KMB systems, s.r.o.
Dr. M. Horákové 559, 460 06 Liberec 7, Czech Republic
tel. +420 485 130 314, fax +420 482 736 896
email : kmb@kmb.cz, internet : www.kmb.cz

SML133 / SMY133 / SMZ133
Measuring Instruments
Communication Protocol Manual

Firmware v. 1.0.0.3030

06/2014

1. Communication Between the Device and the Host System

The SML133 / SMY133 / SMZ133 measuring instruments can be equipped either with a "local" USB communication interface or/and with "remote" communication interfaces : RS-485 or/and Ethernet.

The USB port is capable to emulate virtual serial communication to the host PC. The USB port can be used for data acquisition, configuration and status checks using the proprietary protocol KMB Long supported by the ENVIS software suite.

The remote serial communication ports support the KMB Long, the Modbus-RTU or the Modbus-TCP (TCP/IP based implementation of the Modbus RTU) protocols to provide all information to the operator's PC. Via the Ethernet port, the user gets simultaneous access to various type of data over the protocols including embedded web server with actual data and configuration.

1.1 The Modbus Protocol Description

The instruments implement a Modbus-RTU or Modbus-TCP server interface. For more details about various Modbus implementations see http://www.modbus.org/specs.php .

Instruments with the RS-485 serial line can be configured to use the Modbus-RTU protocol . For this option the address, baud rate and parity bit are specified (see the respective part of user manual for configuration details). A gap between bytes corresponding to maximum 1.5 characters (bytes) is allowed while receiving a command or transmitting a reply.

For the Ethernet line, the Modbus-TCP implementation is available. The listening port can be configured together with other TCP/IP settings (default port: 502). The instrument sends back a reply within 200 ms time frame after receiving each command. Up to three requests from different masters can be processed concurrently by each device. Between each master and the instrument the communication must follow the single request-reply. Master should wait for each reply before submitting new request.

1.1.1 Supported Functions

- 3 (0x03) ... read holding registers
- 4 (0x04) ... read input registers
- 16 (0x10) ... write multiple registers

The "broadcast" mode is not supported.

1.1.2 Modbus Quantity Encoding

Access to data structure components is provided using read/write from/to relevant registers as shown in the chart in the following subsections. Modbus protocol is based on variable mappings into 16 bit registers. Single-byte quantities are stored in such a register in the format of 0x00nn where nn is a single-byte parameter. For multibyte quantities the byte ordering is a big endian. 32-bit and 64-bit integers and floats are ordered in consequent 16-bit registers from MSB to LSB serially. Floats are encoded using the IEEE-754 float number format.

Structures which hold the instrument setting information are stored in an array of 'holding' registers, that can be written or read. The currently measured data and the instrument status can be read as the contents of the ‘input’ registers, that er read only. Each structure component is stored within the array of registers using the base addresses and a given offset.

Each value is encoded in the following way:

1. If not stated otherwise, each register is encoded in the same way as the corresponding variable in the respective message of the KMB Long protocol (Section 3).
2. Actual data values of float type (voltage, current, powers, etc.) hold the value of the respective quantity, no recalculation is needed.

ANSI C and .NET functions (sample code) for time and value conversions can be provided upon request.

1.1.3 Data Structure Register Maps

IR = input register, 16-bit, read only

HR = holding register, 16-bit, read and write

data structure	base address	type
Instrument Identification	0x200 (512 dec)	IR
Communication Setup	0x800 (2048 dec)	IR
Actual Data (General)	0x1000 (4096 dec)	IR
Electricity Meter	0x2000 (8192 dec)	IR
Installation Setup	0x700 (1792 dec)	HR

Generally, IR and HR have separated address spaces. For simplicity those are now taken together so it is possible to map the HR into the IR space and read them also as the IR with function 0x04.

1.1.4 Data Mapping in 16-bit Registers

Used formats :

int8 … 8-bit integer (signed)

uint8 … unsigned 8-bit integer

int16 … 16-bit integer (signed)

uint16 … unsigned 16-bit integer

int32 … 32-bit integer (signed)

uint32 … unsigned 32-bit integer

int64 … 64-bit integer (signed)

uint64 … unsigned 64-bit integer

float … 32-bit IEEE754-format float

Instrument Identification

IR, base address 0x200 (512 dec)

register offset (dec)	format	value
0	uint16	serial number
1	uint16	instrument type code
2	uint16	props-type code
3	uint16	firmware version
4	uint16	hardware version
5	uint16	bootloader version
6 ÷ 9	uint64	work time [sec]

Communication Setup

IR, base address 0x800 (2048 dec)

register offset (dec)	format	value
0	uint16	-
1	uint8	communication address (RS-485)
2	uint8	communication rate (RS-485) 0 = 4800 Bd 1 = 9600 Bd 2 = 19200 Bd 3 = 38400 Bd 4 = 57600 Bd 5 = 115200 Bd 6 = 230400 Bd
3	uint8	communication protocol (RS-485) 0 = communication , 8 databits 1 = communication , 9 databits, no parity 2 = communication , 9 databits, even parity 3 = communication , 9 databits, odd parity 4 = NMEA time synchronisation
4 ÷ 5	uint32	communication IP-address (Ethernet)
6	uint16	communication port (Ethernet)
7 ÷ 10	uint16	-
11 ÷ 12	uint32	communication netmask (Ethernet)
13 ÷ 14	uint32	communication gateway (Ethernet)
15	uint16	communication Modbus-port (Ethernet)
16	uint16	communication web-port (Ethernet)

Actual Data

IR, base address 0x1000 (4096 dec)

register offset (dec)	form at	value	unit
0	uint8	installation setup change counter	
1	uint1 6	error code (see instrument manual for coding)	
2	uint1 6	overflow + undeflow flags bit 0/1/2 … overflow of U1/U2/U3 bit 4/5/6 … overflow of I1/I2/I3 bit 0/1/2 … underlow of U1/U2/U3 bit 4/5/6 … underflow of I1/I2/I3	
3	uint1 6	inputs & outputs status bit 0/1 ... alarm lights A1/2 (0=off, 1=on) bit 2/3 ... digital outputs DO1/2 bit 15 … digital input DI1	
4 ÷ 5	float	f (frequency)	Hz
6 ÷ 7	-	-	
16 ÷ 17	-	-	
10 ÷ 11	float	unbu (voltage unbalance)	%
12 ÷ 13	float	unbi (current unbalance)	%
14 ÷ 15	float	φnsi (current negative sequence angle)	%
16 ÷ 17	float	U1 (phase voltage)	V
18 ÷ 19	float	U2	V
20 ÷ 21	float	U3	V
22 ÷ 23	-	-	
24 ÷ 25	float	U12 (line voltage)	V
26 ÷ 27	float	U23	V
28 ÷ 29	float	U31	V
30 ÷ 31	float	I1 (current)	A
32 ÷ 33	float	I2	A
34 ÷ 35	float	I3 (actual)	A
36 ÷ 37	-	-	
38 ÷ 39	float	P1 (active power)	W
40 ÷ 41	float	P2	W
42 ÷ 43	float	P3	W
44 ÷ 45	-	-	
46 ÷ 47	float	Pfh1 (fundamental harmonic active power)	W
48 ÷ 49	float	Pfh2	W

50 ÷ 51	float	Pfh3	W
52 ÷ 53	-	-	
54 ÷ 55	float	Q1 (reactive power)	var
56 ÷ 57	float	Q2	var
58 ÷ 59	float	Q3	var
60 ÷ 61	-	-	
62 ÷ 63	float	Qfh1 (fundamental harmonic reactive power)	var
64 ÷ 65	float	Qfh2	var
66 ÷ 67	float	Qfh3	var
68 ÷ 69	-	-	
70 ÷ 71	float	THDU1 (total harmonic distortion of voltage)	%
72 ÷ 73	float	THDU2	%
74 ÷ 75	float	THDU3	%
76 ÷ 77	-	-	
78 ÷ 79	float	THDI1 (total harmonic distortion of current)	%
80 ÷ 81	float	THDI2	%
82 ÷ 83	float	THDI3	%
84 ÷ 85	-	-	
86 ÷ 87	float	S1 (apparent power)	VA
88 ÷ 89	float	S2	VA
90 ÷ 91	float	S3	VA
92 ÷ 93	-	-	
94 ÷ 95	float	PF1 (power factor)	-
96 ÷ 97	float	PF2	-
98 ÷ 99	float	PF3	-
100 ÷ 101	-	-	
102 ÷ 103	float	D1 (distortion power)	var
104 ÷ 105	float	D2	var
106 ÷ 107	float	D3	var
108 ÷ 109	float	3cos φ (three-phase fundamental harmonic power factor)	-
110 ÷ 111	float	cos φ1 (fundamental harmonic power factor)	-
112 ÷ 113	float	cos φ2	-
114 ÷ 115	float	cos φ3	-
116 ÷ 117	-	-	
118 ÷ 119	float	3P (three-phase active power)	W
120 ÷ 121	float	3Pfh (fundamental harmonic three-phase active power)	W

122 ÷ 123	float	3Q (three-phase reactive power)	var
124 ÷ 125	float	3Qfh (fundamental harmonic three-phase reactive power)	var
126 ÷ 127	float	3S (three-phase apparent power)	VA
128 ÷ 129	float	3PF (three-phase power factor)	-
130 ÷ 131	float	3D (three-phase distortion power)	var
132 ÷ 133	float	Ufh1 (fundamental harmonic phase voltage)	V
134 ÷ 135	float	Ufh2	V
136 ÷ 137	float	Ufh3	V
138 ÷ 139	-	-	
140 ÷ 141	float	Ifh1 (fundamental harmonic phase current)	A
142 ÷ 143	float	Ifh2	A
144 ÷ 145	float	Ifh3	A
146 ÷ 147	-	-	
148 ÷ 149	float	φU1 (fundamental harmonic voltage phasor angle, abs.)	rad
150 ÷ 151	float	φU2	rad
152 ÷ 153	float	φU3	rad
154 ÷ 155	-	-	
156 ÷ 157	float	φI1 (fundamental harmonic current phasor angle, abs.)	rad
158 ÷ 159	float	φI2	rad
160 ÷ 161	float	φI3	rad
162 ÷ 175	-	-	
176 ÷ 275	float	U1h1 ÷ U50h1 (phase voltage harmonic components 1 ÷ 50)	V
276 ÷ 375	float	U1h2 ÷ U50h2	V
376 ÷ 475	float	U1h3 ÷ U50h3	V
476 ÷ 575	-	-	
576 ÷ 675	float	I1h1 ÷ I50h1 (current harmonic components 1 ÷ 50)	A
676 ÷ 775	float	I1h2 ÷ I50h2	A
776 ÷ 875	float	I1h3 ÷ I50h3	A
876 ÷ 1775	-	-	
1776 ÷ 1875	float	ΔφU1h1 ÷ ΔφU50h1 (voltage-to-current harmonic phasor relative angle 1 ÷ 50)	rad
1876 ÷ 1975	float	ΔφU1h2 ÷ ΔφU50h2	rad
1976 ÷ 2075	float	ΔφU1h3 ÷ ΔφU50h3	rad

Electricity Meter Actual Data

IR, base address 0x2000 (8192 dec)

register offset (dec)	format	value	unit
0 ÷ 1	float	AI1Σt (active energy, import, phase L1, all tariffs, total)	Wh
2 ÷ 3	float	AI2Σt (phase L2)	Wh
4 ÷ 5	float	AI3Σt (phase L3)	Wh
6 ÷ 7	float	AE1Σt (active energy, export, phase L1, all tariffs, total)	Wh
8 ÷ 9	float	AE2Σt (phase L2)	Wh
10 ÷ 11	float	AE3Σt (phase L3)	Wh
12 ÷ 13	float	AL1Σt (reactive energy, inductive, phase L1, all tariffs, total)	varh
14 ÷ 15	float	AL2Σt (phase L2)	varh
16 ÷ 17	float	AL3Σt (phase L3)	varh
18 ÷ 19	float	AC1Σt (reactive energy, capacitive, phase L1, all tariffs, total)	varh
20 ÷ 21	float	AC2Σt (phase L2)	varh
22 ÷ 23	float	AC3Σt (phase L3)	varh
24 ÷ 25	float	3AIt1 (three-phase active energy, import, tariff 1, total)	Wh
26 ÷ 27	float	3AIt2 (tariff 2)	Wh
28 ÷ 29	float	3AIt3 (tariff 3)	Wh
30 ÷ 31	float	3AEt1 (three-phase active energy, export, tariff 1, total)	Wh
32 ÷ 33	float	3AEt2 (tariff 2)	Wh
34 ÷ 35	float	3AEt3 (tariff 3)	Wh
36 ÷ 37	float	3ALt1 (three-phase reactive energy, inductive, tariff 1, total)	varh
38 ÷ 39	float	3ALt2 (tariff 2)	varh
40 ÷ 41	float	3ALt3 (tariff 3)	varh
42 ÷ 43	float	3ACt1 (three-phase reactive energy, capacitive, tariff 1, total)	varh
44 ÷ 45	float	3ACt2 (tariff 2)	varh
46 ÷ 47	float	3ACt3 (tariff 3)	varh
48 ÷ 49	float	AI1Σt_LM (active energy, import, phase L1, all tariffs, last month)	Wh
50 ÷ 51	float	AI2Σt_LM (phase L2)	Wh
52 ÷ 53	float	AI3Σt_LM (phase L3)	Wh
54 ÷ 55	float	AE1Σt_LM (active energy, export, phase L1, all tariffs, last month)	Wh
56 ÷ 57	float	AE2Σt_LM (phase L2)	Wh
58 ÷ 59	float	AE3Σt_LM (phase L3)	Wh
60 ÷ 61	float	AL1Σt_LM (reactive energy, inductive, phase L1, all tariffs, last month)	varh
62 ÷ 63	float	AL2Σt_LM (phase L2)	varh

64 ÷ 65	float	AL3Σt_LM (phase L3)	varh
66 ÷ 67	float	AC1Σt_LM (reactive energy, capacitive, phase L1, all tariffs, last month)	varh
68 ÷ 69	float	AC2Σt_LM (phase L2)	varh
70 ÷ 71	float	AC3Σt_LM (phase L3)	varh
72 ÷ 73	float	3AIt1_LM (three-phase active energy, import, tariff 1, last month)	Wh
74 ÷ 75	float	3AIt2_LM (tariff 2)	Wh
76 ÷ 77	float	3AIt3_LM (tariff 3)	Wh
78 ÷ 79	float	3AEt1_LM (three-phase active energy, export, tariff 1, last month)	Wh
80 ÷ 81	float	3AEt2_LM (tariff 2)	Wh
82 ÷ 83	float	3AEt3_LM (tariff 3)	Wh
84 ÷ 85	float	3ALt1_LM (three-phase reactive energy, inductive, tariff 1, last month)	varh
86 ÷ 87	float	3ALt2_LM (tariff 2)	varh
88 ÷ 89	float	3ALt3_LM (tariff 3)	varh
90 ÷ 91	float	3ACt1_LM (three-phase reactive energy, capacitive, tariff 1, last month)	varh
92 ÷ 93	float	3ACt2_LM (tariff 2)	varh
94 ÷ 95	float	3ACt3_LM (tariff 3)	varh
96 ÷ 99	uint64	electricity meter last readout time	sec
100 ÷ 103	uint64	electricity meter reset time	sec
104 ÷ 105	float	Pavgmax1Σt (maximum active phase power demand, phase L1, total)	W
106 ÷ 107	float	Pavgmax2Σt (phase L2)	W
108 ÷ 109	float	Pavgmax3Σt (phase L3)	W
110 ÷ 111	float	3PavgmaxΣt (three-phase)	W
112 ÷ 115	uint64	Pavgmax1Σt time	s
116 ÷ 119	uint64	Pavgmax2Σt time	s
120 ÷ 123	uint64	Pavgmax3Σt time	s
124 ÷ 127	uint64	3PavgmaxΣt time	s
128 ÷ 129	float	3Pavgmaxt1_CM (maximum active three-phase power demand, tariff 1, current month)	W
130 ÷ 131	float	3Pavgmaxt2 _CM (tariff 2)	W
132 ÷ 133	float	3Pavgmaxt3_CM (tariff 3)	W
134 ÷ 135	float	3PavgmaxΣt_CM (all tariffs)	W
136 ÷ 139	uint64	3Pavgmaxt1_CM time	s
140 ÷ 143	uint64	3Pavgmaxt2 _CM time	s
144 ÷ 147	uint64	3Pavgmaxt3_CM time	s
148 ÷ 151	uint64	3PavgmaxΣt_CM time	s
152 ÷ 153	float	3Pavgmaxt1_LM (maximum active three-phase power demand, tariff 1, last month)	W

154 ÷ 155	float	3Pavgmaxt2 _LM (tariff 2)	W
156 ÷ 157	float	3Pavgmaxt3_LM (tariff 3)	W
158 ÷ 159	float	3PavgmaxΣt_LM (all tariffs)	W
160 ÷ 163	uint64	3Pavgmaxt1_LM time	s
164 ÷ 167	uint64	3Pavgmaxt2 _LM time	s
168 ÷ 171	uint64	3Pavgmaxt3_LM time	s
172 ÷ 175	uint64	3PavgmaxΣt_LM time	s
176 ÷ 179	uint64	Pavgmax reset time	s

Installation Setup

HR, base address 0x700 (1792 dec)

register offset (dec)	format	value
0	uint16	connection mode : 0xFFFF(65535 dec) = direct connection otherwise VT-ratio (example : 350 for 35000/100 V VT)
1	uint16	-
2	uint16	CT ratio : bits 14 ÷ 0 … primary nominal current [A] bit 15 … secondary nominal current : 0 = 1 A, 1 = 5 A
3	uint16	-
4	uint8	connection type : 0 = “1-Y” 2 = “3-D” otherwise “3-Y”
5 ÷ 6	float	Unom [V] Warning : in case of indirect connection, it is the secondary voltage value ! (no VT-ratio multiplication included)
7 ÷ 8	float	Pnom [VA] Warning : measuring transformer secondary value ! (neither VT-ratio not CT-ratio multiplications included)
9	uint16	fnom [Hz]

1.1.5 Modbus Communication Examples

1.1.5.1 Reading Device Identification Example

Request: **01 04 02 00 00 06 71 B0**

01 … device address

04 ... reading input registers (IR)

02 00 ... start address (0x200=512 dec, no. of register - 1)

00 06 ... register count

71 B0 … CRC-16

Answer: **01 04 0C 00 15 11 04 00 40 0B D6 00 00 06 50 B8 DA**

01 ... device address

04 ... reading input registers (IR)

0C data byte count (0x0C=12 dec 16-bit registers)

00 15 … serial number 21

11 04 ... instrument type code

00 40 ... props-type code

0B D6 ... firmware version

00 00 ... hardware version

06 50 ... bootloader version

B8 DA CRC-16

1.1.5.2 Reading Configurable Settings Example

Request: **01 03 07 00 00 09 31 78**

Answer: **01 04 12 FF FF 00 01 A3 28 80 05 00 05 43 66 00 00 43 8E DB 6E F4 28**

1.1.5.3 Write Into (Modify) the Configurable Settings

Request: **01 10 07 00 00 09 12 FF FF FF FF 00 01 00 01 00 05 43 66 00 00 42 C8 00 00 54 11**

Answer: **01 10 07 00 00 09 33 31**

1.1.5.4 Reading Actual Data Example

Reading of “3cos” value : base address 4096 + offset 108 = 4204 (dec) = 106C (hex), 2 registers :

Request: **01 04 10 6C 00 02 B5 16**

Answer: **01 04 04 3F 77 76 3D A0 3B**

Read value 3F 77 76 3D (float) = 0.967

1.2 KMB Long Communication protocol

The communication channel uses the setting of 8 data bits, no parity, and one stop bit. The address and data flow rate can be set. The communication protocol employs the master-slave philosophy. In response to receiving a proper message or command the instrument sends back a relevant reply. All supported messages do have a uniform format (frame):

- instrument address (1 byte), values 0 and 255 are reserved
- length of message body (two bytes)
- type of message (1 byte)
- message body – varies in accordance with type of message
- 16-bit CRC

When the instrument receives a command, it sends back a relevant reply. The type-of-message byte in answer contains zero if no problem has occured. In case of error the type-of-message code is ORed with 0x80 and followed by one-byte message body containing error code value. All values are coded in the Network notation (Big Endian).

The protocol is used primarily for instruments remote control with the the ENVIS software suite. For detailed information ask manufacturer.