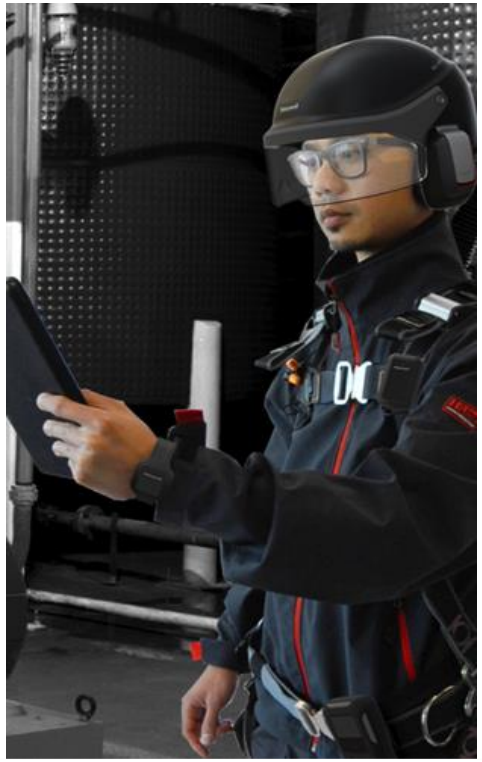
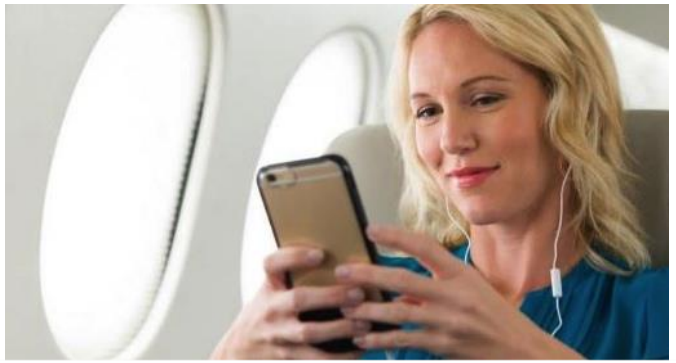
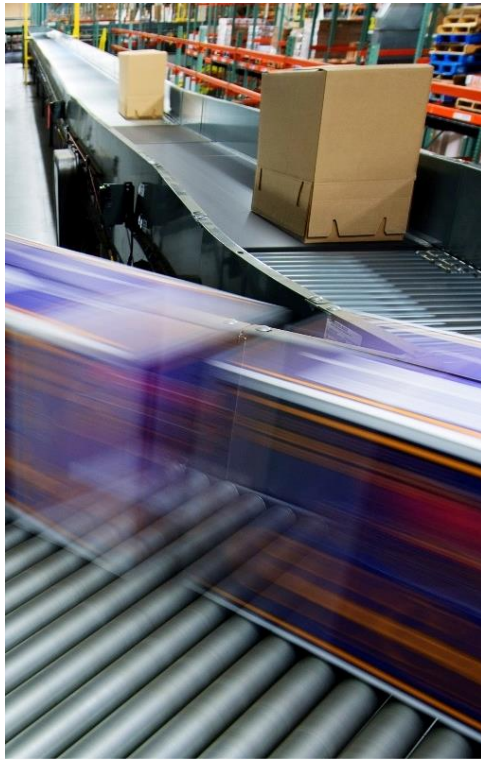


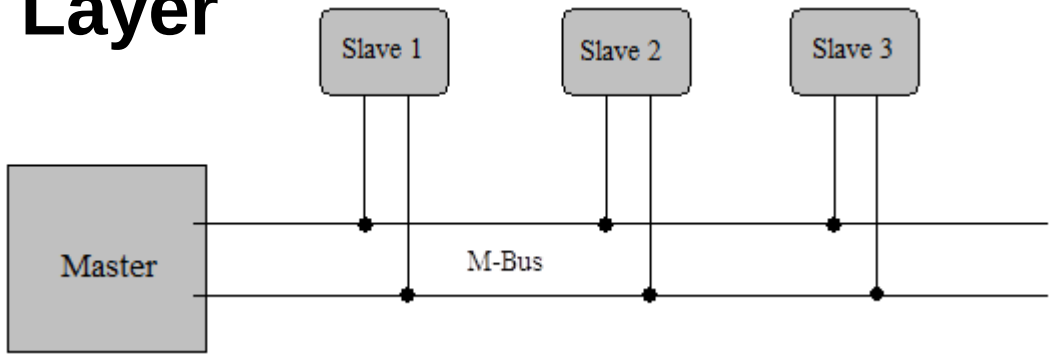
KSMWest
08.05.2018

ELECTRICITY METERING SOLUTIONS

KSMWest H1 interface

Honeywell
THE POWER OF CONNECTED

Overview M-Bus - Physical Layer



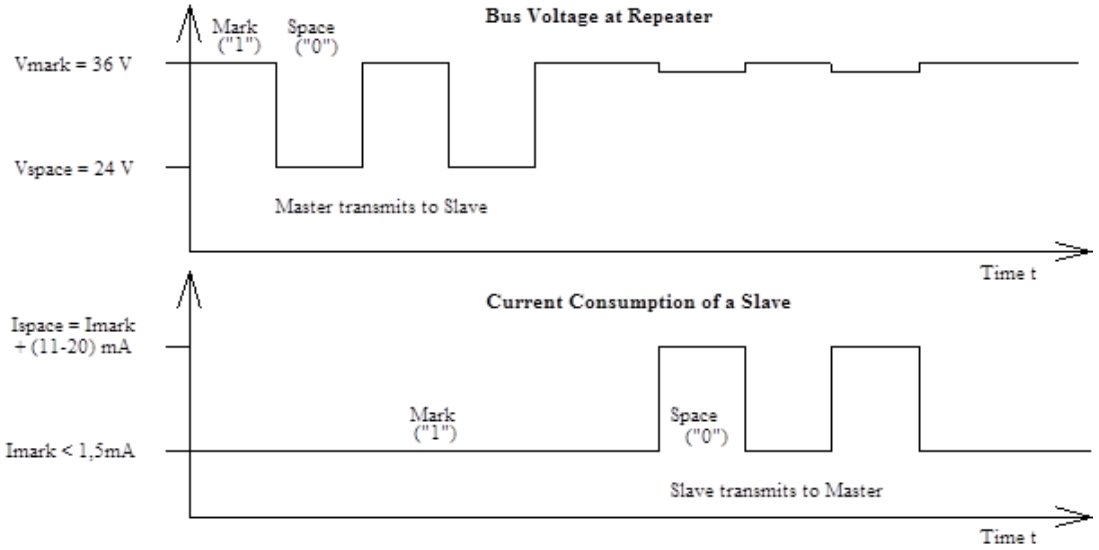
The M-Bus consists of
- The master,
- A number of slaves
- A two-wire connecting cable

Master to Slave => The transfer of bits from master to slave is accomplished by means of voltage level shifts.

- A logical "1" (Mark) corresponds to a nominal voltage of +36 V
- A logical "0" (Space) reduces the bus voltage by 12 V to a nominal +24 V

Slave to Master => The transfer of bits from slave to master slave is accomplished by means of modulating the current consumption of the slave.

- A logical "1" (Mark) is represented by a constant current of up to 1.5 mA,
- A logical "0" (Space) is represented by an increased current drain requirement by the slave of additional 11-20 mA.



Overview M-Bus - Data Link Layer

Telegram format - FT 1.2 according to IEC 870-5:

=> The format class FT 1.2 specifies three different telegram formats, which can be recognized by means of special start characters

Single Character

Single Character
E5h

Short Frame

Short Frame
Start 10h
C Field
A Field
Check Sum
Stop 16h

Control Frame

Control Frame
Start 68h
L Field = 3
L Field = 3
Start 68h
C Field
A Field
CI Field
Check Sum
Stop 16h

Long Frame

Long Frame
Start 68h
L Field
L Field
Start 68h
C Field
A Field
CI Field
User Data (0-252 Byte)
Check Sum
Stop 16h

Single Character
This format consists of a single character, namely the E5h (decimal 229), and serves to acknowledge receipt of transmissions.

Short Frame
This format with a fixed length begins with the start character 10h, and besides the C and A fields includes the check sum (this is made up from the two last mentioned characters), and the stop character 16h.

Long Frame
With the long frame, after the start character 68h, the length field (L field) is first transmitted twice, followed by the start character once again. After this, there follow the function field (C field), the address field (A field) and the control information field (CI field). The L field gives the quantity of the user data inputs plus 3 (for C,A,CI). After the user data inputs, the check sum is transmitted, which is built up over the same area as the length field, and in conclusion the stop character 16h is transmitted.

Control Frame
The control sentence conforms to the long sentence without user data, with an L field from the contents of 3. The check sum is calculated at this point from the fields C, A and CI.

Overview M-Bus - Data Link Layer

C Field (Control Field)
The control field specifies the direction of data flow, and is responsible for various additional tasks in both the calling and replying directions.

A Field (Address Field)
The address field serves to address the recipient in the calling direction, and to identify the sender of information in the receiving direction. The size of this field is one Byte, and can therefore take values from 0 to 255.

- Address 0: indicates an unconfigured slave
- Address 1-250: can be allocated to the individual slaves
- Address 251-252: reserved
- Address 253: Network Layer addressing used instead of Data Link Layer addressing
- Address 254: broadcast - all slaves reply with their own addresses
- Address 255: broadcast - none of the slaves reply

CI Field (control information field)
The control information field is already a part of the Application Layer, The control information allows the implementation of a variety of actions in the master or the slaves.

Check Sum
The Check Sum is calculated from the arithmetical sum of the data mentioned above, without taking carry digits into account.

Coding of the Control Field

Bit Number	7	6	5	4	3	2	1	0
Calling Direction	0	1	FCB	FCV	F3	F2	F1	F0
Reply Direction	0	0	ACD	DFC	F3	F2	F1	F0

Control Codes of the M-Bus Protocol (F : FCB-Bit, A : ACD-Bit, D : DFC-Bit)

Name	C Field Binary	C Field Hex.	Telegram	Description
SND_NKE	0100 0000	40	Short Frame	Initialization of Slave
SND_UD	01F1 0011	53/73	Long/Control Frame	Send User Data to Slave
REQ_UD2	01F1 1011	5B/7B	Short Frame	Request for Class 2 Data
REQ_UD1	01F1 1010	5A/7A	Short Frame	Request for Class1 Data (see 8.1: Alarm Protocol)
RSP_UD	00AD 1000	08/18/28/38	Long/Control Frame	Data Transfer from Slave to Master after Request

Overview M-Bus – Transport Layer

The M-Bus transport layer allows several application layers to co-exist over the M-Bus lower layers.
These may be:
- the M-Bus dedicated AL
- the DLMS/COSEM AL
- some other AL that may be specified in the future.

The AL used is selected by the Control Information (CI) field of the M-Bus frame.

CI field values

CI	Application
00h-1Fh	DLMS/COSEM M-Bus based TL No M-Bus Data Header is present
20h-4Fh	reserved for DLMS-based applications
50h	application reset
51h	data send (master to slave)
52h	selection of slaves
53h	reserved
54h-58h	reserved for DLMS-based applications
55h-5Bh	reserved
5Ch	synchronise action
60h	DLMS/COSEM M-Bus based TL Long M-Bus Data Header present, direction master to slave
61h	DLMS/COSEM M-Bus based TL Short M-Bus Data Header present, direction master to slave
62h-6Fh	reserved
70h	slave to master: report of application errors
71h	slave to master: report of alarms
72h	slave to master: 12 byte header followed by variable format data
73h-77h	reserved
78h	slave to master: Variable data format response without header
79h	reserved
7Ah	slave to master: 4 byte header followed by Variable data format response
7Bh	reserved
7Ch	DLMS/COSEM M-Bus based TL Long M-Bus Data Header present, direction slave to master
7Dh	DLMS/COSEM M-Bus based TL Short M-Bus Data Header present, direction slave to master
7Eh-80h	reserved
81h	Reserved for a future CEN-TC294- Radio relaying and application Layer
82h	Reserved for a future CENELEC-TC205 network/application Layer
82h-8Fh	reserved
90h-97h	manufacturer specific (obsolete)
A0h-AFh	manufacturer specific
B0-B7h	manufacturer specific
B8h	set baudrate to 300 baud
B9h	set baudrate to 600 baud
BAh	set baudrate to 1200 baud
BBh	set baudrate to 2400 baud
BCh	set baudrate to 4800 baud
BDh	set baudrate to 9600 baud
BEh	set baudrate to 19200 baud
BFh	set baudrate to 38400 baud
C0h-FFh	reserved

DLMS/COSEM M-Bus transport layer

DLMS/COSEM AL based CI values

CI_{TL}	Description
0x00-0x1F	No M-Bus Data Header is present [1]
0x60	Long M-Bus Data Header present, direction master to slave
0x61	Short M-Bus Data Header present, direction master to slave
0x7C	Long M-Bus Data Header present, direction slave to master
0x7D	Short M-Bus Data Header present, direction slave to master
[1] In this case, segmentation / reassembly is possible with restrictions.	

CI without M-Bus Data Header

b7	b6	b5	b4	b3	b2	b1	b0
0	0	0	FIN	Sequence number			

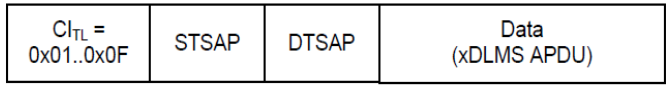
The values CITL = 0x00…0x1F indicate that no M-Bus Data Header is present. In this case, the TL can provide segmentation and reassembly

- Bit 4 (FIN) indicates that the Data field of the TPDU carries either one part of an xDLMS APDU or the complete APDU.
- Bits 3 to 0 are used for sequence numbering. The rollover of the sequence numbers is permitted, meaning that when the sequence number reaches the value 1111 and there are segments remaining to be sent, the next segment sequence number will take the value 0000.

TPDU with no M-Bus Data Header, Data without segmentation

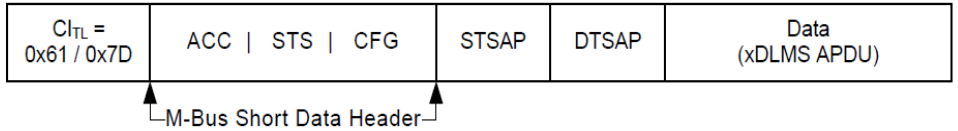
TPDU with no M-Bus Data Header, Data with segmentation, first segment

TPDU with no M-Bus Data Header, Data with segmentation, one segment

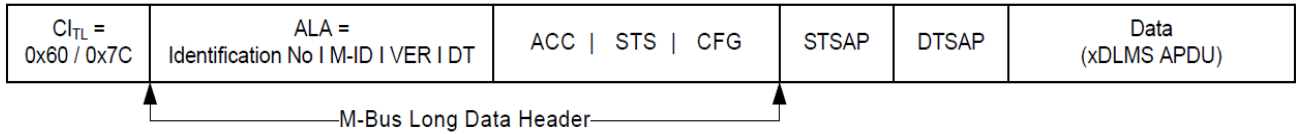


TPDU with no M-Bus Data Header, Data with segmentation, last segment

TPDU with short M-Bus Data Header, Data without segmentation



TPDU with long M-Bus Data Header, Data without segmentation



Example M-Bus frame

```
685D5D6853FF100167DB08454C5365700000014D200000541FE2A330AD29E0D68C09365BA286DBF3A7DF14B7790E14D1556AB974B2
7EC5847D11936DB5191DD0F489BA768C2DBB68F6B001E304C21FEA147E0B2E2CA1B91D574DF4F7F582CEBE928316
```

M-Bus Data link layer	Start Character	0x68	
	L field	0x5D	
	L field	0x5D	
	Start Character	0x68	
	C field	0x53	SND_UD (long frame)
	A field	0xFF	Broadcast Address
DLMS/COSEM M-Bus transport layer	CI field	0x10	TPDU with no M-Bus Data Header, Data without segmentation (Data with segmentation, last segment)
	STSAP	0x01	logical Device ID 1
	DTSAP	0x67	Client ID (CIP client id 103)
DLMS/COSEM Application Layer	Cyphering service	DB	General-Glo-Ciphering
	???	0x08	???
	System title	0x454C536570000001	
	length	0x4D	77 bytes of encrypted data
	security control byte	0x20	Bit 3…0: Security_Suite_Id Bit 4: “A” subfield: indicates that authentication is applied; Bit 5: “E” subfield: indicates that encryption is applied; Bit 6: Key_Set subfield: 0 = Unicast, 1 = Broadcast; Bit 7: Indicates the use of compression.
	frame counter	0x0000541F	
	encrypted payload	0xE2A330AD29E0D68C09365BA286DBF3A7DF1 4B7790E14D1556AB974B27EC5847D11936DB5 191DD0F489BA768C2DBB68F6B001E304C21FE A147E0B2E2CA1B91D574DF4F7F582CEBE92	unencrypted payload: 0x0F000055390C07E0090804130D1900FFC4800207090C07E 0090804130D19000000800906010001080FF060000000002 020F00161E09060100030800FF060000000002020F001620
M-Bus Data link layer	checksum	0x83	
	End character	0x16	

Example M-Bus frame

DLMS/COSEM APDU

```
general-glo-ciphering
    45 4C 53 65 70 00 00 01                          'ELSep...'
system-title: 454c536570000001
ciphered-service:
    length: 77
    security-control-byte
    security-suite-id: 0
    encryption
    key-set: unicast
    frame-counter: 144
    apdu:
    E2 A3 30 F9 B7 E0 D6 8C 09 37 5A A1 B1 F8 F3 A7          '..0......7Z.....'
    DF 14 B7 79 0E 14 D1 55 6A B8 75 B1 49 E6 84 7D          '...y...Uj.u.I..}'
    11 93 6D B5 19 1D D0 F4 89 BA 76 8C 2D BB 68 F6          '..m.......v.-.h.'
    B0 01 E3 04 C2 1F EA 14 7E 0B 2E 2C A1 B9 1D 57          '........~..,...W'
    4D F4 F7 F5 82 CE BE 92                                  'M.......'
```

DLMS/COSEM APDU (decrypted payload)

```
data-notification
long-invoke-id-and-priority
    invoke-id: 366
    not-self-descriptive
    processing-option: continue on error
    service-class: unconfirmed
    priority: normal
date-time
    07 E0 09 09 05 11 3A 00 00 FF C4 80                   '......:.....'
    2016/09/09 17:58:00
    Day of Week: 5
    Deviation to GMT: -60 minutes
    Clock Status: 80
notification-body
data
    structure with 7 elements
    struct-element-0
        octet-string:
            07 E0 09 09 05 11 3A 00 00 00 00 80           '......:.....'
    struct-element-1
        octet-string:
            01 00 01 08 00 FF                              '......'
    struct-element-2
        double-long-unsigned: 0
    struct-element-3
        structure with 2 elements
        struct-element-0
            integer: 0
        struct-element-1
            enum: 30
    struct-element-4
        octet-string:
            01 00 03 08 00 FF                              '......'
    struct-element-5
        double-long-unsigned: 0
    struct-element-6
        structure with 2 elements
        struct-element-0
            integer: 0
        struct-element-1
            enum: 32
```

Honeywell
THE POWER OF CONNECTED

Companion Standard – H1 interface

The H1 interface is specified as a wired M-Bus interface conform to EN 13757-2 with a fixed baud rate is at 2400 baud.

The physical interface is defined as RJ12 Modular Jack 6P6C connector with the following pinout!!

1 - NC
2 - NC
3 - MBUS1 (+)
4 - MBUS2 (-)
5 - NC
6 - NC

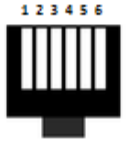


Figure 1: RJ12 connector (Tab Down) front view

The H1 interface is defined as a wired M-Bus master and must support 4 Mbus loads as a minimum (=> total of 6mA on 32V)

This interface allows only one-way communication by pushing data to an attached device. It is not allowed to receiving data via the H1 interface.

In order to support the DLMS data transfer on the wired M-Bus transport layer, please refer to chapter 10.5 in the Green Book [C].

The foreseen communication is one way only i.e. Push from Server to Client.
In this case, the data is sent using the broadcast functionality of the M-Bus.
The details are available in the following sections of the Green Book [C].

- ⇨ 10.5.3.4.2 MBUS-DATA service primitives
  Chapter 10.5.3.4.2.1 MBUS-DATA.request and 10.5.3.4.2.3 MBUS-DATA.confirm are applicable as only broadcast needs be supported.
- ⇨ 10.5.3.4.3 MBUS-DATA protocol specification
  Chapter 10.5.3.4.3.1 Sending COSEM APDUs is applicable as only broadcast needs be supported.
- ⇨ 10.5.4 Identification and addressing scheme
  - ⇨ 10.5.4.4 Link Layer Address for M-Bus broadcast
    The Link Layer Address of LLA = 0xFF is reserved for broadcast.
  - ⇨ 10.5.4.5 Transport layer address
    The Transport layer addressing is using a CI field in the range of 0x00-0x1F without M-Bus data header. In this case, the transport layer can provide segmentation and reassembly.
  - ⇨ 10.5.4.6 Application addressing extension – M-Bus wrapper
    The DLMS/COSEM AL needs to identify the partners involved in the AA: each AA is bound to a pair of client and server SAPs.
    In this case, the serverSAP = 0x01 (Management Logical Device) and the client SAP = 0x67 (Client L_SAP: 103, CIP Client)

Honeywell
THE POWER OF CONNECTED

Thank you!