines two different packet formats, namely format A and B. Multi-byte fields described in the following subsections are transmitted least significant byte first, except the CRC fields, which are transmitted most significant byte first.

2.3.1. Frame Format A

This format can be used in any of the Wireless M-Bus modes listed in Section 2.2. Radio frames with this format are composed of a number of blocks, as illustrated in the figure below.

Preamble	Block 1	Block 2	Block n	Postamble

The preamble is used for synchronization between transmitter and receiver; the EN 13757-4 specification imposes a minimum limit for preamble length, which depends on the mode used:

- Mode S: 6 bytes if short preamble is used, otherwise 72 bytes (long preamble); refer to Section 4.2 for information on how to select short or long preamble
- Mode T: 6 bytes
- Mode R2: 12 bytes
- Mode C: 8 bytes
- Mode N: preamble length depends on the modulation used (4 bytes for GFSK and GMSK, 8 bytes for 4GFSK)
- Mode F: 12 bytes

ME50-868 modules always use the minimum required preamble length when transmitting frames.

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

Block 2 and Block n are optional. A frame can have multiple blocks with the format of Block n; their number depends on the length of the data field. The postamble is a short bit sequence added at the end of frames in modes S, T and R2.

2.3.2. Frame Format B

This format can optionally be used in Modes C and F; frames with this format are composed of the following blocks:

Preamble	Block 1	Block 2	Block 3

The preamble is needed for synchronization between transmitter and receiver; its length is 8 bytes for Mode C and 12 bytes for Mode F.

Block 1 format:

L-field	C-field	M-field	A-field
1 byte	1 byte	2 bytes	6 bytes

Block 2 format:

CI-field	Data-field	CRC-field
1 byte	115 bytes or (L – 12) bytes	2 bytes

Block 3 format:

Data-field	CRC-field
(L – 129) bytes	2 bytes

Block 2 and Block 3 are optional. Block 3 is present only if the length of the data field is bigger than the number of bytes allowed in Block 2. The CRC field of Block 2 is calculated on the concatenation of Block 1 and Block 2 data.

2.3.3. Field Definitions

Frame fields referred to in Sections 2.3.1 and 2.3.2 are defined as follows:

- **L-field** is the length indication: the difference between frame format A and B is that in the former case this field does not include the length of CRC-fields, while in format B frames it includes the length of CRC-fields
- **C-field** is the communication indication (request, send, response expected, ACK…)
- **M-field** is the Manufacturer ID of the sending device
- **A-field** is the address of the sending device and is composed of the concatenation of an identification number (4 bytes), a version code (1 byte) and a device type code (1 byte)
- **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)

2.3.4. Extended Link Layer

When the CI-field assumes the values 0x8C or 0x8D, the first bytes of the Data-field contain an extended link layer, which is followed by another CI-field and then the application data.

The extended link layer can have one of two formats. The first is illustrated below and is present when the CI-field is set to 0x8C.

CC	ACC
1 byte	1 byte

The second format is present when the CI-field is set to 0x8D and is illustrated below.

CC	ACC	SN	PayloadCRC
1 byte	1 byte	4 bytes	2 bytes

CC is a communication control field and is coded using the following bitmask:

B-field	RD-field	S-field	R-field	P-field	Reserved
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bits 2 - 0

- **B-field**, when set to 1, indicates that the sending device implements bidirectional communication
- **RD-field** controls the response delay of the responding device, indicating whether a fast (RD-field set) or slow (RD-field cleared) response delay should be used
- **S-field**, when set to 1, indicates a synchronized frame
- **R-field**, when set to 1, indicates that the frame has been relayed by a repeater
- **P-field**, when set to 1, indicates a high priority frame

ACC is the access number and is used to detect duplicate frames and to associate request and response frames.

SN (Session Number) is a 4 byte field (transmitted least significant byte first) with the following content:

ENC-field	Time-field	Session-field
Bits 31 – 29	Bits 28 – 4	Bits 3 - 0

- **ENC-field** specifies the encryption method, with the value 0 meaning no encryption and the value 1 meaning AES-128 Counter Mode encryption; other values are reserved for future use. If AES-128 Counter Mode is used, the remaining bytes of the frame, from and including the PayloadCRC field (but excluding the CRC fields), will be encrypted.
- **Time-field** is a relative minute counter and is used together with the Session-field to ensure that the encrypted transmission is protected from replay attacks

- **Session-field** is a zero-based index of the communication session within the minute specified by the Time-field

PayloadCRC is a cyclic redundancy check covering the remainder of the frame (excluding the CRC fields).

2.3.5. Data Header

If the application layer defined by EN 13757-3 is used, depending on the value of the CI-field, the first bytes of the Data-field may contain a data header as specified in this section. Two types of data header (short and long) are defined. The short data header is present when the CI-field assumes one of the following values: 0x5A, 0x61, 0x65, 0x6A, 0x6E, 0x74, 0x7A, 0x7B, 0x7D, 0x7F and 0x8A; it is formatted as illustrated below:

ACC	STS	Conf
1 byte	1 byte	2 bytes

The long data header is present when the CI-field has one of the values 0x5B, 0x60, 0x64, 0x6B, 0x6C, 0x6D, 0x6F, 0x72, 0x73, 0x75, 0x7C, 0x7E, 0x80, 0x84, 0x85 and 0x8B; it is formatted as follows:

Identification Number	Manufacturer ID	Version	Device Type	ACC	STS	Conf
4 bytes	2 bytes	1 bytes	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.

Device Type specifies the functionality of the device (for example, electricity meter).

The set of **Identification Number**, **Manufacturer ID**, **Version** and **Device Type** fields identify the Application Layer Address, which is used as described later in this section.

ACC is the access number and is used to detect duplicate frames and to associate request and response frames.

STS is the status byte and its meaning depends on whether the frame is sent by a meter or a concentrator.

Conf is the configuration word, whose primary purpose is to specify the encryption method used to encrypt the frame.

Two encryption algorithms are defined in EN 13757-3:2011, namely DES and AES-128; for both algorithms, Cipher Block Chaining (CBC) is used as mode of operation. Four different 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. Method 3 needs the long data header to initialize the CBC algorithm, therefore it can be used only together with this header type; the other methods can be used with either the short or long data header.

The P2 Companion Standard of Dutch Smart Meter Requirements defines an additional encryption method (with code 15), which uses AES-128 with CBC. This method differs from those defined in EN 13757-3 in that it requires a 32-bit frame counter to initialize the CBC algorithm. The frame counter is transmitted unencrypted with least significant byte first, is preceded by the fixed 3-byte header [0x04, 0xFD, 0x08] and is inserted at the end of the encrypted frame.

The configuration word of the data header contains 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 configuration word do not enter in the count of encrypted bytes, and can be used for other purposes.

The link layer header of Wireless M-Bus frames carries the manufacturer ID and address of the sending device in the M-field and A-field, respectively, as described in Section 2.3.3; the set of these two fields is referred to as Link Layer Address (LLA). In frames sent from concentrators, additional fields are needed to identify the receiving meter; for this purpose, the Application Layer Address (ALA) is used, as defined above in the long data header. Please note that LLA and ALA differ in the relative position of their sub-fields: in the LLA the manufacturer ID is the first sub-field, while in the ALA the manufacturer ID is inserted between the identification number and the version code.

3. Hardware Characteristics

This chapter synthesizes the hardware characteristics of ME50-868 and ME50-169 when used with the EN 13757-4:2010 firmware. For more detailed information, please refer to the user guides of the modules.

Below is a summary of ME50-868 RF module specifications for Wireless M-Bus. Refer to EN 300 220-2 v2.3.1 for the exact definition of the RF parameters.

	Min	Typ	Max	Unit	Note
Output power	-	+13	+14	dBm	Selectable by software from 0 to +14 dBm
Sensitivity @ 32.768 kcps	-	-100	-	dBm	
Sensitivity @ 100 kcps	-	-101	-		
Sensitivity @ 4.8 kcps	-106	-107	-108		
Sensitivity @ 50 kcps	-	-104	-		
Blocking@ 32.768 kcps	28 min @ ± 2 MHz 53 min @ ± 10 MHz			dB	
Blocking@ 100 kcps	24 min @ ± 2 MHz 49 min @ ± 10 MHz				
Blocking@ 4.8 kcps	37 min @ ± 2 MHz 62 min @ ± 10 MHz				
Blocking@ 50 kcps	TBD				

The following table summarizes the RF specifications of ME50-169.

	Min	Typ	Max	Unit	Note
Output power	0	-	+14	dBm	Selectable by software from 0 to +14 dBm

Sensitivity @ 2.4 kcps	-	-120	-	dBm	
Sensitivity @ 4.8 kcps	-	TBD	-		
Sensitivity @ 38.4 kcps	-	TBD	-		
Blocking@ 2.4 kcps	TBD			dB	
Blocking@ 4.8 kcps	TBD				
Blocking@ 38.4 kcps	TBD				

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

The module can operate in two 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, and <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 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 '+' characters 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

AT/V	'AT/V' command displays the modem's firmware and bootloader version number as follows: pp.UP3.MM.mm-Bbbb<CR>pp.B00.NN.nn With: pp indicating the hardware platform (GC for ME50-868, GI for ME50-169) UP3: 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.U03.01.02-B011<CR>GC.B00.01.10 indicates an EN 13757-4:2010 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
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
ATT	Continuous modulated carrier, simulating transmission of '01' data (or '0111' data if 4GFSK modulation is used in Mode N). Answer : OK 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. Valid values for ME50-868: • **'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 • '10': Mode C1-meter • '11': Mode C1-other • '12': Mode C2-meter • '13': Mode C2-other Note: to activate Mode S1-m, select S1 in this register and then act on preamble length in register 421. Valid values for ME50-868: • **'14': Mode N1-meter (default)** • '15': Mode N1-other • '16': Mode N2-meter • '17': Mode N2-other
R/W	401	Serial Rx Format	Indicates the serial format options for serial frames sent from user to RF module

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

Default value : 0

<table>
<tr><td></td><td></td><td colspan="2">

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)

</td></tr>
<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><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>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 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.</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>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 and N modes only).
Valid values for R2 mode: from 0 to 9
Valid values for N mode: from 0 to 6, corresponding to the channels listed below:
• ‘0’: 1a (default)
• ‘1’: 1b
• ‘2’: 2a
• ‘3’: 2b
• ‘4’: 3a
• ‘5’: 3b
• ‘6’: 0
Default : 0</td></tr>
<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).
This register is only available for ME50-868.</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
‘3’: +14 dBm (default)</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><th>Min. timeout</th><th>Serial speed</th></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="3"><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></table></td></tr>
</table>

<table>
<tr><td></td><td></td><td colspan="2">
<table>
<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>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 (only for ME50-868); the timer period is 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>
<tr><td>R/W</td><td>441</td><td>Wakeup Time Out</td><td>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 after frame transmission when the module is configured as bidirectional meter. For unidirectional meters this register may be set to zero 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</td></tr>
<tr><td>R/W</td><td>442</td><td>Sleep Time</td><td>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
This register is only available for ME50-868.</td></tr>
<tr><td>R/W</td><td>452</td><td>Rx Filter</td><td>Indicates whether received radio frames are filtered based on their M-field and A-field.
• ‘0’: Rx filter disabled (default)
• ‘1’: Rx filter enabled</td></tr>
<tr><td>R/W</td><td>453</td><td>Tx Options</td><td>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: enable frame format B when in Mode C
• Bit 3: enable automatic frame transmission
• Bit 4: enable synchronized frame transmission
• Bit 5–7: reserved
Refer to Section 4.5 for details on transmission options.
Default: 0</td></tr>
<tr><td>R/W</td><td>454</td><td>Repeater</td><td>Enables or disables repeater operation in Mode S or T.
Refer to Section 4.5.12 for details on repeater functionality.
Valid values: 0 (disable), 1 (enable)
Default: 0
This register is only available for ME50-868.</td></tr>
</table>

<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>Automatic ACK</td><td>Automatic CNF-IR</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’ in concentrators to enable sending to the serial port frames received from the registered meter
Bit 2: Activates encryption and decryption to frames exchanged with the registered meter
Bit 3: enable automatic generation of CNF-IR frames to registered meter (refer to Section 4.5.10 for more details)
Bit 4: enable automatic generation of ACK frames to registered meter (refer to Section 4.5.10 for more details)

</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. 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>

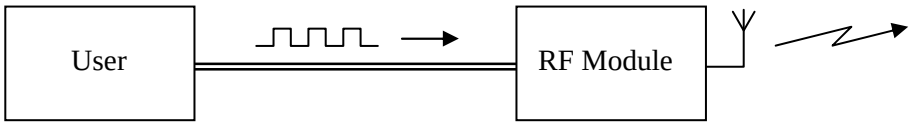
4.3. Operating Mode

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 rules do not apply when repeater operation is enabled; refer to Section 4.5.12 for information on repeater operation.

Data transmitted or received over the serial port will have a specific format depending on the module configuration defined through the different registers. It allows a high flexibility in the use of the module in a Wireless M-Bus application.

A module configured as unidirectional meter (register 400 set to 0, 4 or 10) does not activate frame reception on the radio interface. 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 allows 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. 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 ID 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.
Data	Variable	**Data field.** User application data; its minimum length is 0 bytes and its maximum length is 245 for frame format A and 241 for frame format B.

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

When the Length field is activated in the serial Rx format options, if the value of the field received by the module is outside the range of values allowed to build a valid data frame, the received byte is discarded.

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, the frame will have the following format (assuming frame format A is used):

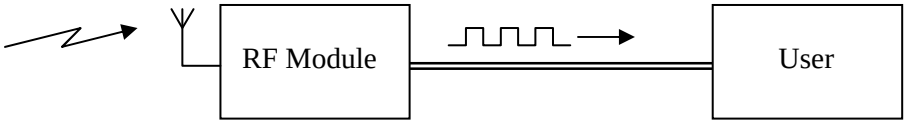
Preamble

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 Mode R2 to work as “Wake On Radio” way. With this character 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 the subsequent bytes, including other serial options fields if any, but excluding LQI and RSSI fields.
C	1	**C-field** Specifies the role of the frame (Request, ACK, ...).
M	2	**Manufacturer ID and Address fields** Indicate the M-field and A-field 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.
Data	Variable	**Data field.** User application data; its minimum length is 0 bytes and its maximum length is 245 for frame format A and 241 for frame format B.
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. Stand-by mode is not activated when repeater operation is enabled (refer to Section 4.5.12): in this case, the configuration options set in register 440 do not have effect and the module remains always active.

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 (only for ME50-868): 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 two 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 the wakeup timeout defined by register 441 expires, if a radio frame reception is ongoing, the module does not enter stand-by mode but waits for the incoming frame to be received. Frame reception is considered to be initiated when the preamble has been received (refer to Sections 2.3.1 and 2.3.2 for more information on frame preamble). If a device expects to receive a frame within a defined time interval, the wakeup timeout of the module should be set to a value higher than the expected delay of the beginning of the frame, to take into account preamble transmission. The duration of frame preamble for a given mode can be calculated from the bit rate value (reported in Section 2.2) and the preamble length.

When timer is enabled, the stand-by consumption of the RF module is higher (refer to consumption data in Chapter 5).

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 returns 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 the module. 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 10%, depending on M-Bus mode and device type. When the duty cycle limit is 10% (as is for concentrator devices operating in Mode C or Mode N, as well as for meter devices operating in Mode N in channels from 0 to 5), this limit is not enforced by the module because of limited memory resources; in this case the user application should take care of staying within the limit.

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 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 the module 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, the module listens to the wireless medium before transmitting a radio frame. The minimum listen time is 5 ms; if during this time no activity is detected on the radio link, frame transmission starts immediately, otherwise the module 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, the module waits for the channel to become free and then restarts the listen procedure.

4.5.4. Date and Time

The module 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 on command syntax).

4.5.5. Frame Format B

When operating in Mode C, the module is able to send and receive Wireless M-Bus frames coded with format B (refer to Section 2.3.2 for format details). Frames with either format A or B can be received by the module without any specific configuration; to send frames with a specific format, bit 2 of configuration register 453 is used: when this bit is set to 1, frame transmission is done using format B, otherwise the default format A is used. Bit 2 of register 453 can be set to 1 only when the module is configured to operate in Mode C.

4.5.6. Registered Meters

A module can register up to 32 meters, to be used for filtering received M-Bus frames, encrypting radio communication, or generating automatic messages. 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, if present in the list, is unregistered. An error response is returned by the module 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 Sections 4.5.8, 4.5.9 and 4.5.10 for details on how to use registered meters and their option flags.

4.5.7. Frame Filtering

An optional filter on received M-Bus frames can be activated, which allows transmitting to the serial port only frames whose meter manufacturer ID and address match one or more specific values. If an Application Layer Address if present in a received frame, the meter manufacturer ID and address are taken from those fields, otherwise the Link Layer Address is used to identify the meter; refer to Section 2.3 for details on the address formats. 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.

Concentrators can use the frame filtering feature of the module 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 2.3.3 for a description of C-field format). In order to be able to receive frames from meters in installation mode, when the module is configured to act as concentrator, filtering does not apply to received frames in which the C-field has the PRM bit set to 1 and the function code set to 6: these frames are sent to the serial port regardless of the frame filtering option.

4.5.8. Encryption

The module can encrypt and decrypt Wireless M-Bus frames to provide secure communication between nodes. Both DES and AES-128 encryption algorithms as defined in EN 13757-3:2011 are supported, as well as AES-128 with Counter Mode as defined in EN 13757-4:2010.

In order to use encrypted communication, frames sent by the user application must contain either an extended link layer containing the Session Number field with a valid encryption method (refer to Section 2.3.4), or a data header as defined in Section 2.3.5. Depending on the contents of the frame, the module encrypts or decrypts it with the appropriate method.

AES-128 with Counter Mode encryption, as defined in EN 13747-4:2010, is supported only for communication from meters to concentrators, thus it is most suited to unidirectional modes.

The encryption methods defined in EN 13757-3 are identified by codes 2, 3, 4 and 5. 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. Beside the methods defined in EN 13757-3, the module supports method 15 defined in the Dutch Smart Meter Requirements. Refer to Section 2.3.5 for more details on the different encryption methods.

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 2 must be set to 1 in the option register 460. A meter device must insert its own manufacturer ID, address and key in an entry of the registered meter list and set bit 2 of register 460. The manufacturer ID and address of the meter in a given frame are taken from the Link Layer Address if the CI-field of the frame does not indicate a long data header, otherwise they are taken from the Application Layer Address.

Once all the relevant configuration registers for encryption have been set, when a frame with an extended link layer or a data header specifying one of the supported encryption methods is received from the serial port, the module encrypts the frame using the key corresponding to the meter manufacturer ID and address and the given encryption method. If method 15 is used, the user application must insert a frame counter and its header at the end of the serial frame, as described in Section 2.3.5. If the encryption method is incompatible with the CI-field, or if method 15 is specified but the frame counter and its header are not present at the end of the data field, the frame is discarded. If the encryption method is not supported (or is 0, which means no encryption), the frame is sent unencrypted. Before encrypting a frame, if CBC is used (as defined in EN 13757-3) 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); if filler bytes cannot be added because the maximum frame length has been reached, the frame is discarded. If encryption method 15 is used, when filler bytes are added to the frame to be encrypted, the frame counter and its header are moved accordingly so that they are placed after the encrypted data. The number of encrypted blocks contained in the configuration word provided by the user is ignored, and the value corresponding to the length of the encrypted content is inserted in the configuration word before sending the frame (sent frames cannot be partially encrypted).

When receiving from the radio interface an encrypted Wireless M-Bus frame, if the meter address corresponds to a registered meter with encryption enabled, the module decrypts the frame before sending it to the serial port, provided the frame contains a valid extended link layer or 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 configuration word, or encryption method incompatible with data header) are discarded, and frames with unsupported encryption methods are sent unaltered to the serial port. Decryption of partially encrypted frames is supported. The module does not modify the SN field or the configuration 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.

4.5.9. Remote AT Commands

The module 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 the module from a remote host.

A Wireless M-Bus frame containing an AT command for a given module must have the C-Field set to 0x4B 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 first 8 bytes of the Data-Field must contain the manufacturer Id and address of the module to which the command is directed, corresponding to the contents of configuration registers 411 to 418 of the receiving module. After the module identification, 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, the module, 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 CI-Field set to 0xA0; the first part of the Data-Field contains the manufacturer Id and address of the module which sent the command frame, while the rest of 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.

4.5.10. Automatic frame transmission

In typical installations, meter devices are battery-powered, thus energy saving mechanisms must be implemented in order to optimize battery consumption. The standard approach prescribed in the EN 13757-4:2010 specification for battery-operated meters is to enable the radio receiver for a small amount of time after every frame transmission, and then disable radio reception until the next frame transmission. If the meter receives a frame during the short interval in which reception is activated, it enters the so-called Frequent Access Cycle (FAC), during which it sends a frame every few seconds and then listens for a frame from the concentrator; the FAC allows the concentrator to communicate with meter with a short latency. The FAC ends either when a specific frame is sent by the concentrator, or when the meter does not receive frames for a specified amount of time.

In order for a frame to be received by a meter operating with the above logic, the concentrator must transmit the frame within a short time interval after the meter transmission. This constraint is particularly severe in modes T and N, in which frame transmission by the concentrator must start within 3 milliseconds after reception of the frame from the meter; since each frame received and transmitted by the module must pass through the serial port in order to interact with the user application, standard module operation might not be able to satisfy the timing requirements of EN 13757-4. For this reason, a feature has been introduced

which allows a module configured as concentrator to automatically send frames to meters, based on specific rules as described in the rest of this section.

When bit 3 of configuration register 453 is set to 1, a frame received on the serial port by a module configured as concentrator is not sent immediately to the radio interface, but is stored in the module memory to be sent later when specific conditions are met, as described later in this section. This stored frame can either refer to a specific destination meter, or be a generic frame, based on the meter address; as always, the meter address is taken from the Application Layer Address if the stored frame has a CI-field indicating the presence of a long data header, otherwise it is taken from the Link Layer Address. The stored frame is a generic frame when its meter address has a special value in which all bytes are set to 0xFF; generic frames are used to let the module generate automatically the meter destination address based on frames received from the radio interface. Only one frame can be stored in the module memory for deferred transmission: if the module receives more than one frame from the serial port, the last frame will overwrite the preceding frames.

Standard Wireless M-bus frames sent by a meter should contain information on whether the meter is able to receive a response frame from the concentrator. If the meter uses the extended link layer, this information is carried in the B-field of the CC field (refer to Section 2.3.4), which is set to 1 to indicate that the meter supports bi-directional communication. If no extended link layer is present and a standard data header (Section 2.3.5) is used instead, and the configuration word indicates an encryption method with one of the values 0, 4, 5, 6 and 15, the most significant bit of the second byte of the configuration word indicates whether the meter is able to receive frames: if this bit is set to one, it means that the meter can receive frames. When a module configured as concentrator receives a frame indicating that the sending meter can receive a response, the module can automatically send a frame to the meter based on the following rules:

- If the received frame has a C-field with the PRM bit set to 1 and a function code set to 6 (installation request), and the sending meter is a registered meter in the concentrator module with bit 3 (automatic CNF-IR) of the option flags set to 1, the concentrator automatically sends a response frame with the C-field set to 6 and a long data header containing the meter address. This frame exchange is typically used at installation time when the meter searches for a concentrator to bind to; the response from the concentrator indicates that the concentrator accepts the installation request from the meter.
- If the received frame has a C-field with the PRM bit set to 1 and a function code set to 8, and the sending meter is a registered meter in the concentrator module with bit 4 (automatic ACK) of the option flags set to 1, the concentrator automatically sends a response frame with the C-field set to 0 and a long data header containing the meter address. This frame exchange is typically used when the meter has data to transmit and wants the concentrator to request this data; the concentrator response activates the Frequent Access Cycle.
- If the module in the concentrator has a stored frame and its meter address corresponds to the address of the sending meter, the concentrator sends automatically the stored frame.
- If the module in the concentrator has a stored frame and its meter address has all bytes set to 0xFF (generic frame), the concentrator sends automatically the stored

frame after replacing the 0xFF bytes of the meter address with the address of the sending meter.

In the above rules, if the CI-field of the frame sent by the meter indicates the presence of a long data header the meter address is taken from the Application Layer Address, otherwise the meter address is taken from the Link Layer Address.

When a stored frame is automatically sent by the concentrator, it is encrypted as described in Section 4.5.8 if the destination meter is a registered meter with encryption enabled. In case of a generic frame, the encryption must be carried out after determining the address of the sending meter; since AES-128 encryption is a computationally intensive process, if more than four 16-byte blocks have to be encrypted in a generic frame, the module is unable to satisfy the timing requirement of Mode T. For this reason, if frames with more than 4 encrypted blocks have to be automatically transmitted in Mode T, it is recommended to use stored frames with a specific meter address, because in this case frame encryption can be performed as soon as the frame is received from the serial port.

4.5.11. Synchronized frame transmission

Bit 4 of configuration register 453 allows controlling the timing of frames sent by the concentrator. If this bit is cleared, every frame to be sent to the radio interface is sent as soon as the module is ready to send it, after the internal processing done by the firmware (such as encryption and CRC calculation). If this bit is set to 1, the module sends frames after a specific delay from the last received frame; this feature is useful to ensure that the concentrator response to a frame sent by a meter satisfies the requirements on minimum response delay prescribed by EN 13757-4.

The minimum response delay values used by the module for the different modes are taken from the EN 13757-4:2010 specification and are listed below:

- Mode S: 3 ms
- Mode T: 2 ms
- Mode R2: 10 ms
- Mode C: the delay value depends on the contents of the frame received from the meter: if the frame contains an extended link layer, the RD-field of the CC byte (refer to Section 2.3.4) indicates whether a fast (90 ms) or slow (1000 ms) response delay should be used; if no extended link layer is present, by default a fast response delay is used.
- Mode N: 2 ms

Synchronized frame transmission can be used together with the automatic frame transmission mechanism described in the previous section; in this case, automatic frames are sent by the concentrator after the minimum response delay defined for the different modes.

If synchronized transmission is used without automatic transmission, when a frame is received from the serial port the module checks if the minimum delay value has passed since the last received frame, and if necessary the module waits for this delay to pass before transmitting the frame.

4.5.12. Repeater operation

The Open Metering System Specification defines the functionality of repeater devices, used to extend the communication range between meters and concentrators. These devices are unidirectional repeaters, which receive frames sent by meters and forward them toward the concentrator; the use of such repeaters is limited to modes S and T.

ME50-868 modules can provide autonomous repeater functionality according to the OMS specification. This feature is enabled when configuration register 454 is set to 1 and register 400 is set to either 3 (for Mode S) or 7 (for Mode T). When repeater operation is enabled, the module can work autonomously (i.e. without an external host connected to the serial port).

A module functioning as repeater does not send or receive frames through the serial port; any character received from the serial port is discarded by the module, except the '+' character which is used to enter configuration mode. As soon as three '+' characters are received, the module sends the "OK\r" response, deactivates repeater operation and enters configuration mode (refer to Section 4.1).

A Wireless M-Bus frame received by a repeater is forwarded only if its C-field is either 0x44 or 0x46; also, the received frame must have a data header as described in Section 2.3.5, its configuration word must indicate an encryption method with one of the values 0, 5 and 6, and the two least significant bits of the first byte of its configuration word must be zero. When the above conditions (dictated by the OMS specification) are met, the repeater stores the received frame and forwards it automatically after a random delay between 5 and 25 seconds; the repeated frame is identical to the original frame, with the exception that the least significant bit of the first byte of the configuration word is set to 1.

If a received frame has the C-field set to 0x46 (typically used during the installation process), the repeater stores an additional frame to be sent (with a random delay of at least 2 seconds) after repeating the received frame. This additional frame has the M-field and A-field set to the manufacturer ID and address of the repeater, the C-field set to 0x40 and a long data header with the Application Layer Address of the sending meter and a status byte containing the RSSI of the received frame coded as described in EN 13757-3; if the RSSI of the received frame is greater than -6 dBm, the status byte is set to 63, otherwise it contains a value expressed by the following formula: (RSSI + 130 dBm) / 2. This additional frame is typically used by an optional installation service tool to verify that the repeater is in communication range with a given meter.

The module is able to store internally up to 16 frames (whose Data-field has a maximum length of 15 bytes) to be transmitted when the random delay expires; for frames with a Data-field bigger than 15 bytes, the maximum number of storable frames decreases proportionally. When a frame cannot be stored due to unavailable memory resources, the frame is discarded.

As prescribed in the OMS specification, a module operating as repeater sends periodically (every 240 minutes) a management frame containing its status.

When repeater operation is enabled, the configuration settings in register 440 are ignored and module does not enter stand-by mode.

5. Power Consumption

The table below lists ME50-868 and ME50-169 power consumption values in different conditions, with 3.0 V power supply.

Mode	Current Consumption ME50-868	Current Consumption ME50-169
Tx at 25 mW	39 mA	52 mA
Rx	28 mA	35 mA
Stand-by without wakeup on timer	1.4 µA	1.4 µA
Stand-by with wakeup on timer	1.9 µA	-

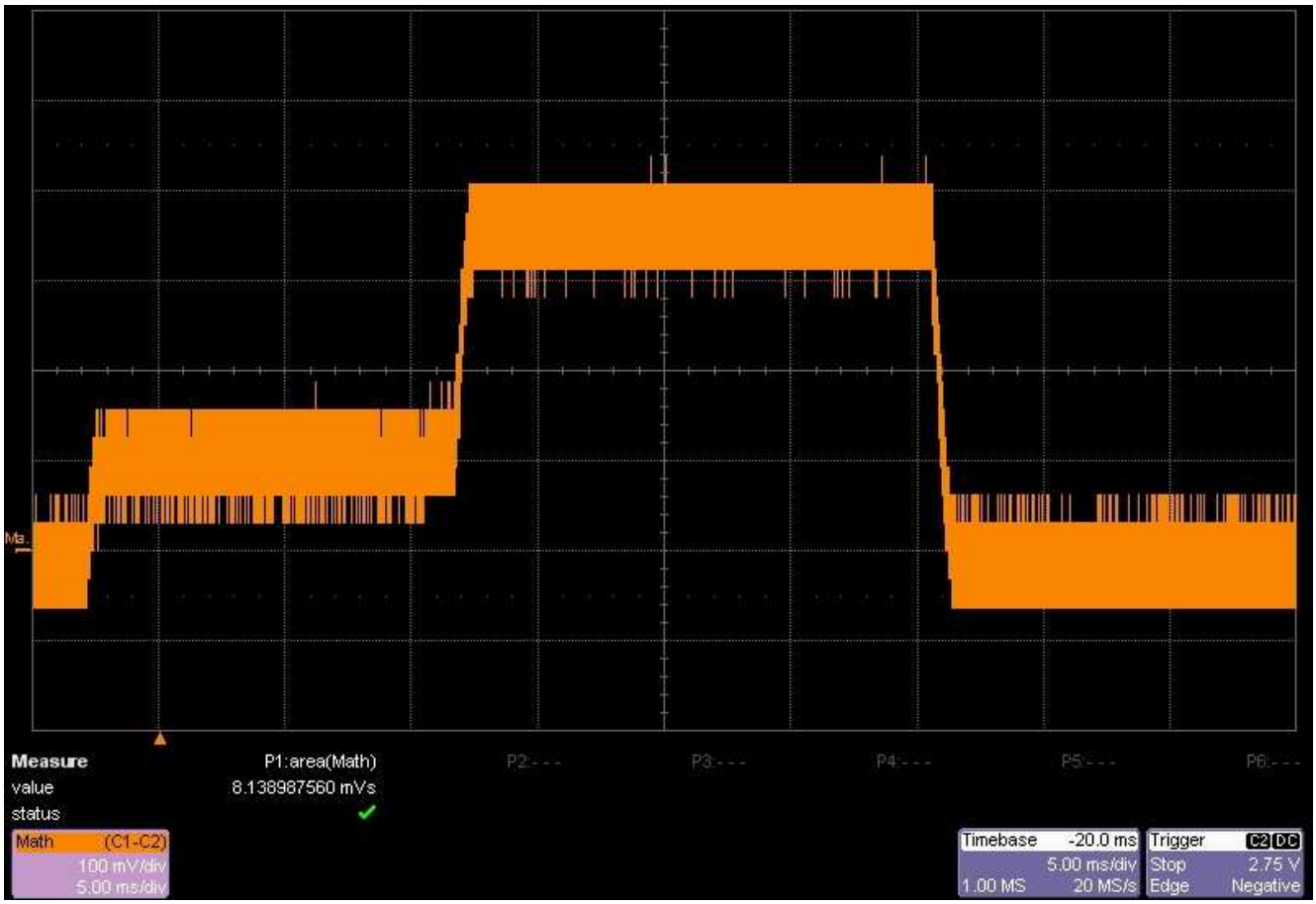
The remainder of this chapter reports a few examples showing power consumption values in typical operating conditions.

5.1. S1 Mode

The following example is using Mode S1 (stationary) of Wireless M-Bus. The stand-by mode is activated, with serial wake-up, and the wakeup timeout value (register 441) is set to zero.

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

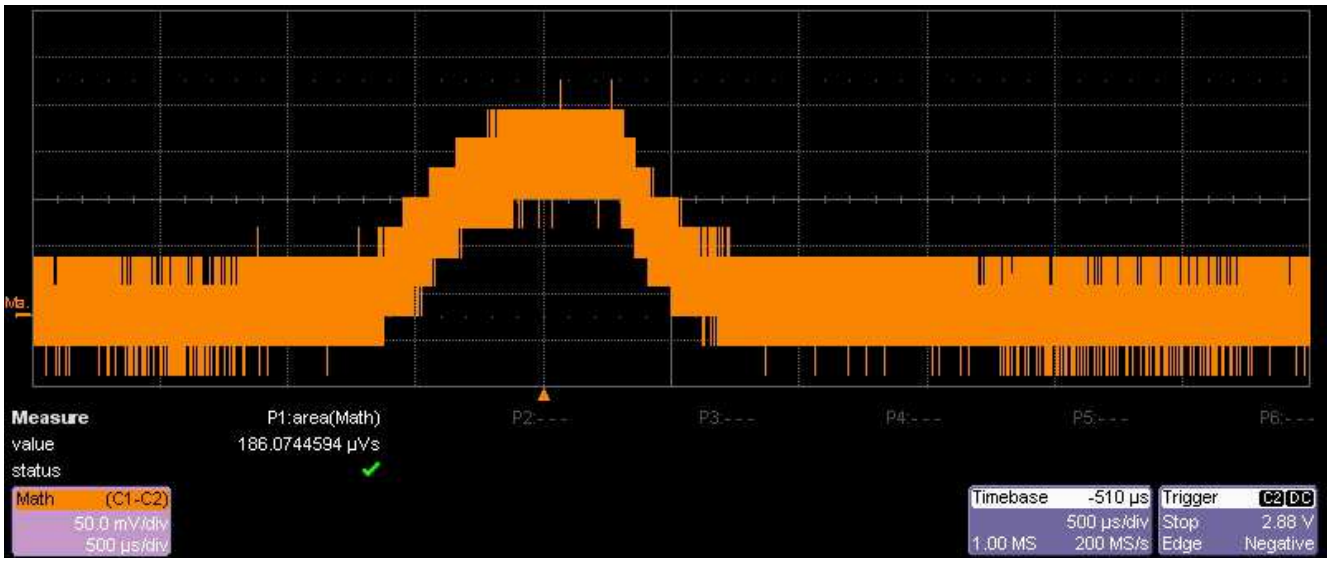
5.2. R2 Mode

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

6. Acronyms and Abbreviations

ACP	Adjacent Channel Power
AES	Advanced Encryption Standard
ALA	Application Layer Address
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
FAC	Frequent Access Cycle
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
LLA	Link Layer Address
LNA	Low Noise Amplifier
LQI	Link Quality Indication
M-Bus	Meter Bus
MHz	Mega Hertz
OMS	Open Metering System
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
VHF	Very High Frequency

7. Document History

Revision	Date	Changes
0	2011-09-08	First issue
1	2011-09-29	Added ME50-169 product