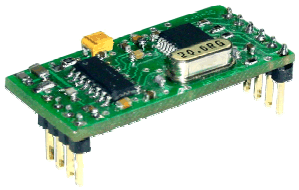
NETRONIX

Technical Data Sheet

Q5M-005

Q5M005-DTRdoc-01.06
In reference to Q5M005-c-02.00



Contents

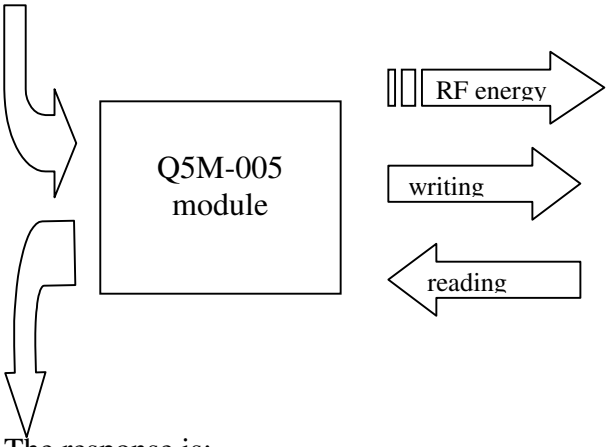
Contents 2
Introduction 3
Pin diagram 3
Connection diagram 4
General Specifications 4
Frame format of serial transmission: 4
Q5 transponder overview 5
Command overview: 7
High level commands: 7
Writing the Q5 transponder as a Unique 7
C_HL_UniqueWrite 7
Reading out the Unique transponder 7
Writing the transponder sector 7
Reading out the transporter sector 8
Writing the sector password protected 8
Reading out the transponder sector password protected 8
Low level commands 8
Switching on the antenna electromagnetic field 8
Switching off the antenna electromagnetic field 9
Writing the transponder sector 9
Reading out the transponder sector 9
Writing the transponder sector password protected 9
Reading out the transponder sector password protected 10
Writing the Q5 transponder as a Unique 10
Reading out Unique transponder 10
Additional commands 10
Setting the gain of receiving path for the transponder signals 10
Setting the address of Q5M-005 module RSXX bus 11
Writing bit to the I/O port 11
Reading out bit from the I/O port 11
Reading out the software version of Q5M-005 module 11
Calculation the CRC value 12
Examples of Q5 transponder operation with the help of Q5M-005 12
High level function operation 13
Example 1 Unique write 13
Example 2 Sector write 14
Example 3 Password protection 15
Example 4 Read-out with password 16
Example 5 Removing the password 17
Low level function operation 18
Example 6 Sector decrementation 18

Introduction

Module Q5M-005 operates on principle of the contactless information writing and reading from and to the transponder Q5 (RFID). The module can read data from Unique transponders as well. Data are transmitted via RS-232 interface compatible with TTL voltage level.
The principle of operation:
query from (master unit- host) - (module) action - (module) response.

The query is sent to the module Q5M:

module address	frame length	command	data	CRCH,CRCL
xx	xx	xx	xx xx xx	xx xx



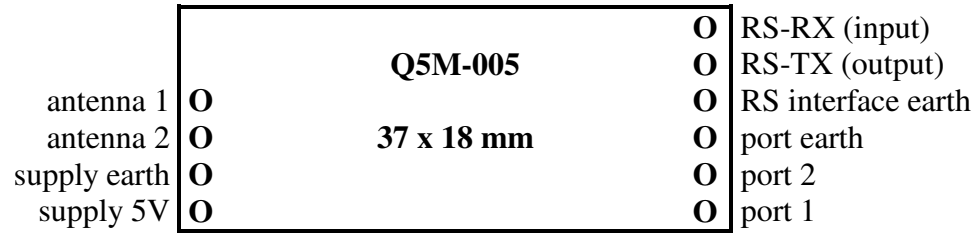
Sector no.	Q5 Transponder sectors			
0				
1				
2				
3				
4				
5				
6				
7				

The response is:

Module address	frame length	response	data	operation code	CRCH,CRCL
xx	xx	xx	xx xx	xx	xx xx

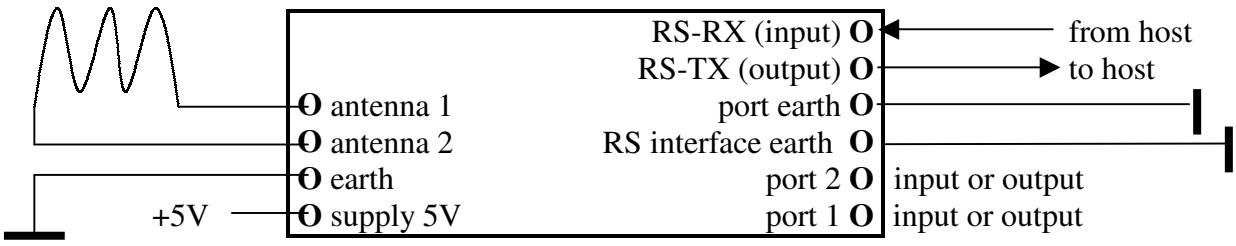
The module is equipped with two 1-bit user ports, which can be used for reading and writing. Connect an air coil antenna to the Q5M-005. The antenna will produce an electromagnetic field and supply a transponder located in the field.

Pin diagram



drwg.: module pins – element side view

Connection diagram



General Specifications

Supply voltage Uz: . . . . . 4,5...5,5V
Supply current: . . . . . 5...55mA
Module rated operating radio frequency 125kHz
Modulation type of data received from transponder . . . . . .Manchester
Baud rate of data received from transponder RF/64 (1953b/s)
Baud rate of data sent to transponder RF/50 (2500b/s)
Output current capacity: port1, port2 and RS-TX 10mA
Transporter read / write distance (depending on antenna used): . . . . . up to 12cm
Antenna inductance . . . . . 1mH +-5%
Interface specifications. . . . . .baud rate: 9600 b/s, data bit: 8, stop bit 1, no parity, voltage levels comply TTL format.

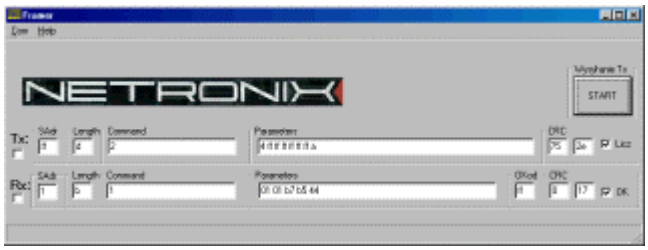
Frame format of serial transmission:

Command: ModuleAddress, FrameDataNumber, Command, Parameters1...n, CrcH,CrcL

Where:
Module address – unique address of module in system
If:
ModuleAddress = 0 - no module responds
ModuleAddress = 0xff – any module in network will respond
FrameDataNumber – total frame length
Command - even value
Parameters 1...n - exists optionally and depends on command
CrcH,CrcL - MSByte and LSByte of CRC value respectively

Response: ModuleAddress, FrameDataNumber, Anwer, Parameters1...n, OperationCode, CrcH,CrcL

ModuleAddress – assigned the real address of responding module
FrameDataNumber - total frame length
Response =Command+1 = odd value
Parameters1...n - exists optionally and depends on command
OperationCode- informs about correctness executed command
CrcH,CrcL-, older and younger byte of CRC value respectively



Module can be tested with FRAMER software tool, which makes work with frames easier.

Q5 transponder overview

Q5 transponder comprises eight sectors, of which one is reserved as a configuration registry. Remained sectors are used by user and can be written in and read out in case of lock lack „Lock" (L) of given sector. If such lock has been set for given sector before, the only possibility is to read out the sector.
In case of configuration which protects transponder with password, the password is saved in sector no. 7.

Sector no.	Q5 transponder sectors				
0	32 configuration bits				L
1	8b	8b	8b	8b	L
2	8b	8b	8b	8b	L
3	8b	8b	8b	8b	L
4	8b	8b	8b	8b	L
5	8b	8b	8b	8b	L
6	8b	8b	8b	8b	L
7	possible password				L

32 configuration bits+ L

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	26	28	29	30	31	32	33
0	1	1	0	0	0	0	0	0	0	0	0	0		r5	r4	r3	r2	r1	r0			f1	f0		m2	m1	m0	b2	b1	b0	0	L
													Fast write	Data Bit Rate						Use AOR	Use PWD	PSK carrier frequency		Invers data output	Modulation			Max Block				Lock

Fast write - determines the data write mode, for operation of transponder with Q5M-005 the Fast write should be equal to 0.

Data Bit Rate - sets the rate of transmitted data according to equation RF/(2r+2), for the Q5M-005 the rate is equal to RF/64, it means that for transponder r5 r4 r3 r2 r1 r0 = 0 1 1 1 1 1 (1fh)

Use AOR – determines the data receiving mode via transponder.
If AOR=1, the transponder will send the data as the second one (the first one should be a reader which sends a password).

If AOR=0 transponder sends data as the first one. It takes place in case of configuration conformed to Unique.

Use PWD – protects the transponder with a password saved in block no. 7. If PWD=1 the transponder will require functions which use the password for writing/reading to/from the sector.

If a user needs to use the Q5 transponder Q5, as a Unique, and additionally save password protected data, he should format the transponder with AOR=0 PWD=1.

PSK carrier frequency - Q5M-005 does not use PSK modulation. f0 f1 are any.

Invers data output - determines logic inversion of data sent – for Q5miko it should be = 0.

Modulation – modulation type of data send by transponder. During data receiving Q5M-005 decodes them conformed to Manchester (and to Unique too), it means that transponder should be formatted as a Manchester, m2 m1 m0 = 0 0 0.

Max Block – determines blocks number sent by transponder. When transponder cross the antenna area (and in case of AOR=0), it begins automatically to send the data beginning from block no.1 to a block determined by Max Block. In case of the Unique, Max Block=2.

Lock – decides if given sector does not change. Any time the sector has been written with parameter Lock=1, it wouldn't be possible to re-write the sector any longer.

Command overview:

Lock- byte which decide if card can be re-written.
When Lock = 1 the data cannot be re-written, in other case the data existing on card can be re-written.

SectorNr – value = (0…7)

OperationCode – informs about correctness of command execution by module Q5M-005.
(During sector reading process the number of received bits is checked but not their correctness. User must secure the data for instance for CRC writing in the sector or in a part of it.)

High level commands:

By means of high level commands it is possible to carry on full communication process with Q5 transponder. It means, that field switching on, normal process and field switching off is executed automatically. Normal process can consist of many write and/or many read out operations. Using many high level commands, we get longer sector access time, but we have an advantage we don't have to generate many write/read-outs in case of complex functions.

Writing the Q5 transponder as a Unique

Name of command – query	Command code	Parameters
C_HL_UniqueWrite	0x00	ID1…5,Lock

ID1…5 – ID number which we are to program on Q5 card to make it to simulate UNIQUE card.

Name of command – response	Response code	Parameters
A_HL_UniqueWrite	0x01	OperationCode

OperationCode – always is 0xff

Reading out the Unique transponder

Name of command – query	Command code	Parameters
C_HL_UniqueRead	0x02	-

Name of command – response	Response code	Parameters
A_HL_UniqueRead	0x03	ID1…5, OperationCode

ID1…5 – ID-UNIQUE number which is programmed for Q5 or UNIQUE transponder.
OperationCode – when = 0xff-read-out is correct (Unique control sum has been checked).

Writing the transponder sector

Name of command – query	Command code	Parameters
C_HL_Q5SectorWrite	0x10	Data1...4, SectorNo, Lock

Data1...4 - data we are to write in the sector
SectorNo –sector of destination

Name of command – response	Response code	Parameters
A_HL_Q5SectorWrite	0x11	OperationCode

OperationCode – always is 0xff

Reading out the transporter sector

Name of command – response	Response code	Parameters
C_HL_Q5SectorRead	0x12	SectorNo

SectorNo – source sector

Name of command – response	Response code	Parameters
A_HL_Q5SectorRead	0x13	Data1...4, OperationCode

Data1...4 – data from sector
OperationCode - 0xff - read-out is correct

Writing the sector password protected

Name of command – query	Command code	Parameters
C_HL_WithPasswordQ5SectorWrite	0x20	Data1...4, SectorNo, Password1...4, Lock

Data1...4 – written data
SectorNo – sector of destination
Password1...4 - password

Name of command – response	Response code	Parameters
A_HL_WithPasswordQ5SectorWrite	0x21	OperationCode

OperationCode – always is 0xff

Reading out the transponder sector password protected

Name of command – query	Command code	Parameters
C_HL_WithPasswordQ5SectorRead	0x22	SectorNo, Password1...4

SectorNo – sector of destination
Password1...4 - password

Name of command – response	Response code	Parameters
A_HL_WithPasswordQ5SectorRead	0x23	Data1...4, OperationCode

Data1...4 – red out data from the sector
OperationCode - 0xff - read-out is correct

Low level commands

Low level commands can be used in free strings without frequently on/off field switching.

Switching on the antenna electromagnetic field

Name of command – query	Command code	Parameters
C_TurnOnAntennaPower	0x30	-

Name of command – response	Response code	Parameters
A_ TurnOnAntennaPower	0x31	OperationCode

OperationCode – is always 0xff

Switching off the antenna electromagnetic field

Name of command – query	Command code	Parameters
C_TurnOffAntennaPower	0x32	-

Name of command – response	Response code	Parameters
A_TurnOffAntennaPower	0x33	OperationCode

OperationCode – is always 0xff

Writing the transponder sector

Name of command – query	Command code	Parameters
C_Q5SectorWrite	0x40	Data1...4, SectorNo, Lock

Data1...4 - data we are to write in sector
SectorNo – sector of destination

Name of command – response	Response code	Parameters
A_Q5SectorWrite	0x41	OperationCode

OperationCode – is always 0xff

Reading out the transponder sector

Name of command – query	Command code	Parameters
C_Q5SectorRead	0x42	SectorNo

SectorNo – source sector

Name of command – response	Response code	Parameters
A_Q5SectorRead	0x43	Data1...4, OperationCode

Data1...4 – sector data
OperationCode - 0xff – the read-out is correct

Writing the transponder sector password protected

Name of command – query	Command code	Parameters
C_WithPasswordQ5SectorWrite	0x50	Data1...4, SectorNo, Password1...4, Lock

Data1...4 – written data
SectorNo – sector of destination
Password1...4 - password

Name of command – response	Response code	Parameters
A_WithPasswordQ5SectorWrite	0x51	OperationCode

OperationCode – always is 0xff

Reading out the transponder sector password protected

Name of command – query	Command code	Parameters
C_WithPasswordQ5SectorRead	0x52	SectorNo, Password1...4

SectorNo – source sector
Password1...4 - password

Name of command – response	Response code	Parameters
A_WithPasswordQ5SectorRead	0x53	Data1...4, OperationCode

Data1...4 – red-out sector data
OperationCode - 0xff- read-out is correct

Writing the Q5 transponder as a Unique

Name of command – query	Command code	Parameters
C_UniqueWrite	0x60	ID1..5,Lock

Where: ID1..5 –ID number we are to program on card, to make it to simulate UNIQUE card

Name of command – response	Response code	Parameters
A_UniqueWrite	0x61	OperationCode

Where: OperationCode – always is 0xff

Reading out Unique transponder

Name of command – query	Command code	Parameters
C_UniqueRead	0x62	-

Name of command – response	Response code	Parameters
A_UniqueRead	0x63	ID1..5, Ope rationCode

ID1..5 – ID number which has been programmed on the UNIQUE card
OperationCode - 0xff - read-out is correct (Unique control sum has been checked)

Additional commands

Setting the gain of receiving path for the transponder signals

Name of command – query	Command code	Parameters
C_GainSet	0xa0	NewGain

NewGain – sensitivity of receiver circuit which reads data out the card (0..3)
This value is being written in non- violated memory

Name of command – response	Response code	Parameters
A_GainSet	0xa1	OperationCode

OperationCode – 0xff - operation is correct
0x20 - beyond parameter range

Setting the address of Q5M-005 module RSXX bus

Name of command – query	Command code	Parameters
C_SlaveAddressSet	0xa2	NewSlaveAddres

NewSlaveAddres – new module address in system = (1..0xfe)
This value is being written in non- violated memory

Name of command – response	Response code	Parameters
A_SlaveAddressSet	0xa3	OperationCode

OperationCode – 0xff - operation is correct
0x20 - beyond parameter range

Writing bit to the I/O port

Name of command – query	Command code	Parameters
C_WritePort	0x70	PortNr, Bit

PortNr=1,2
Bit=0,1

Name of command – response	Response code	Parameters
A_WritePort	0x71	OperationCode

OperationCode – always is 0xff
This operation sets given port as the "output" (low impedance) automatically.
After switching the power on, both of the ports operate in "input" mode (high impedance).

Reading out bit from the I/O port

Name of command – query	Command code	Parameters
C_ReadPort	0x72	PortNr

PortNr=1,2

Name of command – response	Response code	Parameters
A_ReadPort	0x73	Bit, OperationCode

Bit=00 for read-out value L
=01 for read-out value H
OperationCode –always is 0xff
This operation sets given port as the "input" (high impedance) automatically.
After switching the power on, both of the ports operate in the "input" mode.

Reading out the software version of Q5M-005 module

Name of command – query	Command code	Parameters
C_SoftwareVersion	0xfe	-

Name of command – response	Response code	Parameters
A_SoftwareVersion	0xff	Dane1..n, OperationCode

Dane1..n – software version written in ASCII code
OperationCode –always is 0xff

Calculation the CRC value

The CRC value is calculated from equation x^16+x^12+x^5+1 with initial value equal to 0x0000. The CRC value is calculated in virtue of all the bytes except of CRCH and CRCL.
Example of calculation of CRC value, written in C language:

```
void LiczCRC2(unsigned char *ZAdr, unsigned short *DoAdr,  unsigned char Ile)
{
int     i,NrBajtu;
 unsigned short C;
       *DoAdr=0;
       for (NrBajtu=1;NrBajtu<=Ile;NrBajtu++,ZAdr++)
       {
             C=((*DoAdr>>8)^*ZAdr)<<8;
             for (i=0;i<8;i++)
                   if (C&0x8000) C=(C<<1)^0x1021;
                   else C=C<<1;
             *DoAdr=C^(*DoAdr<<8);
       }

}
```

where:
*Zadr - is the data first byte flag
Ile - informs how many data bytes will be used for calculation
*DoAdr - is the flag for the calculated CRC value

Examples of Q5 transponder operation with the help of Q5M-005

Foundations:

- The messages are sent as broadcast (to the all modules in the network, AdresModu³u=ff).

Typical command frame:

module address	frame length	command	data	CRCH,CRCL
ff	XX	XX	XX XX XX XX	XX XX

- All write commands are executed as reversible ones (Lock=00).

Typical command frame:

module address	frame length	command	data	CRCH,CRCL
ff	XX	XX	XX XX XX **00**	XX XX

- Assume that, it has been assigned before to the reader an address 01 using the C_SlaveAddressSet function. It means that the reader with the address 01 will respond.

Typical response frame:

module address	frame length	response	data	operation code	CRCH,CRCL
01	XX	XX	XX	XX	XX XX

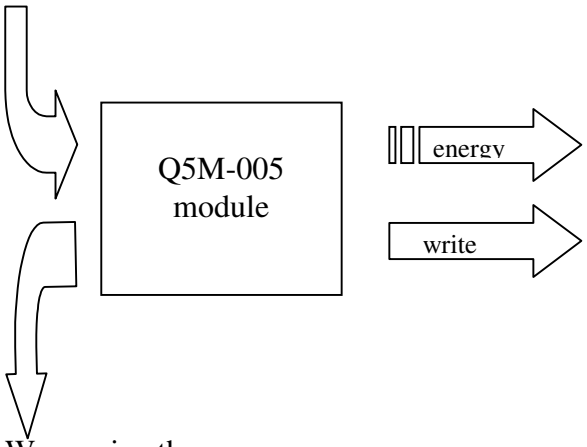
High level function operation
Example 1 Unique write

We are to write the Q5 transponder as a Unique transponder with number e1 e2 e3 e4 e5 and to check the correctness of that write.

For this purpose we can use two high level functions C_HL_UniqueWrite and C_HL_UniqueRead.

We send the string to the Q5M-005 module:

module address	frame length	command	data	CRCH,CRCL
ff	0b	00	e1 e2 e3 e4 e5 00	67 05



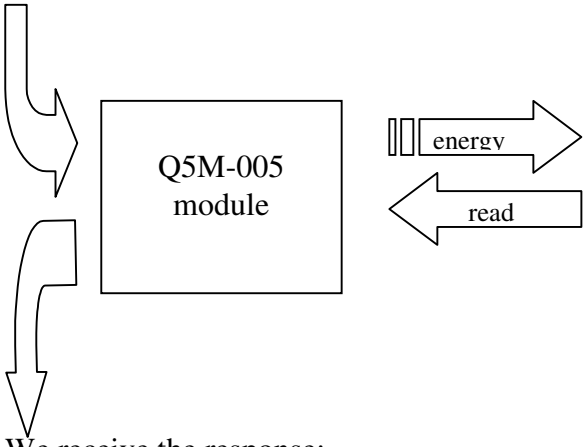
sector no.	Q5 transponder sectors			
0	60	01	F0	04
1	e1 e2 e3 e4 e5 including Unique conformed control sums			
2				
3				
4				
5				
6				
7				

We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	0b	01	-	ff	e9 d5

To verify reading correctness of the sent string:

module address	frame length	command	data	CRCH,CRCL
ff	05	02	-	10 d4



Sector no.	Q5 transponder sectors			
0	60	01	F0	04
1	e1 e2 e3 e4 e5 including Unique conformed control sums			
2				
3				
4				
5				
6				
7				

We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	0b	03	e1 e2 e3 e4 e5	ff	c6 69

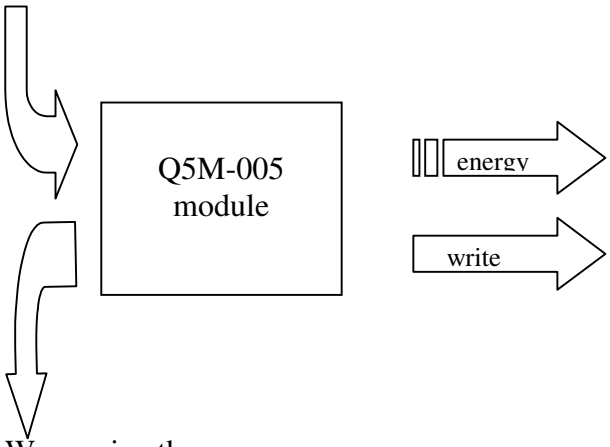
The read-out number is the same as write one. It means that writing process is correct.

Example 2 Sector write

We are to write the sector no. 3 as a c1 c2 c3 c4 and check if that write process is correct. For this purpose we can use two high level functions _HL_Q5SectorWrite and C_HL_Q5SectorRead.

We send the string to Q5M-005 module:

module address	frame length	command	data	CRCH,CRCL
ff	0b	10	c1 c2 c3 c4 03 00	66 5e



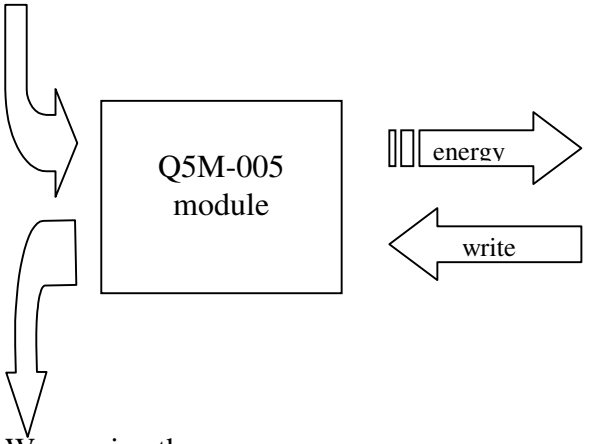
Sector no.	Q5 transponder sectors			
0				
1				
2				
3	c1	c2	c3	c4
4				
5				
6				
7				

We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	06	11	-	ff	ea a6

To verify reading correctness of the sent string:

module address	frame length	command	data	CRCH,CRCL
ff	06	12	03	ac 71



Sector no.	Q5 transponder sectors			
0				
1				
2				
3	c1	c2	c3	c4
4				
5				
6				
7				

We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	0a	13	c1 c2 c3 c4	ff	1c 1b

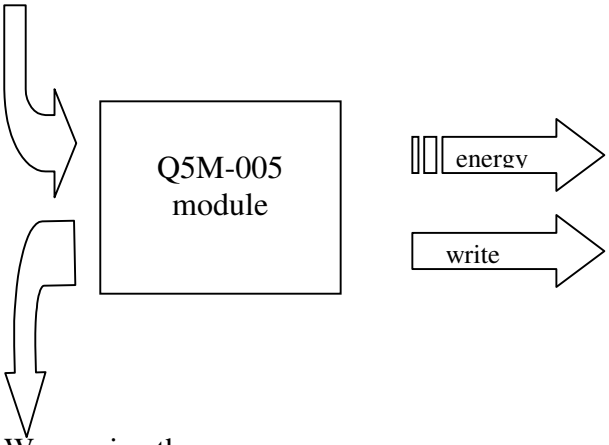
The read-out number is the same as write one. It means that writing process is correct.

Example 3 Password protection

We are to protect Q5 transponder with password.
For this purpose configure the sector no. 0 properly.
To the transponder would require the password, the value of 60 01 fc 04 must have been written to the sector no. 0. But remember to set the password saved in the sector no. 7 first. Let our password be the 01 02 03 04.

We send the setting password string to the Q5M-005 module:

module address	frame length	command	data	CRCH,CRCL
ff	0b	10	01 02 03 04 07 00	b2 41



Sector no.	Q5 transponder sectors			
0				
1				
2				
3				
4				
5				
6				
7	01	02	03	04

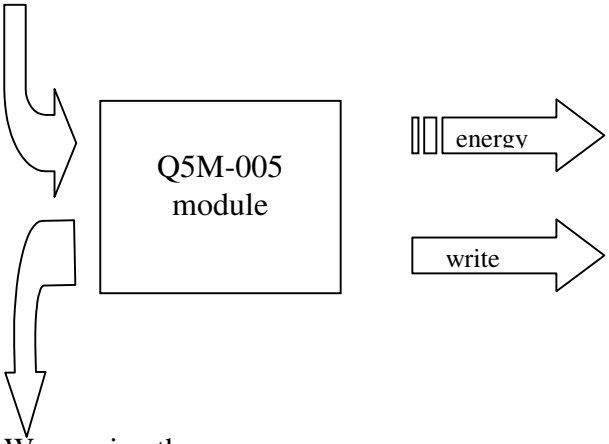
We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	06	11	-	ff	ea a6

(Verify the password write - C_HL_Q5SectorRead)

We send the configuration setting string to the module Q5M-005:

module address	frame length	command	data	CRCH,CRCL
ff	0b	10	60 01 fc 04 00 00	94 1f



Sector no.	Q5 transponder sectors			
0	60	01	fc	04
1				
2				
3				
4				
5				
6				
7	01	02	03	04

We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	06	11	-	ff	ea a6

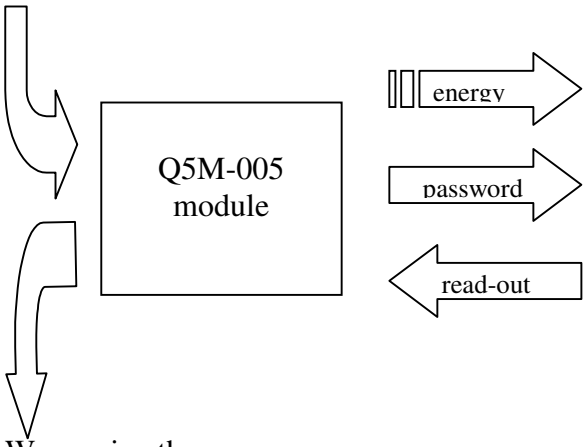
If the write is correct, we will use only the password for access to the transponder next time.

Example 4 Read-out with password

We are to read the sector no. 7 of transponder protected with 01 02 03 04 password.
For this purpose you can use high level function C_HL_WithPasswordQ5SectorRead.

We send the sector number for read-out and the password to the Q5M-005 module:

module address	frame length	command	data	CRCH,CRCL
ff	0a	22	07 01 02 03 04	b3 9e



Sector no.	Q5 transponder sectors			
0				
1				
2				
3				
4				
5				
6				
7	Written password			

We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	0a	23	01 02 03 04	ff	83 28

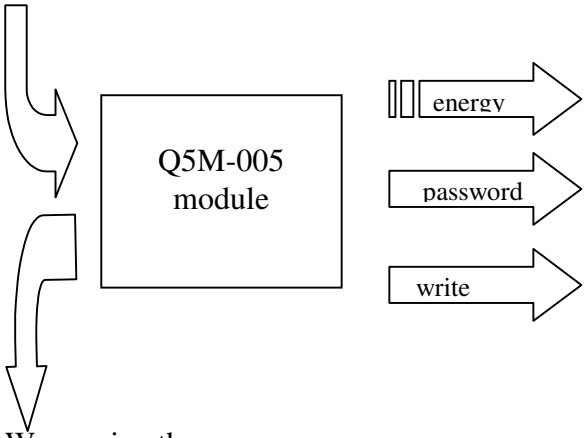
That means, that we have red the sector with the password.

Example 5 Removing the password

We are to unprotect Q5 transponder, which is secured with 01 02 03 04 password.
For this purpose, we should configure sector no. 0 properly.
To the transponder will not require the password, write the value of 60 01 f0 04 to the sector no. 0.

We send the new configuration and password to the Q5M-005 module:

module address	frame length	command	data	CRCH,CRCL
ff	0f	20	60 01 f0 04 00 01 02 03 04 00	52 b5



Sector no.	Q5 transponder sectors			
0	60	01	f0	04
1				
2				
3				
4				
5				
6				
7	Written password			

We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	06	21	-	ff	ef 33

If the write process is correct, we won't need a password for access to the transponder any longer.

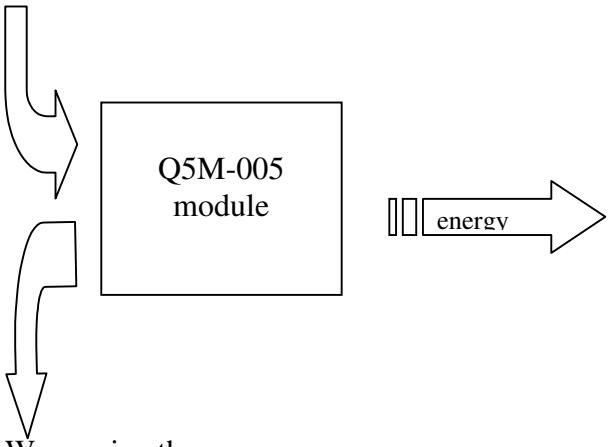
Low level function operation

Example 6 Sector decrementation

We are to decrement the sector no. 3 of the transponder.
Assuming that, the value of 44513 is written into sector no. 3 and it is equal to ade1 in hexadecimal code.

We switch the antenna generated field on:

module address	frame length	command	data	CRCH,CRCL
ff	05	30	-	06 c5



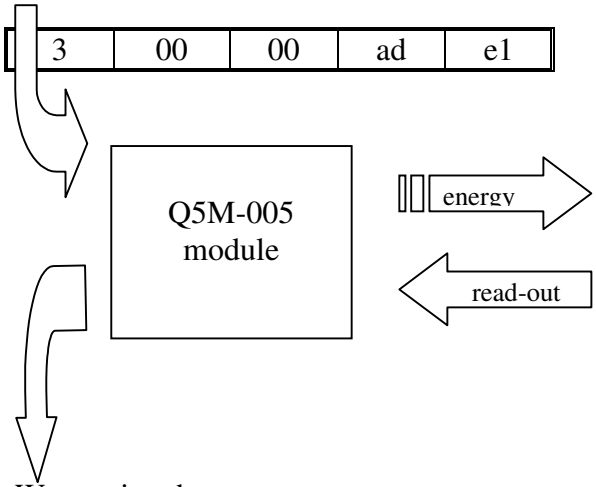
Sector no.	Q5 transponder sectors			
0				
1				
2				
3	00	00	ad	e1
4				
5				
6				
7				

We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	06	31	-	ff	ec 40

We read-out the sector no. 3:

module address	frame length	command	data	CRCH,CRCL
ff	06	42	03	a2 ce



Sector no.	Q5 transponder sectors			
0				
1				
2				
4				
5				
6				
7				

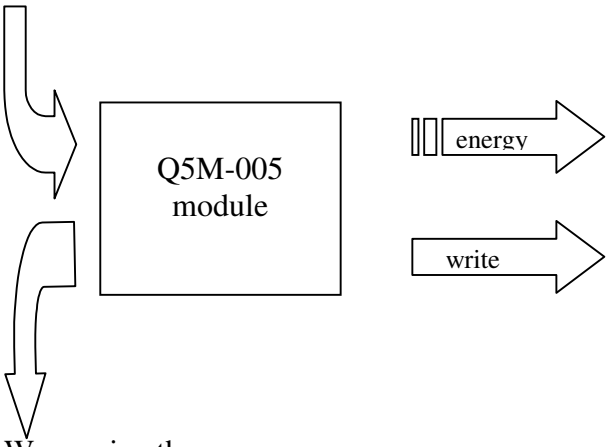
We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	0a	43	00 00 ad e1	ff	d2 d3

The user application layer decrements read-out value ade1-1=ade0

We write the decremented value:

module address	frame length	command	data	CRCH,CRCL
ff	0b	40	00 00 ad e0 03 00	a1 ec



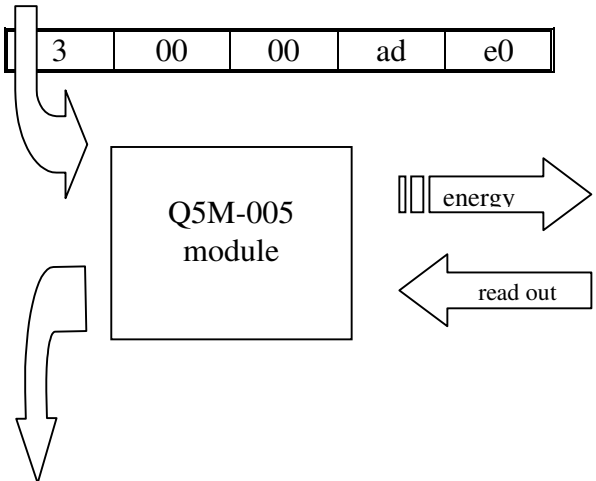
Sector no.	Q5 transponder sectors			
0				
1				
2				
3	00	00	ad	e0
4				
5				
6				
7				

We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	06	41	-	ff	e4 19

In that case to verify the write it is recommended to read-out the sector.
We read out the sector no. 3:

module address	frame length	command	data	CRCH,CRCL
ff	06	42	03	a2 ce



Sector no.	Q5 transponder sectors			
0				
1				
2				
4				
5				
6				
7				

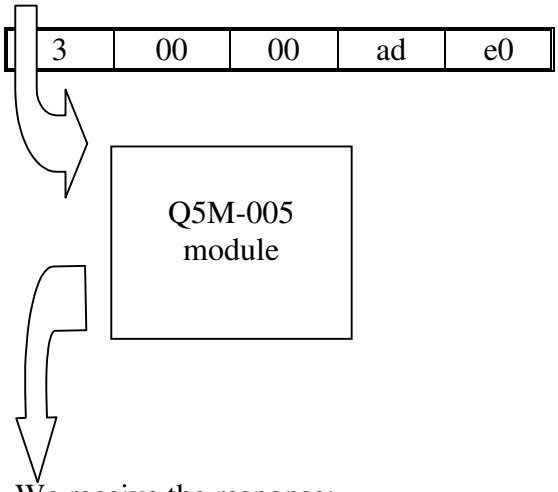
We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	0a	43	00 00 ad e0	ff	e1 e2

It means that decrementation of sector no. 3 has been finished successfully.

We switch the antenna produced field off:

module address	frame length	command	data	CRCH,CRCL
ff	05	32	-	26 87



Sector no.	Q5 transponder sectors			
0				
1				
2				
4				
5				
6				
7				

We receive the response:

module address	frame length	command	data	operation code	CRCH,CRCL
01	06	33	-	ff	92 45

NETRONIX products overview is available on website:
http://www.netronix.pl/