Modbus Communication

Protocol Specification
V1.6.0

Gesytec GmbH
Pascalstr. 6
52076 Aachen
Germany

Tel. +(49) 24 08 / 9 44-0
FAX +(49) 24 08 / 9 44-100
e-mail: info@gesytec.de
www.gesytec.com

Document: .../GesySense/UserDoc/Modbus Spezifikation GesySense/GS_Modbus-Spezifikation-v1.6.0-EN.docx
version: 1.6.0 released: June 24, 2013

Gesytec

Remarks

This document specifies the Modbus based communication protocol used between a GesySense receiver and a data server as destination of the collected data – called “master” in the following and having this position within the Modbus communication concept.

The documentation covers the Modbus communication via EIA-485 as well as via Ethernet (Modbus/TCP).

The document structure largely follows the sequence of Modbus addresses used. Chapter 1 describes elements used from of the Modbus specification. After a short overview on the address ranges chapter 2 provides information on the single addresses of each range showing a range overview followed by further descriptions of the usage and if applicable examples. Aspects of coding for some information and general information on system concepts and function can be found in chapter 3. The last chapter provides a complete list of the addresses.

Revisions

Version	Author	Modified
1.5.3	snd	Translation based on German version 1.5.2; editorial corrections and amendments
1.5.3a	snd	Corrections
1.5.4	snd	Editorial corrections and amendments
1.6.0	Hz / snd	Added information on Sensor-Actuator and Mixed-Signal modules; and for self-configuring systems

Abbreviations and Terms

Data server	Master device within the Modbus concept. The device to which the Receiver transmits measured values and additional information collected in the GesySense system. A local data server can be connected to superior external servers.
MX	Mixed-Signal modules for measuring temperatures and digital inputs.
Receiver	designates the central radio device of the GesySense system receiving messages from the GesySense wireless modules. The word “receiver” is used as a product designation as well as in its proper, functional sense.
Repeater	receiving and emitting radio device used to bridge longer distances.

Receiver/Repeater	There are some Receiver devices (no SD card, no Ethernet) which are hardware identical to repeaters. These devices are just differently used.
SAM	Sensor-Actuator module; the SAM can transmit measured values and receive control parameters.

Notations

Read/write:	Read/Write information in tables is given as seen from the slave (receiver): Output = slave is writing to this address Input = slave is reading from this address.

Reference Documents and Further Information

[1]	Modbus Application Protocol Specification V1.1b
[2]	GesySense LogIt User Manual

Contents

1 General Information

1.1 Communication Protocol

For communication between local control level and device level the Modbus protocol is used [1]. The receiving station is using the RTU mode and conformity class 0 (read and write words).

This protocol is used for both, the EIA-485 connection and the communication via Ethernet.

1.2 General Functionality

A master/slave protocol is used with an assigned master (host computer) and up to 255 slaves (devices). Within the GesySense system this corresponds to a data server as the master communicating with a GesySense receiver as the slave.

Semi-duplex communication is used, i.e. a slave connected to the master will only become active (respond) if it receives a valid message telegram. After this the master can only become active if a valid response is received from the slave queried or after a defined timeout.

1.3 Communication Settings

The following table shows possible master/slave settings in an EIA-485 communication. The first column shows the factory settings of GesySense receivers.

Parity	None	Even	Odd	None	None
Data bits	8	8	8	8	8
Stop bit	1	1	1	1	2
Transmission speed	19200	19200	19200	38 400	38400

Receivers with Ethernet connection come with the IP address 192.168.100.100. The address used in operation depends on the installation.

1.4 General Structure

N° of Bytes	Meaning	Comment
1	slave address (0…255)	0: broadcast
1	function code	cf. 1.5
N	Data	dependent on command
1	CRC16 low byte	error check cf. 1.6
1	CRC16 high byte	error check cf. 1.6

1.5 Function Codes

Code	Meaning	Comment
2 (0x02)	read discrete inputs	Alarm states
3(0x03)	read holding registers	Reading of values and parameters (16-bit words)
5(0x05)	write single coil	Start action (e.g. reset) (single bit)
16(0x10)	write multiple regis-ters	Writing of values and parameters (16-bit words)
20 (0x14)	read file record	File transfer
21(0x15)	write file record	Download firmware update

1.6 Error Check

The error check is according to the Modbus specification [1] 16 bit CRC.

1.7 Request for Sensor Values (Function code 3)

Example for read process:

Modbus master query:

Byte N°	Meaning
1	slave address (1…255)
2	function code 3
3	word address (high byte)
4	word address (low byte)
5	number of words (high byte)
6	number of words (low byte)
7	CRC 16 (low byte)
8	CRC 16 (high byte)

Slave response:

Byte N°	Meaning
1	Slave address (1…255)
2	function code 3
3	N° of bytes (n)
4	data (n/2 word)
4+1	data+1
…	
4+n	CRC 16 (low byte)
5+n	CRC 16 (high byte)

If the word address does not exist or the number of words requested is too large the slave will return the respective error code according to the Modbus specification [1].

1.8 Write Start Time (Function code 16)

Example for write process:

Modbus master query:

Byte N°	Meaning
1	slave address (0…255)
2	function code 16
3	word address (high byte)
4	word address (low byte)
5	number of words (high byte)
6	number of words (low byte)
7	N° of bytes (n)
8	word data (n/2 word)
…	high byte first
8+n	CRC 16 (low byte)
9+n	CRC 16 (high byte)

Slave response:

Byte N°	Meaning
1	slave address (1…255)
2	function code 16
3	word address (high byte)
4	word address (low byte)
5	number of words (high byte)
6	number of words (low byte)
7	CRC 16 (low byte)
8	CRC 16 (high byte)

If the word address does not exist or the number of words requested is too large or the data content is not acceptable the slave will return the respective error code according to the Modbus specification [1].

2 Address Assignment

Grouped according to the usage of the address ranges this chapter describes the assignment of Modbus addresses in the GesySense system. It starts with an overview on address ranges and their usage.

2.1 Address Ranges

Address	Comment
0 – 65	monitoring wireless sensor system
70 – 78	control and status register for repeater firmware update, p.12
79 – 86	parameterizing and control functions of receivers, p 14
100 – 196	data transmission from wireless modules unknown to master, p. 17
200 – 999	data transmission from temperature modules known to master , p. 18
1000 – 1033	configuration data storage for up to 7 repeaters, p. 20
1500 – 1534	data of receivers/repeaters unknown to master, p. 21
1600 – 1999	parameter definition for counters of SAM and MX modules, p. 22
2000 – 2298	data transmission from digital status modules known to the master; 1 value for 2 objects for each module; sufficient for 30 status sensors, p. 24
2300 – 2629	data transmission from digital counter modules known to master; 2 * 2 values per module (32 bit counter); sufficient for 30 counter modules, p25
2700 – 2997	data transmission from analog modules known to master: 0 – 10 V or 4 – 20 mA; sufficient for 30 analog modules, p. 27
3000 – 4999	data transmission from Mixed Signal and Sensor- Actuator modules, p. 28
5000 –	communication between Sensor-Actuator modules and receiver, p. 32
10000 – 10299	unit identifier reference table for Mixed Signal and Sensor-Actuator modules, p. 35

2.2 Monitoring of Wireless Sensor System

The address range 0 – 65 holds information on all infrastructural wireless network components installed, i.e. on the repeaters and the receiver. All entries are made in an individual range assigned to each device by its system internal number. Usually only the data of the (maximally 7) repeaters known to the master are stored there. Known repeaters are defined to be those with configuration data stored in this address range 1000 – 1033. If an unknown repeater is active in the network its data is stored in the 1500 –1533 address range.

Address	Read/write	Comment
0 – 1	output	serial number receiver
2	output	start date receiver (cf. chapter 3.1.1)
3	output	firmware version receiver
4	output	hardware version receiver
5	output	error status receiver
6 – 7	input	system time + date receiver (can be modified by master)
8	output	number of received modules
9	output	number of received repeaters
10 – 11	output	serial number repeater 1
12	output	start date repeater 1
13	output	firmware version repeater 1
14	output	hardware version repeater 1
15	output	transmission strength repeater 1
16	output	error status repeater 1
17	output	number of modules directly received by repeater 1 within the last 30 min.
18 – 19	output	serial number repeater 2
20	output	start date repeater 2
21	output	firmware version repeater 2
22	output	hardware version repeater 2
23	output	transmission strength repeater 2
24	output	error status repeater 2
25	output	number of modules directly received by repeater 2 within the last 30 min.
...		...
58 – 59	output	serial number repeater 7
60	output	start date repeater 7
61	output	firmware version repeater 7
62	output	hardware version repeater 7
63	output	transmission strength repeater 7
64	output	error status repeater 7
65	output	number of modules directly received by repeater 7 within the last 30 min.

Representation of Values

Address	Value	Comment
0	5232	serial number receiver (cf. chapter 3.3): serial number: 8.000.005.232
1	32768	
2	4356	start date receiver (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000);); i.e. 04.08.2008
3	1	firmware version of receiver: value / 100; i.e. 0.01
4	17	hardware version of receiver: value / 100; i.e. 0.17
5		receiver error code
6	32600	system time receiver (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 18:06:40
7	4367	current date (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 15.08.2008
8	24	number of received modules: 24
9	2	number of received repeaters: 2
10	1234	serial number repeater 1 (cf. chapter 3.3): serial number: 2000001234
11	32768	
12	4356	start date repeater 1 (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000);); i.e. 04.08.2008
13	10	firmware version repeater: value/ 100; i.e. 0.10
14	11	hardware version repeater: value/ 100; i.e. 0.11
15	95	transmission strength repeater 1: 95%
16		error code repeater 1
17	20	number of modules directly received by repeater 1 during the last 30 min: 20
…		
cont. to 65		8 addresses for each of max 7 repeaters

2.3 Firmware Update of Repeaters and Receivers without Ethernet

The address range 70 – 78 is dedicated to the firmware update of Repeaters.

Address	Type	Comment
70	input	start firmware download
71	output	download status
72	input	manual start of firmware update for repeater 1
73	input	manual start of firmware update for repeater 2
...		...
78	input	manual start of firmware update for repeater 7
79	input	backup control

Firmware Update Process

Address	Value	Comment
70	1	start download; set by master device and reset by receiver
71	1 to 16	status and result of download
72	1	the master device issues a command to the receiver to update firmware of repeater 1; the result can be read from error code address of repeater 1 (Modbus address 16); after termination of download this address is set to 0 by the receiver
73 – 78	1	analog for repeaters 2 to 7

The process is monitored by status register with Modbus address 71. A “1” is written to Modbus address 70 after a successful download. This will trigger a reset of the receiver and the downloaded firmware is written from the temporary serial memory to the permanent memory. Modbus address 70 is set back to “0” by the receiver afterwards.

In a next step the receiver distributes the new firmware to all registered repeaters. The result is reflected in the monitoring addresses of each repeater: firmware version number and error code. An update is only executed if the version in the receiver is higher than that in the repeater.

With an entry in the addresses 72 – 78 the master can re-initiate at any time a download of the firmware existing in the receiver to each of the 7 repeaters. The result is stored at the respective repeater’s error code address. Further information on repeater updates is provided in chapter 3.5.

Routing of Updates

During distribution of a new firmware to the repeaters it may occur that, depending on the installation situation, the firmware cannot be sent directly to every repeater, but only via one or even more intermediate repeaters. The routing to the single repeaters the receiver will take from the route information contained in the respective addresses in Modbus address range1000 – 1036. The routing address contains the repeater number of the repeater over which the update has to be sent.

Example: Repeater 5 can only be reached via Repeater 3 and Repeater 4. For messages from Repeater 5 the user observed, a better strength at Repeater 4 than at Repeater 3. Therefore a "4" should be set in the routing address of Repeater5.

2.4 Parameterizing and Control Functions of the Receiver

The address range 79 – 86 holds data configuring for the control function of receivers

Address	Type	Comment
79	input	interval for the cyclic storing of the configuration
80	input	method and interval for the automatic read-out of archives from modules with receiver
81	input	automatic registration of active wireless modules
82	input	interval of activity for receivers using a battery
83	input	time period for reading out archived data from modules, if no data exists in the receiver
84	input	switch relay of Receiver \LAN
85	Input	start firmware update of Sensor-Actuator modules
86	Input	repetitions of an SAM firmware update

Representation of Values

Address	Value	Comment
79	961	Save configuration every 60 minutes (0x3c1) time 60, condition 1
80	4323	The archive is read out at 00:00 and 04:30 (0x10e3) condition 3, time 270 minutes
81	1	modules are to be registered automatically

82	22588 or e.g. 22888	turn on every 60 minutes for 5 minutes (0x583c) duration 5, 1 = turn on cyclically, interval 60 min. or turn on every 6 hours for 5 minutes (0x5968) duration 5, 1 = turn on cyclically, interval 360
83	24	read out data, starting from 1 day before current time
84	1	the relay of Receiver \LAN is set. "0" will set it back
85	1	distribute SAM firmware update
86	5	repeat SAM firmware update 5 times

Modbus address 79 holds the settings for saving an dynamically generated configuration. Next to the save/don't save information the interval in minutes is set, in which the configuration data (from automatically registered modules) is cyclically stored. This configuration will then be available even after a restart of the receiver.

Format:	0xbbba
a:	0 / 1 / 2 = don't save / save / delete configuration
bbb	time interval in minutes for saving the configuration

Modbus address 80 controls the reading out of archives from Sensor-Actuator modules. Different options are available. The settings apply to all these modules in the system.

Format:	0xbbba
a	condition for readout: 0: don't read out automatically 1: if DI1 is switched from 0 to 1 and at least the time bbb has elapsed since last time stamp; 2: if after ≥ bbb minutes without message a new radio message is received; 3: regularly at bbb minutes after 00:00 o'clock; 4: cyclically at the interval bbb set (should be ≥ 3 hours, i.e. ≥180)
bbb	time in minutes from 60 to 1440 (hex: 3c – 5A0)

Modbus address 81 controls the registration of models in the receiver. If automatic registration is active, the receiver will assign the modules to its register structure according to the information received. The module type is used as basis for assigning modules to certain address rages. Further information to these dynamic systems is provided in chapter 3.6

Modbus address 82 controls the on-time of battery power receivers. Further to the runtime from 1 to 15 minutes the turn on time can be set and if this shall happen repeatedly. A switch on time of "0" means "always on"

Format: 0xcb(a)aa
c: on time (1– 15 min.);
b(a): -> xyyy
x = 0 no repetition;
= 1 repetition;
yyy together with aa a time interval in minutes from 0 to 1440 = 24 h can be represented
(a)aa: switch on interval

Bit	Coding	Value (hex)	Comment
0	aa	0 – 5A0	switch-on time minutes (0 to 1440) from midnight, or since last on-time; 0 = always on
1			
2			
3			
4			
5			
6			
7			
8	y		used additionally to specify switch-on time
9	y		
10	y		
11	x	0 / 1	repeat switching on yes / no
12	c	Wert (hex)	On-time duration in minutes restarts, if a module transmits its archive during the period
13			
14			
15			

Modbus address 83 sets the backward period of time in hours for which data has to be read out from the module archive if no measuring data at all is available from this module in the receiver. Default value is 0, which is interpreted as 24 hours.

Modbus address 84 allows the user to switch the relay available on “Receiver \LAN”.

Modbus addresses 85 and 86 control the firmware update procedure for Sensor-Actuator modules via radio.

2.5 Data Transmission from Unregistered Modules

The address range 100 – 196 holds data about wireless modules (temperature, digital, …) for which the master cannot assign the serial number to a data point (serial number was not written to an address range for registered modules 200 – 997 or 2000 – 4999). Thus, all types of modules can be found here. The sequence of modules is accidental. If more than 10 unknown modules exist on a site, the last 10 detected can be found here.

Address	Type	Comment
100 – 101	output	serial number module 1
102	Output	signal quality (=strength)
103	output	transmission quality
104	output	battery status
105	output	measuring time
106	output	measured value
110 – 111	output	serial number module 2
112	output	signal quality (=strength)
113	output	transmission quality
114	output	battery status
115	output	measuring time
116	output	measured value
...		...
190 – 191	output	serial number module 10
192	output	signal quality (=strength)
193	output	transmission quality
194	output	battery status
195	output	measuring time
196	output	measured value

Representation of Values

Address	Value	Comment
100	57920	serial number module 1 (cf. chapter 3.3): serial number: 0.000.123.456
101	1	
102	98	signal quality (=strength): 98%
103	99	transmission quality: 99%
104	87	battery status: 87%

105	25620	measuring time (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 14:14:00
106	1230	measured value of a temperature module (cf. chapter 3.1.3): value / 100; i.e. 12.30
110	57919	serial number of module 2 (cf. chapter 3.3): serial number: 123455
111	1	
112	98	signal quality (=strength) : 98%
113	99	transmission quality: 99%
114	87	battery status: 87%
115	25622	measuring time (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 14:14:00
116	63485	measured value of a temperature module (cf. chapter 3.1.3): value / 100; i.e. -20.50
120	3	serial number of module 3 (cf. chapter 3.3): serial number: 1.000.000.003
121	4096	
122	98	signal quality (=strength) : 98%
123	99	transmission quality: 99%
124	87	battery status: 87%
125	25620	measuring time (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 14:14:00
126	0	measured value of status sensor (cf. chapter 3.1.6): input 1: open, input 2: open

2.6 Data Transmission from Registered Temperature Modules

The address range 200 – 997 holds data from all wireless temperature sensors for which the master has an assignment between serial number and data point. The data point “serial number” and “start date” are written to the Modbus based on the internal assignment table (cf. chapter 3.4.1) of the master device.

Address	**Type**	**Comment**
200 – 201	input	serial number temperature module 1
202	output	signal quality (=strength)
203	output	transmission quality
204	output	battery status
205	output	measuring time
206	output	measured value

207	input	start date
208	input	lower limit value for temperature
209	input	upper limit value for temperature
210 - 211	input	serial number temperature module 2
212	output	signal quality (=strength)
213	output	transmission quality
214	output	battery status
215	output	measuring time
216	output	measured value
217	input	start date
218 - 219	input	Lower and upper temperature limit values
990 – 991	input	serial number temperature module 80
992	output	signal quality (=strength)
993	output	transmission quality
994	output	battery status
995	output	measuring time
996	output	measured value
997	input	start date
998 – 999	input	Lower and upper temperature limit values

Representation of Values

Address	**Value**	**Comment**
200	26848	serial number module 1 (cf. chapter 3.3): serial number: 0.000.223.456
201	3	
202	98	signal quality (=strength): 98%
203	99	transmission quality: 99%
204	87	battery status: 87%
205	25620	measuring time (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 14:14:00
206	2230	measured value (cf. chapter 3.1.3): value / 100; i.e. 22.30
207	4356	start date (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 04.08.2008
208	1800	lower temperature limit 18 degree
209	2400	upper temperature limit 24 degree

210	26847	serial number module 2 (cf. chapter 3.3): serial number: 223.455
211	3	
212	98	signal quality (=strength): 98%
213	99	transmission quality: 99%
214	87	battery status: 87%
215	35622	measuring time (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 19:47:24
216	63605	measured value (cf. chapter 3.1.3): value / 100; i.e. -19.30
217	4356	start date (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 04.08.2008
218	63035	lower temperature limit -25 degree
219	2500	upper temperature limit 25 degree

2.7 Configuration Data for Repeaters

The configuration data for the repeaters are transmitted to the master during system commissioning. These are held at Modbus addresses 1000 – 1033. If these entries are modified in the master device, the modifications are automatically – without restating the master– transmitted to the respective Modbus addresses. The receiver will then re-configure the repeaters. Neither reset nor disconnect are necessary.

Address	**Type**	**Comment**
1000 – 1001	input	serial number repeater 1
1002	input	repeater 1: number within the system
1003	input	route repeater 1
1005– 1006	input	serial number repeater 2
1007	input	repeater 2: number within the system
1008	input	route repeater 2
…		...
1030 - 1031	input	serial number repeater 7
1032	input	repeater 7: number within the system
1033	input	route repeater 7

Representation of Values

Address	Value	Comment
1000	25	serial number repeater 1 (cf. chapter 3.3): serial number: 8.000.000.025
1001	32768	
1002	1	repeater 1: number within the system: 1
1003	0	route repeater 1: 0, direct communication
1004	4356	start date repeater 1 (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 04.08.2008
1005	120	serial number repeater 2 (cf. chapter3.3): serial number: 8.000.000.120
1006	32768	
1007	2	repeater 2: number within the system: 2
1008	1	route firmware update via repeater 1
1009	4356	start date repeater 2 (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 04.08.2008

2.8 Data Transmission from Unregistered Repeaters

The receiver writes serial number and the start date from repeaters unknown to the master to the address range 1500 – 1534. This refers to repeaters which are not found in the address range 1000 – 1033.

Address	Type	Comment
1500 - 1501	output	serial number unknown repeater 1
1502	output	repeater number of unknown repeater 1
1503	output	start date unknown repeater 1
1504	output	error code at configuration of repeater 1
1505 - 1506	output	serial number unknown repeater 2
1507	output	repeater number of unknown repeater 2
1508	output	start date unknown repeater 2
1509	output	error code at configuration of repeater 2
…		...
1530 - 1531	output	serial number unknown repeater 7
1532	output	repeater number of unknown repeater 7
1533	output	start date unknown repeater 7
1534	output	error code at configuration of repeater 7

Representation of Values

Address	Value	Comment
1500	29	serial number repeater 1 (cf. chapter 3.3): serial number: 8.000.000.029
1501	32768	
1502	0	repeater N°: 0
1503	4356	start date of repeater (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 04.08.2008
1504	0	error code from parameterization: 0
1505	123	serial number repeater 2 (cf. chapter 3.3): serial number: 8.000.000.123
1506	32768	
1507	2	repeater N°: 2
1508	4356	start date of repeater (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 04.08.2008
1509	1	error code from parameterization: 1

2.9 Parameter Definitions for Counters of Mixed Signal and Sensor-Actuator Modules

The address range 1600 –1999 holds definition data for the parameterization of counters of type 5 and type 6 modules as interval counters.

Address	Type	Comment
1600 – 1601	input	serial number module 1, (type 5 or 6)
1602	input	time interval for counters 1 and 2
1603	Input	dimension unit and pulse valence for counter 1 and 2
1604 – 1605	input	serial number module 2
1606	input	time interval for counter 1 and 2
1607	input	dimension unit and pulse valence for counter 1 and 2
1608 – 1609	input	serial number module 3
1610	input	time interval for counter 1 and 2
1611	input	dimension unit and pulse valence for counter 1 and 2
etc. to 1999		*corresponding to 100 modules*

Representation of Values

Address	Value	Comment
1600	100	serial number (cf. chapter 3.3): serial number: 6.000.000.100
1601	24576	
1602	69	time interval: counter 1: 60 min, counter 2: 360 min 0x45 ⇔ ab (cf. chapter 2.9.1.1)
1603	17686	dimension: counter 1: Liter, counter 2: cbm pulse valence: counter 1: 1, counter 2: 1.000 0x4516 ⇔ abcd

2.9.1.1 Coding of Parameters for Counters of SAM and MX Modules

The counters of Mixed-Signal and Sensor-Actuator modules can be assigned a time interval, pulse valence and measurement unit in order to use them as interval counters. This information is store in two addresses as follows:

1602	ab (Hex)	a: time interval counter 1, b: time interval counter 2
1603	abcd (Hex)	a: measurement unit counter 1, b: measurement unit counter 2, c: pulse valence counter 1, d: pulse valence counter 2

a, b, c and d represent ciphers from 1 to 7. The parameter is the hexadecimal value of the sequence of ciphers.

The following table shows the meaning of the ciphers dependent of their position:

Cipher a, b, c or d	Time interval	Measurement unit	Pulse valence
1	5 min.	W	1
2	15 min.	kW	10
3	30 min.	MW	20
4	60 min. = 1 h	Liter	50
5	360 min. = 6 h	cbm	100
6	720 min. = 12 h		1.000
7	1440 min. = 24 h		10.000

Time interval: time span to realize the pulse counter

Measurement unit: unit, to be connected with the measured pulses.

Pulse valence: factor by which the counted pulses are multiplied.

2.10 Data Transmission from Registered Status Modules

The address range 2000 – 2298 holds data from all wireless digital status modules for which the master has an assignment between serial number and data point. The data point “serial number” and “start date” are written to the Modbus based on the internal assignment table (cf. chapter 3.4.1) of the master device.

Address	Type	Comment
2000 –2001	input	serial number module 1
2002	output	signal quality (=strength)
2003	output	transmission quality
2004	output	battery status
2005	output	measuring time
2006	output	status of digital inputs 1 and 2
2008	input	start date
2010 – 2011	input	serial number module 2
2012	output	signal quality (=strength)
2013	output	transmission quality
2014	output	battery status
2015	output	measuring time
2016	output	status of digital inputs 1 and 2
2018	input	start date
…		...
2290 – 2291	input	serial number module 30
2293	output	signal quality (=strength)
2294	output	transmission quality
2295	output	battery status
2296	output	measuring time
2297	output	status of digital inputs 1 and 2
2298	input	start date

Representation of Values

Address	Value	Comment
2000	100	serial number module 1 (cf. chapter 3.3): serial number: 1.000.000.100
2001	4096	
2002	98	signal quality (=strength): 98%

2003	99	transmission quality: 99%
2004	87	battery status: 87%
2005	25620	measuring time (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 14:14:00
2006	0	measured value of status module (cf. chapter 3.1.6): input 1 open and input 2 open
2008	4356	start date (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 04.08.2008
2010	331107	serial number module 2 (cf. chapter3.3): serial number: 1.000.360.787
2011	4101	
2012	98	signal quality (=strength): 98%
2013	99	transmission quality: 99%
2014	87	battery status: 87%
2015	25622	measuring time (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 14:14:04
2016	1	measured value of status module (cf. chapter 3.1.6): input 1 closed and input 2 open
2018	4356	start date (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 04.08.2008

2.11 Data Transmission from Registered Counter Modules

This address range 2300 – 2629 holds data from all wireless counter modules for which the master has an assignment between serial number and data point. The data points “serial number” and “start date” are written to the Modbus based on the internal assignment table (cf. chapter 3.4.1) of the master device.

Counter values are 32 bit values with the lower word at first and upper word at the second address.

Address	**Type**	**Comment**
2300 – 2301	input	serial number module 1
2302	output	signal quality (=strength)
2303	output	transmission quality
2304	output	battery status
2305	output	measuring time
2306 – 2307	output	lower word (32 bit counter)
2308 – 2309	output	upper word (32 bit counter)
2310	input	start date

2311 –2312	input	serial number module 2
2313	output	signal quality (=strength)
2314	output	transmission quality
2315	output	battery status
2316	output	measuring time
2317 – 2318	output	lower word (32 bit counter)
2319 – 2320	output	upper word (32 bit counter)
2321	input	start date
..		
2619 – 2620	input	serial number module 30
26213	output	signal quality (=strength)
2622	output	transmission quality
2623	output	battery status
2624	output	measuring time
2625 – 22626	output	lower word (32 bit counter)
22627 – 2628	output	upper word (32 bit counter)
2629	input	start date

Representation of Values

Address	**Value**	**Comment**
2300	1000	serial number module 1 (cf. chapter 3.3): serial number: 3.000.001.000
2301	8192	
2302	98	signal quality (=strength): 98%
2303	99	transmission quality: 99%
2304	87	battery status: 87%
2305	25620	measuring time (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 14:14:00
2306	10	value of counter 1: 10
2307	0	
2308	122	value of counter 2:122 + 65535 = 65657
2309	1	
2310	4356	start date (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 04.08.2008
2311	1010	serial number module 2 (cf. chapter 3.3): serial number: 3.000.001.010
2312	8192	
2313	98	signal quality (=strength): 98%

2314	99	transmission quality: 99%
2315	87	battery status: 87%
2316	25620	measuring time (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 14:14:00
2317	10	value of counter 1: 10
2318	0	
2319	144	value of counter 2: 144 + 65535 = 65679
2320	1	
2321	4356	start date (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 04.08.2008

2.12 Data Transmission from Registered Analog Modules

The address range 2700 – 2997 holds data from all wireless analog modules for which the master has an assignment between serial number and data point. The data points “serial number” and “start date” are written to the Modbus based on the internal assignment table (cf. chapter 3.4.1) of the master device.

Address	**Type**	**Comment**
2700 – 2701	input	serial number module 1
2702	output	signal quality (=strength)
2703	output	transmission quality
2704	output	battery status
2705	output	measuring time
2706	output	measured value
2707	input	start date
2710 – 2711	input	serial number module 2
2712	output	signal quality (=strength)
2713	output	transmission quality
2714	output	battery status
2715	output	measuring time
2716	output	measured value
2717	input	start date
…		...
2990 – 2991	input	serial number module 30
2992	output	signal quality (=strength)

2993	output	transmission quality
2994	output	battery status
2995	output	measuring time
2996	output	measured value
2997	input	start date

Representation of Values

Address	Value	Comment
2700	888	serial number module 1 (cf. chapter 3.3): serial number 4.000.000.888
2701	12288	
2702	98	signal quality (=strength) : 98%
2703	99	transmission quality: 99%
2704	87	battery status: 87%
2705	25620	measuring time (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 14:14:00
2706	2230	measured value analog input: 2230 for interpretation cf. chapter 3.1.4
2707	4356	start date (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 04.08.2008
2710	5778	serial number module 2 (cf. chapter 3.3): serial number 4.000. 136.850
2711	12290	
2712	97	signal quality (=strength): 97%
2713	96	transmission quality: 96%
2714	87	battery status: 87%
2715	35622	measuring time (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 19:47:24
2716	1250	measured value analog input: 1250, for interpretation cf. chapter 3.1.4
2717	4356	start date (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 04.08.2008

2.13 Data Transmission from Registered Mixed-Signal and Sensor-Actuator Modules

The address range 3000 – 4999 holds data from all wireless Sensor-Actuator and Mixed-Signal modules (module types 5 and 6) for which the master has an assignment between serial number and data point. The data points “serial number”

and “start date” are written to the Modbus based on the internal assignment table (cf. chapter 3.4.1) of the master device.

Sensor-Actuator modules are additionally fitted with a receiver enabling bi-directional communication between module and the receiver of the wireless network.

Address	**Type**	**Comment**
3000 – 3001	input	serial number module 1
3002	input	start date
3003	input	Module configuration
3004	output	signal quality (=strength)
3005	output	transmission quality
3006	output	battery status
3007	output	measuring time
3008	output	temperature value 1 of module, (ambient temp. if measured, first PT100 probe otherwise)
3009	output	temperature value 2
3010 – 3011	output	counter 1 (32 bit counter)
3012 – 3013	output	counter 2 (32 bit counter)
3014	output	Status of digital inputs 1 and 2
3015	output	interval counter 1 (16 bit counter)
3016	output	interval counter 2 (16 bit counter)
3017	output	not used
3018	output	not used
3019	input	ate of last archive read-out
3020 – 3021	input	serial number module 2
3022	input	start date
3023	input	Module configuration
3024	output	signal quality (=strength)
3025	output	transmission quality
3026	output	battery status
3027	output	measuring time
3028	output	temperature value 1 of module, (ambient temp. if measured, first PT100 probe otherwise)
3029	output	temperature value 2
3030 – 3031	output	counter 1 (32 bit counter)
3032 – 3033	output	counter 2 (32 bit counter)
3034	output	Status of digital inputs 1 and 2

3035	output	interval counter 1 (16 bit counter)
3036	output	interval counter 2 (16 bit counter)
3037	output	not used
3038	output	not used
3039	output	Date of last archive read-out
…		…
4980 – 4981	input	serial number module 2
4982	input	start date
4983	input	Module configuration
4984	output	signal quality (=strength)
4985	output	transmission quality
4986	output	battery status
4987	output	measuring time
4988	output	temperature value 1 of module, (ambient temp. if measured, first PT100 probe otherwise)
4989	output	temperature value 2
4990 – 4991	output	counter 1 (32 bit counter)
4992 – 4993	output	counter 2 (32 bit counter)
4994	output	Status of digital inputs 1 and 2
4995	output	interval counter 1 (16 bit counter)
4996	output	interval counter 2 (16 bit counter)
4997	output	not used
4998	output	not used
4999	output	Date of last archive read-out

Module configuration
Depending on module type and configuration temperatures and/or digital pulses can be collected. Pulse values are recorded as 32-bit values in the receiver.

The module configuration of SAM and MX modules is sent to the receiver in intervals and store there. The configuration code contains the information which features of the module can be used. This is a simple number evaluated by the application to process data correctly.

Interval counters:
The receiver in the wireless network can implement an interval counter by calculating the pulses per time interval from the transmitted values. In the definition section of Modbus addresses 1600 – 1999 the corresponding definitions can be made. For the modules to be used as interval counters time interval, pulse valence, and unit of measurement can be set there. (Parameterization is done with

an installation tool, such as e.g. GesySense LogIt.) The receiver will record the calculated values at the corresponding addresses.

Date of last archive read-out:
The register contains the date and time until which the local archive of the module has already been read out. Representation is based on a bit sequence (abc) built from month (aaaa) day (bbbbb) and time of the day in quarters of an hours (ccccccc).

Representation of Values

Address	Value	Comment
3000	888	serial number module 1 (cf. chapter 3.3): serial number 6.000.000.888
3001	24576	
3002	5966	start date (cf. chapter 3.1.1): dd+mm*32+512*(yyyy-2000); i.e. 14.10.2011
3003	42050	Module configuration: 0xa442 MX with internal temperat., PT 1000, 1 status 0x8951: MX with internal temperat., 2 status, logger 0x9482: MX with internal temperat., PT 1000 and 1 counter
3004	98	signal quality (=strength) : 98%
3005	99	transmission quality: 99%
3006	87	battery status: 87%
3007	25620	measuring time (cf. chapter 3.1.2): seconds from 0:00 / 2; i.e. 14:14:00
3008	2230	measured value of 1st temperature sensor: (cf. chapter 3.1.3): value /100 i.e.: 22.30 °C
3009	1250	measured value of 2nd temperature sensor: (cf. chapter 3.1.3): 12.50°C
3010	10	counter 1 = 10
3011	0	
3012	430	counter 2, counter 2 = 430 + 2*65535 = 131500
3013	2	
3014	1	status of digital inputs 1 and 2 (cf. chapter 3.1.6): (0/1/2/3)
3015		interval counter 1 (16-bit- counter)
3016		interval counter 2 (16-bit- counter)
3017		unused
3018		unused
3019	23451	last archive read out: 1011|10111|0011011 = 23.5.6:45

2.14 Communication between Receiver and Sensor-Actuator Modules

The address range 5000 – 5999 is used for the data exchange between Sensor-Actuator modules and the receiver. There are two blocks of registers, one request block and (5000 – 5009) one response block.

The **request block** is structured in the following way:

Address	Type	Comment
5000	input	Command code
5001	input	1st parameter, word
5002	input	2nd parameter, byte
5003	input / output	handshake

The response block is structured in the following way:

Address	Type	Comment
5010	input/ output	handshake
5011	output	number of response registers
5012	output	start of response

The content of the response depends on the command code type: the values 2 and 3 are used in replies to NVR and NVW. For AUX the CMD code itself is used, i.e. 24. The subsequent addresses also have a CMD-code dependent content, which is shown in examples below.

Communication Process

Request block:
Example: Set transmission interval to 2 minutes.

Address	Value	Comment
5000	12	Command code 12, NVW write NV
5001	8	Word parameter, 8 times the standard-time interval of 15 sec.
5002	5	Byte parameter, NV value
5003	1	handshake, request

The handshake register is set to 1 by the application if a request has been issued. It is set back to 0 after processing the request.

If a request can't be processed correctly the handshake register 5010 is set to 0x8001. Only one command can be issued at a time. If the user switches over to

another module without having reset the handshake of the last reply, the response handshake for that module I set to 0x4001.

Response block for the request above:
After a response has arrived the addresses from 5010 onwards show:

Address	Value	Comment
5010	1	handshake
5011	4	number of response registers
5012	3	Response to NVW command
5013	4	value set
5014	5	NV number

The handshake register is set to 1 by the receiver after a response has arrived. The application will set it back to 0 after the response has been processed.

Addresses from 5012 onwards are reserved for the response. The result is shown in the respective register and the user can get the data and set back the handshake. Further examples cf. 2.14.2.

2.14.1 Available Commands

The following commands are available for communication between receiver and Sensor-Actuator modules (type 5).

- NVR (CMD code 11)
- NVW (CMD code 12)
- VER (CMD code 15)
- Aux1 (CMD code 24)
- OPR (CMD code 16)
- Read archive from x minutes backwards (CMD code 1001)
- Read archive from block x to block y (CMD code 1002)

NVR will read the network variables using the respective byte parameter bp:

- bp 0x41: GetTimeb minutes from 0 h
- bp 0x42: GetDateb year*512 + month*32 + day
- bp 0x05: transmission interval

NVW will write the network variables using byte parameter bp and word parameter wp:

- bp 0x05;
  wp 18: transmission interval is set to 18 x 15 sec = 4.5 min
  15 seconds is used as a standard time interval here.
- bp 0x4x set RTC
  - bp 0x42; wp BCD (minutes)*256 + BCD (seconds)

- bp 0x44; wp BCD (day)*256 + BCD (hours)
- bp 0x47; wp BCD (year)*256 + BCD (month)

- bp 0x50; delete archive
  wp module address ID_Low

Aux1 commands to set functions and parameters:

- bp 0x01; switch off temperature
  wp temp. in 0,01 °C (TMIN – TMAX)
- bp 0x02; switch on temperature
  wp temp. in 0,01 °C (TMIN – TMAX)
- bp 0x03; Priority setting "Relay off"
  wp duration in minutes (0 – 900)
- bp 0x04; Priority setting "Relay on
  wp duration in minutes (0 – 900)
- bp 0x05; „Regulation off"
  wp duration in minutes (0 – 7*1440)

NOTE: Absolute limit values have been pre-defined for a cooling temperature regulation. These cannot be modified by the user:

- TMAX = -18 degree and
- TMIN = -34 degree.

Below TMIN cooling always set to OFF and above TMAX it is always ON. Only in the "stop regulation" mode (e.g. for de-icing) the TMAX limit is ignored.

Commands for reading out archives:

- cmd:1001; read out beginning this time backwards
  wp time in minutes,
- cmd:1002; read out from block x to block y
  wp block# x; bp block# y
- Cmd:11 (NVR);
  bp 128 wp 0 read out complete archive

2.14.2 Examples of Applying Commands

2.14.2.1 Example: Priority setting for "relay on"

This command will turn the relay on for the time set.

The **request block** is structured in the following way:

Address	Value	Comment
5000	24	AUX1
5001	5	on-time in minutes, 5 minutes
5002	4	coding for priority setting relay on
5003	1	is set to 1 by the application if a request is entered; will be set to 0 by the receiver after the request has been processed

After a response arrived the addresses from 5010 onwards show:

Address	Value	Comment
5010	1	is set to 1 by the receiver if a response arrived; will be set to 0 by the application after the response has been processed
5011	4	
5012	24	mirroring AUX1
5013	5	mirroring time parameter
5014	132	mirroring the coding for priority setting relay on +0x0080

2.14.2.2 Example: Priority setting for “relay off”

This command will turn the relay off for the time set.

The **request block** is structured in the following way:

Address	Value	Comment
5000	24	AUX1
5001	3	off-time in minutes, 3 minutes
5002	3	coding for priority setting relay off
5003	1	is set to 1 by the application if a request is entered; will be set to 0 by the receiver after the request has been processed

After a response arrived the addresses from 5010 onwards show:

Address	Value	Comment
5010	1	is set to 1 by the receiver if a response arrived; will be set to 0 by the application after the response has been processed
5011	4	
5012	24	mirroring AUX1
5013	3	mirroring time parameter
5014	131	mirroring the coding for priority setting relay off +0x0080

2.15 Module Register for Self-configuring Systems - Unit Identifier Reference

The address range 10 000 – 10 299 holds a table referencing module ID and “Unit Identifier”, the Modbus address used for access from clients to the GesySense systems in which the receiver organizes its configuration regarding

the modules itself. Further information is provided in chapter 3.6 .

Address	Type	Comment
10 000 – 10 001	Output	Serial number module 1 (module of type 5 or 6)
10 002	input/output	Modbus device address of the module
10 003 – 10 004	Output	Serial number module 2
10 005	input/output	Modbus device address of the module
…		
10 297 – 10 298	output	Serial number module 100
10 299	input/output	Modbus device address of the module

The table is defined for the capacity of the Receiver \LAN, for 100 modules. Due to lower memory capacity other receivers can only register up to 50 modules in this way.

Representation of Values

Address	Value	Comment
10 000	888	serial number module 1 (cf. 3.3): serial number 6.000.000.888
10 001	24576	
10 002	2	Modbus device address of the module

2.16 Use Case Repeater Data

When the wireless sensor system is turned on, all repeater data found is written to the address range 10 – 65 or 1500 – 1534 by the receiver. Independent of that, the total of all repeaters found is written to address 9. Active repeaters are always written into the 0 – 65 range. If there are several repeaters in the system with the same repeater number (not serial number), the serial number is written alternatingly to the respective (repeater number) address.

NOTE: If the same Repeater number is used more than once, this will cause unnecessary collisions in the wireless network and thus not allowed.

Further to that, data of repeaters which have not been made known to the system through an external application by writing them to the 1000 – 1033 range are written to the range 1500 – 1534. If an external system later assigns a repeater serial number to the 1000 – 1033 range, the receiver will –provided that it receives the repeater via radio– write data of that repeater to the respective addresses in the 10 – 65 range and delete it from the range 1500 – 1534, if it existed there.

3 Explanations and Annotations

3.1 Algorithms and Codings

3.1.1 Calculation of Start Date Representation

The value of the start date is calculated:

Day of month +32*number of month +512*(year-2000)

Example:	August 15, 2008:	15+32*8+512*8	= 4367
	January 13, 2009:	13+32*1+512*9	= 5013

3.1.2 Calculation of Measuring Time Representation

The value for measuring time is the number of seconds since 00:00 divided by 2.

Example: 17:25:12 → 62712 seconds → value: 31356

NOTE: Odd numbers of seconds are increased by 1.

3.1.3 Calculation of Temperature Value Representation

Decimal values for temperatures are written multiplied by 100.

Negative values are written as two's complement to a 16 bit word.

Example: 2050 is equivalent to 20.5 °C
63605 is equivalent to -19.3 °C

3.1.4 Calculation of Analog Values

The values from analog modules are represented as figures between 0 and 10,000.

Examples:

0 – 10 V	1250	≙	1250*10/10 0000 mV	= 1,25 V
0 – 20 mA	1250	≙	1250*20//10 00 mA	= 2,5 mA
4 – 20 mA	1250	≙	1250 *16/10 000 mA	= 2 mA

3.1.5 Calculation of Counter Values

The value of a counter is stored in two subsequent addresses of 32 bit in total. Thus a range of 1 to 2 ^32 -1 (=4.294.967.295) is available for pulse counting. The first address holds the lower value, the second the higher.

The number of measured pulses results from:

lower value + higher value * 65535

3.1.6 Status Sensor Value Coding

The value transmitted for the digital inputs (DI) is coded as follows:

Value	Digital input 1	Digital input 2
0	OFF	OFF
1	ON	OFF
2	OFF	ON
3	ON	ON

These values have to be resolved by the master according to the table to get separate values for each of the 2 data points.

3.2 Reset Behavior

The moment the receiver starts up the value of Modbus address 7 (date) is 0. Time (address 6) will start to count immediately and is set by the master device. The master recognizes the reset from the date value and the error code and act accordingly:

- Module identifications (ID) of wireless modules are set again
- Time and date (addresses 6 and 7) are set again
- Repeater configuration data (starting at address 1000) are set again

3.3 Module Identification

Each module is identified by a unique ID, its serial number. It is stored in 2 subsequent addresses of 32 bit altogether, bits 1 – 28 for a sequential number and bits 29 – 32 as a module type code. The lower address holds the lower word, the following the upper word with the type code.

Device type code

The upper 4 bits (29 – 32) of the 32 bit module ID (serial number) are used for the type code in the following way:

Device	Type Code	Bit 29 – 32	Upper Word
Temperature module	0	0 0 0 0	0
Status module	1	0 0 0 1	4096
Counter module	2	0 0 1 0	8192
Analog module	3	0 0 1 1	12288
Sensor-Actuator module	5	0 1 0 1	20480
Mixed-Signal module	6	0 1 1 0	24576
Repeater / receiver	8	1 0 0 0	32768

The bit sequence of the type code has to be interpreted by the master and represented according to the definition in the Type Code column.

Sequential part of module ID
The sequential part of the ID number is contained in bits 1 – 28. This means there are up to 2 ^28 -1 = 268,435,455 IDs available for the GesySense system. Only the range from 1 to 200,000,000 is used for module ÎDs. In front of this the type code is placed as first digit.

Complete with type code
For a digital status sensor module the serial number has the structure 1.xxx.xxx.xxx, with xxx.xxx.xxx ≤ 200.000.000 and type code 1. A receiver or repeater has the same structure with type code 8: 8.xxx.xxx.xxx.

Examples:

Type	Serial number	Modbus address, lower	Modbus address, upper
Temperature module	0.000.000.100	100	0
Temperature module	0.000.070.000	4464	1
Status module	1.000.000.120	120	4096
Status module	1.000.110.533	44997	4097
Counter module	2.000.000.555	555	8192
Counter module	2.000.090.788	25252	8193

Analog module	3.000.000.444	444	12288
Analog module	3.000.194.300	63228	12290
Sensor-Actuator module	5.000. 000.444	444	20480
Sensor-Actuator module	5.000. 194.300	63228	20482
Mixed-Signal module	6.000.000.444	444	24576
Mixed-Signal module	6.000.194.300	63228	24578
Receiver/repeater	8.000.000.222	222	32768
Receiver/repeater	8.000.150.400	19328	32770

3.4 Representation in Master Device

3.4.1 Data Point Assignment in Master Device

The master device must have an internal “assignment table” mapping the serial numbers of the wireless modules to individual data points. Thus every single bit of information from a wireless module corresponds to a distinct data point.

3.4.2 Temperature Module

Comment	**module 1**	**module 2**
serial number of the module	123.456	123.455
signal quality (=strength) of the module	98	97
transmission quality of the module	99	96
battery status of the module	87	87
measuring time of the module	12:30:00	12:30:3
measured value of the module	12,32	12,33

3.4.3 Status Module with 2 digital inputs

Comment	**module 3**	**module 4**
serial number of the module	1.000.123.480	1.000.123.491
signal quality (=strength	99	96
transmission quality	97	98
battery status	87	87
measuring time	12:30:00	12:30:03
measured value	1	3

3.4.4 Counter Module with 2 counters

Comment	module 5	module 6
serial number of the sensor	3.000.123.480	1.000.123.491
signal quality (=strength)	99	96
transmission quality	97	98
battery status	87	87
measuring time	12:30:00	12:30:03
counter 1	144	65123
counter 2	73123	12

3.4.5 Analog Module

Comment	module 7	module 8
serial number of the sensor	3.000.123.687	3.000.125.777
signal quality (=strength)	98	97
transmission quality	99	96
battery status	87	87
measuring time	12:30:00	12:30:3
measured value	5232	3233

3.4.6 Monitoring data

Together with the monitoring data (address 0 – 65) the repeater configuration information “repeater number in system” and “Route Repeater” (1000 – 1033) is passed on as a figure. Interpretation by the master depends on the device type used.

3.4.7 Repeater Routing Information

Information on routes to repeaters (i.e. “Repeater number in system” and “Route Repeater”) is not interpreted by the master but passed on as a number.

3.4.8 Setting Date and Time

Once every day the time must be synchronized between master device and receiver by setting the values for addresses 6 and 7.

3.5 Wireless Firmware Update

The firmware of devices with a receiver can be updated via radio. Currently this is applicable to repeaters and Sensor-Actuator modules.

The distribution is governed by the central receiver. The procedure depends on the receiver type.

Receivers which are only accessible via EIA-485 get the new firmware via Modbus and will distribute by radio to the installed repeaters, cf. chapter 2.3, “Firmware Update of Repeaters and Receivers without Ethernet” and chapter 3.5.1.

Receiver with Ethernet connection get their firmware updates and those for repeater and SAM modules together with a control file via ftp. Then the receiver will run the update operation. Distribution to repeaters follows the process describe for receivers without Ethernet. The distribution to SAM modules is described in chapter 3.5.2,”Firmware Update of Sensor-Actuator Modules via Radio”

3.5.1 Firmware Update of Receivers/Repeaters without Ethernet via Radio

A new firmware for receiver and repeater devices is downloaded into a receiver without Ethernet via EIA-485 Modbus. The procedure follows the Modbus Specification [1].

The update is a binary file including a checksum. The updated firmware is distributed from the main server to the data servers (Modbus master) and downloaded via Modbus to the central receiver of the system.

The function code 21 (0x15) “Write File Record” initiates the firmware download. The “file number” of the software is “1”. The Modbus file download is record based; the record size is set to 128 Byte. One file may consist of 10,000 records maximum.

A download always starts with record number 0. This signals to the receiver that a new download is coming. The downloaded firmware is preliminarily written into a serial memory.

Transmission end is explicitly indicated to the receiver by transmitting the record number 9999. Thus transmission can be cancelled by the mast at any time.

NOTE: There must not be any interruption of more than 30 seconds between 2 telegrams or the receiver will terminate the download. Any following telegrams referring to the download will be answered with a negative reply unless record number 0 is sent to indicate the restart.

Name	Value
Function Code	0x15
Request data length	x bytes
Reference type	6
File number	1
Record number	0 … n
Record length	64 or remainder/2 (data is a multiple of 2 byte)
Record data	128 bytes or remainder in last record

3.5.2 Firmware Update of Sensor-Actuator Modules via Radio

A new firmware for SAM modules is first downloaded to the Receiver with Ethernet via FTP. Further distribution is run by the receiver using the broadcast method.

The update process is initiated by setting Modbus address 85 to “1”. Update data is sent block by block with an adjustable delay. Address 86 provides the information how often the transmission shall be repeated. After all blocks have been sent, the receiver will query every module for its firmware version number. If for some module it is not the latest version this module will be asked which blocks are missing. The missing blocks will be transmitted repeatedly until all block have arrived.

NOTE SAM Module will only receive firmware updates if they are connected to the external 24 V power supply.

3.6 Addressing Modules in Self-Configuring Systems

In a system with fixed, pre-defined configuration the GesySense Receiver is a single Modbus device, the configuration of which is known to the Modbus master. As the master knows all addresses in the device, all information received by the receiver from wireless modules can be accessed.

If however, auto-configuration is permitted, i.e., if the receiver captures new modules based on a massage with new module ID and organizes them by itself, a direct access to the data from a specific module is not possible. The querying system, in case of Modbus TCP the client, would need processing capacities which usually cannot be expected to be available on simple devices.

Therefore a concept of virtual Modbus devices is introduced applicable with certain receiver devices[1] and type 5 and type 6 modules (controlled by the entry at Modbus address 81). Applying this concept the single sensor modules are availa-

[1] currently: Receiver \LAN, receiver with Ethernet.

ble to the master as independent Modbus devices, identifiable by their Modbus device address.

Access to system (module) data is given on one hand via the Modbus device address of the receiver (=1) and fixed the address range known to the master. Thus the master can obtain from the receiver data for all modules already known. On the other hand access is provided by means of the unit identifier, the access address behind which information is stored in a known structure. In the Modbus address range of the receiver these are the address beginning at 3000. For commands to SAM modules addresses beginning at 5000 are used.

Figure 3-1 gives a representation of the virtualization concept for modules with the address ranges.

Removing Modules

As the table of dynamically registered modules is automatically filled by the receiver the Modbus client has to enter a “0” for the Modbus device address (Unit identifier) of the module to be removed. The receiver will then set the address for module ID to “0” as well. The table is not sorted in any way. Thus there may be empty records in the table, which has to be observed by any evaluation.

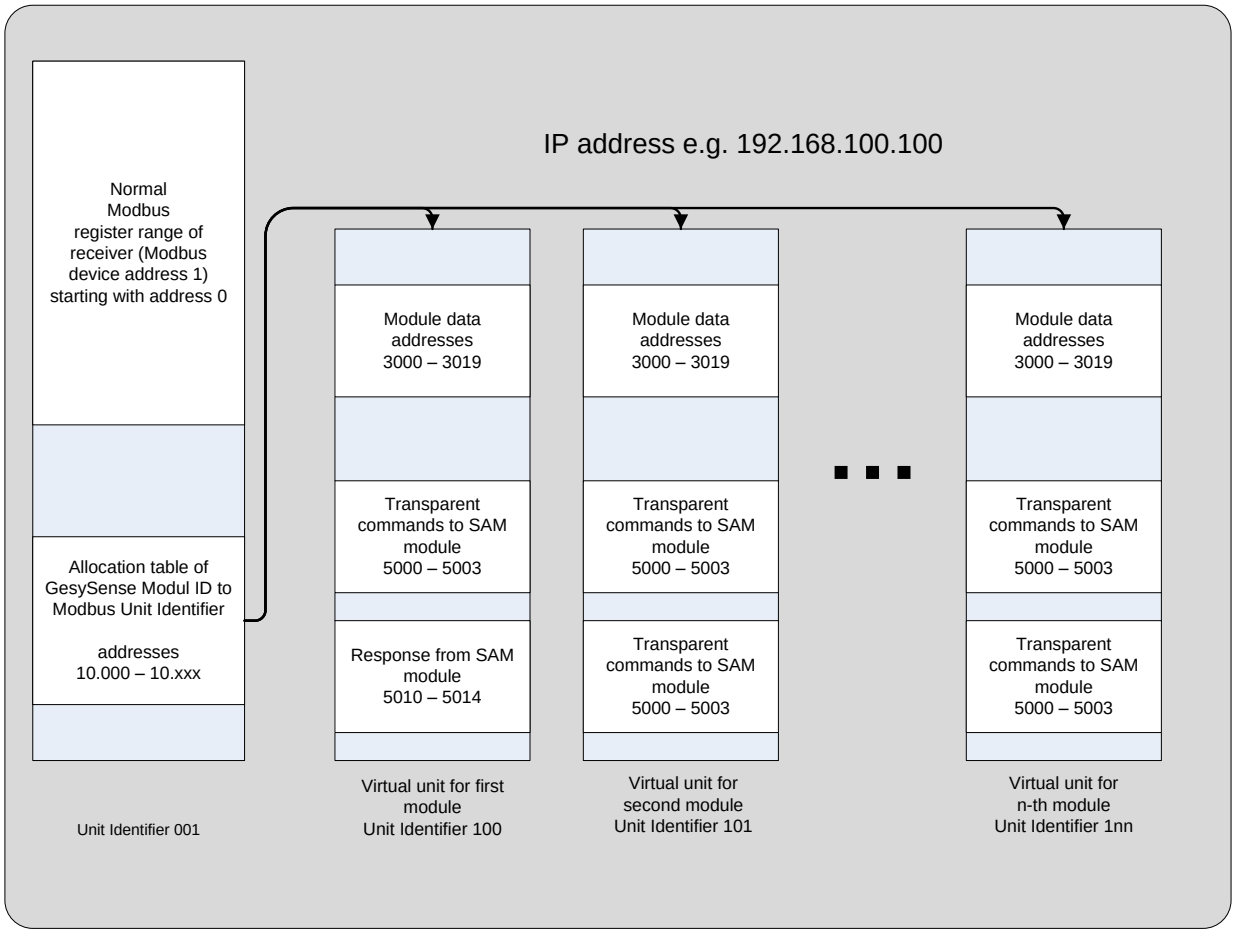

Figure 3-1: Addressing virtual Modbus devices

4 Complete Modbus Address List

NOTE: The table is a representation from the receiver's point of view (slave). Out means the receiver (slave) will write to this address, input means the receiver will read from this address.

Symbolic Name	Type	Address	Comment
serial number 1 receiver	output	0	lower Address
serial number 2 receiver	output	1	upper Address
start date receiver	output	2	tt+32*mm+512*(yyyy -2000)
firmware version receiver	output	3	
hardware version receiver	output	4	
error status receiver	output	5	
system time1 receiver	input	6	time in seconds per day/2
system time2 receiver	input	7	date: dd+32*mm+512*(yyyy -2000)
number of received modules	output	8	
number of received repeaters	output	9	
serial number 1 repeater 1	output	10	lower Address
serial number 2 repeater 1	output	11	upper Address
start date repeater 1	output	12	
firmware version repeater 1	output	13	
hardware version repeater 1	output	14	
transmission strength repeater 1	output	15	
error status repeater 1	output	16	
number of directly received modules repeater 1	output	17	
serial number 1 repeater 2	output	18	
serial number 2 repeater 2	output	19	
start date repeater 2	output	20	
firmware version repeater 2	output	21	
hardware version repeater 2	output	22	
transmission strength repeater 2	output	23	
error status repeater 2	output	24	
number of directly received modules repeater 2	output	25	
.... Up to 7 repeaters		*to 65*	
start Firmware distribution	input	70	Will be reset by receiver

status Firmware distribution	output	71	
manual start of firmware update for repeater 1	input	72	will be reset by receiver
manual start of firmware update for repeater 2	input	73	will be reset by receiver
manual start of firmware update for repeater 3	input	74	will be reset by receiver
manual start of firmware update for repeater 4	input	75	will be reset by receiver
manual start of firmware update for repeater 5	input	76	will be reset by receiver
manual start of firmware update for repeater 6	input	77	will be reset by receiver
manual start of firmware update for repeater 7	input	78	will be reset by receiver
control for cyclic storage of a dynamically registered configuration	input	79	value: 0xbbba; bbb: interval in minutes until configuration is stored again. a: 0 = do not save 1 = save 2 = delete configuration
Read out archive automatically	input	80	value: 0xbbba; bbb: interval in minutes; a: 0 = don't read out archive; 1 = read out if DI1 is switched from 0 to 1 and at least the time bbb has elapsed; 2 = read out if after ≥ bbb minutes without message a new radio message is received; 3 = read out regularly at 00:00 o'clock plus bbb minutes; 4 = read out cyclically at the interval bbb set
Automatic configuration	input	81	Values: 0: off, the configuration has to be loaded into the receiver 1: on, new modules are automatically assigned to the respective registers

power control (for battery powered receivers)	input	82	value: 0xa(1)bbbb; a: on time in minutes (1 to 15); (1): 1 switch on repeatedly; 0 switch on only once a day; bbbb: switch on time and repetition interval (1 to 1440 minutes)
read archive from module if no data is present on receiver	input	83	the value defines how many minutes backwards from "now" archive data is to be read from type 5 modules. The default value 0 is defined as 1440 minutes, i.e. 24 hours.
switch relay of Receiver \LAN on/off	input	84	1 = on, 0 = off;
SAM firmware update	input	85	start SAM firmware update
SAM firmware update	input	86	repetitions of an SAM firmware up-date
serial number 1 module 1	output	100	lower address unregistered module
serial number 2 module 1	output	101	upper address with type identification
signal quality (=strength)	output	102	figure between 0 and 100
transmission quality	output	103	figure between 0 and 100
battery status	output	104	figure between 0 and 100
measuring time	output	105	seconds from 0:00 / 2
measured value	output	106	
serial number 1 module 2	output	110	
serial number 2 module 2	output	111	
signal quality (=strength)	output	112	
transmission quality	output	113	
battery status	output	114	
measuring time	output	115	
measured value	output	116	
... up to 10 unregistered modules		*... 190 – 196*	
serial number 1 module 1	input	200	lower address registered temperature module
serial number 2 module 1	input	201	upper address with type identification
signal quality (=strength)	output	202	figure between 0 and 100
transmission quality	output	203	figure between 0 and 100
battery status	output	204	figure between 0 and 100

measuring time	output	205	seconds from 0:00 / 2
measured value	output	206	
start date module 1	input	207	
lower limit for temperature	input	208	alarm if temp is below value
upper limit for temperature	Input	209	alarm if temp is above value
serial number 1 module 2	input	210	
serial number 2 module 2	input	211	
signal quality (=strength)	output	212	
transmission quality	output	213	
battery status	output	214	
measuring time	output	215	
measured value	output	216	
start date module 2	input	217	
lower limit for temperature	input	218	
upper limit for temperature	Input	219	
... up to 80 modules		*..990 - 997*	
serial number 1 repeater 1	input	1000	lower address Repeater 1
serial number 2 repeater 1	input	1001	upper address
repeater number of repeater 1	input	1002	Sequence number within the system
route repeater 1	input	1003	
serial number 1 repeater 2	input	1005	lower address Repeater 2
serial number 2 repeater 2	input	1006	upper address
repeater number of repeater 2	input	1007	
route repeater 2	input	1008	
... up to repeater 7		*..1030 1033*	
serial number 1 unknown repeater 1	output	1500	lower address of unknown repeater
serial number 2 unknown repeater 1	output	1501	upper address of unknown repeater
repeater number of unknown repeater 1	output	1502	
start date unknown repeater 1	output	1503	dd+32*mm+512*(yyyy -2000)
error code at configuration of repeater 1	output	1504	
serial number 1 unknown repeater 2	output	1505	lower address
serial number 2 unknown repeater 2	output	1506	upper address
repeater number of unknown repeater 2	output	1507	

start date unknown repeater 2	output	1508	
error code at configuration of repeater 2	output	1509	
...up to unknown repeater 7		*...1530 – 1534*	
serial number 1 module 1	input	1600	lower address, module type 5 or 6
serial number 2 module 1	input	1601	upper address, module type 5 or 6
time interval for counters 1 and 2	input	1602	value: ab (Hex) a: time interval channel 1, b: time interval channel 2; in minutes
dimension and pulse valence for counter 1 and 2	input	1603	value: abcd (Hex) a: dimension unit channel 1; b: dimension unit channel 2; c: number of pulses channel 1; d: number of pulses channel 2
serial number 1 module 2	input	1604	lower address
serial number 2 module 2	input	1605	upper address
time interval for counters 1 and 2	input	1606	
dimension and pulse valence for counter 1 and 2	input	1607	
serial number 1 module 3	input	1608	lower address
serial number 2 module 3	input	1609	upper address
time interval for counters 1 and 2	input	1610	
dimension and pulse valence for counter 1 and 2	input	1611	
...for up to 100 SAM or MX modules		*...1996 – 1999*	
serial number 1 module 1	input	2000	lower address registered status module
serial number 2 module 1	input	2001	upper address
signal quality (=strength)	output	2002	figure between 0 and 100
transmission quality	output	2003	figure between 0 and 100
battery status	output	2004	figure between 0 and 100
measuring time	output	2005	seconds from 0:00 / 2
digital value	output	2006	0: DI1 = 0, DI2 = 0 1: DI1 = 1, DI2 = 0 2: DI1 = 0, DI2 = 1 3: DI1 = 1, DI2 = 1
start date module 1	input	2008	dd+32*mm+512*(yyyy -2000)
serial number 1 module 2	input	2010	lower address

serial number 2 module 2	input	2011	upper address
signal quality (=strength)	output	2012	
transmission quality	output	2013	
battery status	output	2014	
measuring time	output	2015	
digital value	output	2016	
start date module 2	input	2018	
... for up to 30 Status-Modules		*...2290 – 2298*	
serial number 1 module 1	input	2300	lower address registered digital counter module
serial number 2 module 1	input	2301	upper address
signal quality (=strength)	output	2302	figure between 0 and 100
transmission quality	output	2303	figure between 0 and 100
battery status	output	2304	figure between 0 and 100
measuring time	output	2305	seconds from 0:00 / 2
counter 1 value (lower value)	output	2306	lower value of 32 bit counter
counter 1 value (upper value)	output	2307	upper value of 32 bit counter
counter 2 value (lower value)	output	2308	
counter 2 value (upper value)	output	2309	
start date module 1	input	2310	dd+32*mm+512*(yyyy -2000)
serial number 1 module 2	input	2311	
serial number 2 module 2	input	2312	
signal quality (=strength)	output	2313	
transmission quality	output	2314	
battery status	output	2315	
measuring time	output	2316	
counter 1 value (lower value)	output	2317	
counter 1 value (upper value)	output	2318	
counter 2 value (lower value)	output	2319	
counter 2 value (upper value)	output	2320	
start date module 2	input	2321	
... for up to30 Counter-Modules		*... 2619 – 2629*	
serial number 1 module 1	input	2700	lower address registered analog module
serial number 2 module 1	input	2701	upper address
signal quality (=strength)	output	2702	figure between 0 and 100

transmission quality	output	2703	figure between 0 and 100
battery status	output	2704	figure between 0 and 100
measuring time	output	2705	seconds from 0:00 / 2
measured value	output	2706	
start date module 1	input	2707	dd+32*mm+512*(yyyy -2000)
serial number 1 module 2	input	2710	
serial number 2 module 2	input	2711	
signal quality (=strength)	output	2712	
transmission quality	output	2713	
battery status	output	2714	
measuring time	output	2715	
measured value	output	2716	
start date module 2	input	2717	
... up to30 Analog-Modules		*...2990 – 2997*	
serial number 1 module 1	input	3000	lower address, registered module type 5 or 6
serial number 2 module 1	input	3001	upper address
start date	input	3002	dd+32*mm+512*(yyyy -2000)
module configuration	input	3003	cipher, indicating the configuration, i.e. which hardware functions are activated
signal quality (=strength)	output	3004	figure between 0 and 100
transmission quality	output	3005	figure between 0 and 100
battery status	output	3006	figure between 0 and 100
measuring time	output	3007	seconds from 0:00 / 2
Temperature value 1	output	3008	0.01, ambient or PT1000
Temperature value 2	output	3009	0.01 PT1000
counter 1	output	3010	32 bit counter, lower bits
counter 1		3011	upper bits
counter 2	output	3012	32 bit counter, lower bits
counter 2	output	3013	upper bits
Digital value of module	output	3014	0,1,2,3 (for 2 DI's); bit 7 for DO
interval counter 1	output	3015	16 bit counter per interval
interval counter 2	output	3016	16 bit counter per interval
unused	output	3017	
unused	output	3018	

Last date of archive read-out	input	3019	Bit sequence: month (aaaa) day (bbbbb) time in quarters of an hourint (ccccccc)
serial number 1 module 2	input	3020	
serial number 2 module 2	input	3021	
start date	input	3022	
module configuration	input	3023	
signal quality (=strength)	output	3024	
transmission quality	output	3025	
battery status	output	3026	
measuring time	output	3027	
Temperature value 1	output	3028	
Temperature value 2	output	3029	
counter 1	output	3030	
counter 1		3031	
counter 2	output	3032	
counter 2	output	3033	
Digital value of module	output	3034	
interval counter 1	output	3035	
interval counter 2	output	3036	
unused	output	3037	
unused	output	3038	
Last date of archive read-out	output	3039	
... for up to 100 SAM and MX modules		*… 4980 – 4999*	
command code	input	5000	code and format according to command description
1st parameter	input	5001	word parameter
2nd parameter	input	5002	byte parameter
handshake	input/ output	5003	set to 1 by the application if a request has been entered and is reset to 0 by receiver when the request has been processed.
handshake	input/ output	5010	set to 1 by the receiver if a reply has been entered and is reset to 0 by application when the reply has been processed.
number of reply registers	output	5011	
content of reply	output	5012	start of reply

content of reply	*output*	*5013 …*	*Reply continued according to 5011*
serial number module 1 ()	output	10 000	lower address, module type 5 or 6
serial number module 1 (type 5 or 6)	output	10 001	upper address
Modbus device address	input/ output	10 002	8 bit value
... for up to 100 SAM and MX modules		*… 10 297 – 10 299*	