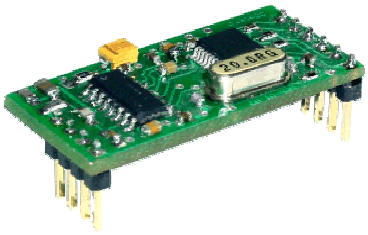
NETRONIX

Technical Data Sheet

H1M-005-p

H1M005p-doc-01.02
In reference to H1M005-c-01.06



Contents

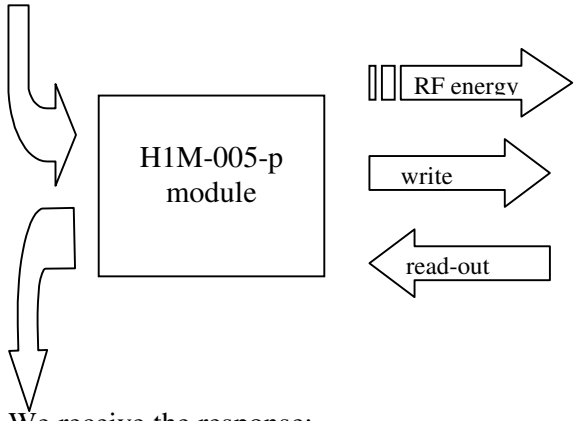
Contents 2
Introduction 3
General specification 3
Pin diagram 4
Connection diagram 4
The frame format of serial transmission 5
The general response frame format from the reader 5
The transponder HITAG1 description 6
High-level level commands 7
  Write of one side of the transponder 7
  Read-out of one side of the transponder 7
Low level commands 8
  Switching on the antenna electromagnetic field 8
  Switching off the antenna electromagnetic field 8
  Selecting the one transponder of many transponders 8
  Writing the one side of the transponder 8
  Reading out of the one side of the transponder 9
  Setting the transponder into sleep mode 9
  Writing the bit to the I/O port 9
  Reading out the bit from the I/O port 9
Additional commands 10
  Setting the gain of receiving path for the transponder signals 10
  Setting the address of the H1M-005-p module RSXXX bus 10
  Reading out the software version of the H1M-005-p module 10
Calculation the CRC value 11
Examples of the Hitag1 transponder operation with the help of H1M-005-p module 12
Work with high level functions 12
  Example 1 Writing the sector of the transponder 12
Work with low level functions 13
  Example 2 Writing the two transponders existing in the field 13

Introduction

The H1M-005-p module operates on principle of the contact-less information writing/reading from/to the HITAG1 (RFID) transponders in the „plain" mode. Data is transmitted via RS-232 interface compatible with TTL voltage level.
The module operates on the principle:
query (from the master unit - host) - action (of the module) - response (of the module).

We send the query-response to the module H1M-005-p:

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



Page No.	The transponder HITAG1 memory			
0	8b	8b	8b	8b
1	8b	8b	8b	8b
2	8b	8b	8b	8b
3	8b	8b	8b	8b
⋮	⋮	⋮	⋮	⋮
60	8b	8b	8b	8b
61	8b	8b	8b	8b
62	8b	8b	8b	8b
63	8b	8b	8b	8b

We receive the response:

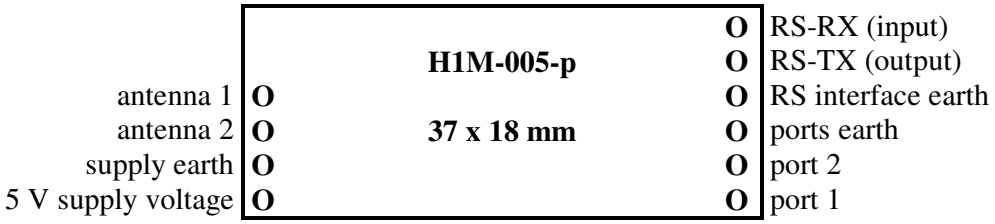
module address	frame length	response	data	operation code	CRCH,CRCL
xx	xx	xx	xx xx	xx	xx xx

The module comprises two user (1-bit) ports, with reading and writing possibility.
Connect an air coil antenna to the H1M-005 module. The antenna will produce an electromagnetic field and supply a transponder located in the field.

General specification

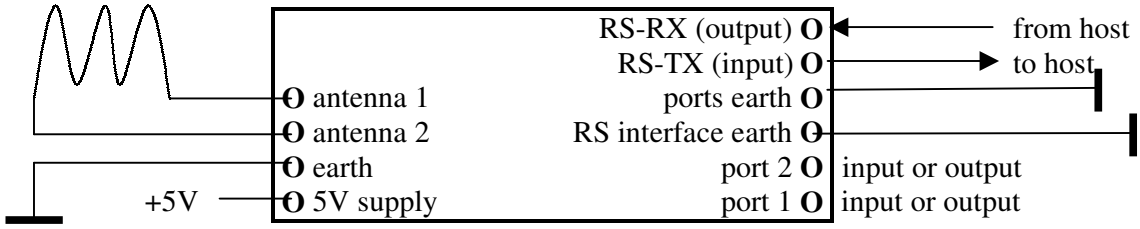
Supply voltage Uz	4.1...5.5 V
Supply current	5...55 mA
Module rated operating radio frequency	125 kHz
Baud rate of data received from transponder	4 kb/s
Baud rate of data sent to the transponder	5.2 kb/s
Output current capacity: port1, port2 and RS-TX	5 mA
Transporter read / write distance	depending on the antenna used: up to 20 cm
Antenna	external +-5%
Transmission	.9600 b/s, 8 data bits, 1 stop bit, no parity, with voltage levels comply TTL format

Pin diagram



Module pins – element side view

Connection diagram



The frame format of serial transmission

General command frame format for the reader

Module address	Frame length	Command	Parameters1..n	CRCH	CRCL
1 byte	1 byte	1 byte	n bytes	1 byte	1 byte

Where:

Module address – the unique module address in the system

If:

Module address = 0 - no module will respond

Module address = 0xFF - all modules in network will respond in the same time

Frame length – the total number of the frame bytes

Command - even value

Parameters1..n - exist optionally and depend on command

CRCH, CRCL - MSByte and LSByte of CRC16 respectively

The general response frame format from the reader

Module address	Frame length	Response	Parameters 1..n	Operation code	CRC H	CRC L
1 byte	1 byte	1 byte	n bytes	1 byte	1 byte	1 byte

Where:

Module address - assigned the real address of responding module

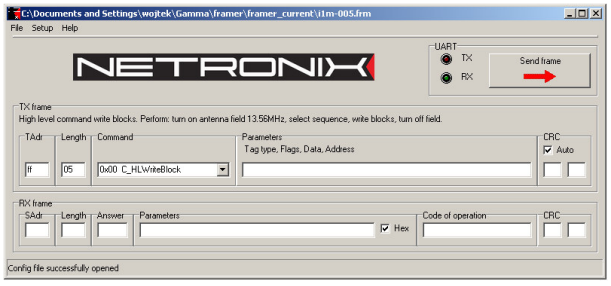
Frame length – the total number of the response frame bytes

Response = Command + 1 (odd value)

Parameters 1..n - exist optionally and depend on command

Operation code - informs about correctness of executed command

CRCH, CRCL - MSByte and LSByte of CRC16 respectively



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

The transponder HITAG1 description

The HITAG1 transponder comprises 16 blocks, and each of the blocks comprises four pages. One page contains four bytes. It gives 63 pages, four bytes each.

Two of first blocks (blocks: 0 and 1, pages: 0...7) are reserved as a configuration blocks and include:
the serial number of the transponder, blocks configuration, keys A and B, reader passwords A and B and transponder passwords A and B.
The user uses other blocks.
Depending on the chosen configuration of 6 blocks (blocks: 2...7 i.e. pages: 8...31), we can write or read only: 8 blocks (blocks: 8...15 i.e.. pages: 32...63) (access type is non-configurable).
Because of data evidence, the transponder memory is divided into blocks.
The configuration memory is divided in this way:
The pages which contain keys and passwords (pages: 2...7) are of „secret" type. The pages which contain serial number and blocks configuration (pages 0,1) are of „public" type.
The user memory is divided in this way:
Blocks 2...3 – „secret"
Blocks 4...7 – „secret" or „public" depending on configuration
Blocks 8...15 – „public"
The user has an access to the „secret" blocks by the help of special procedures, but in case of H1M-005-p module that is impossible.

public	block 0	page 0	Serial Number	ro
		page 1	Configuration	r/w or ro
secret	block 0…1	page 2…7	Keys and passwords	wo or 0 r/w or 0
	block 2…3		User data	r/w or ro
secret or public	block 4…7		User data	
public	block 8…15		User data	r/w

ro – (read only) the user can read-out this page only
wo – (write only) the user can write this page only
r/w – (read/write) the user can write and read-out this page only
0 – the user can not read out nor write this page

High-level level commands

With high level commands, you can fully communicate with the transponder Hitag1. It means, that switching the field on, selection the transponder, proper process and switching the field off will be done automatically. The proper process can consist of many writes and/or read-outs. Using many high level functions, we extend the excess time to the sectors and the same time we cannot to generate many writes/read-outs in case of complex functions.

Meaning of the descriptions:

PageAddr..... Informs, to which side of the transponder command concerns. It is the value =(0..0x3f), and the „public" type pages are from (0...1) and (0x20...0x3f) ranges and from (0x10...0x1f) range optionally.

OperationCode... informs if H1M-005-p module executed the command correctly.

Write of one side of the transponder

Name of command - query	Command code	Parameters
C_HL_PageWrite	0xa0	Data1...4, PageAddr

Data1...4 – written data
PageAddr =(0...0x3f)

Name of command – response	Response code	Parameters
A_HL_PageWrite	0xa1	ID1...4,OperationCode

ID1...4 – the transponder ID numbers, which have been selected and written to.
(ID1...4 numbers exist optionally and depend on if the operation is correct or not)
OperationCode – 0xff – the execution of the operation is correct.

Read-out of one side of the transponder

Name of command - query	Command code	Name of command - query
C_HL_PageRead	0xa2	PageAddr

PageAddr =(0...0x3f)

Name of command – response	Response code	Parameters
A_HL_PageRead	0xa3	ID1...4, Data1...4, OperationCode

ID1...4 – the transponder ID numbers, which have been selected and red-out.
Data1...4 – the red-out data of the page
(ID1...4 and Data1...4 - exist optionally depending on the operation is correct or not)
OperationCode – 0xff - the execution of the operation is correct.

Low level commands

The level commands can be used in freely sequences without multiple on/off switching of the field.

Switching on the antenna electromagnetic field

Name of command – query	Command code	Parameters
C_TurnOnAntennaPower	0x10	-

Name of command – response	Response code	Parameters
A_ TurnOnAntennaPower	0x11	OperationCode

OperationCode –0xff always

Switching off the antenna electromagnetic field

Name of command – query	Command code	Parameters
C_TurnOffAntennaPower	0x12	-

Name of command – response	Response code	Parameters
A_TurnOffAntennaPower	0x13	OperationCode

OperationCode –0xff - always

Selecting the one transponder of many transponders

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

Name of command – response	Response code	Parameters
A_Select	0x31	ID1...4, OperationCode

ID1...4 – the ID no. of the selected transponder
(ID1...4 - exist optionally and depend on the operation is correct or not)
OperationCode – 0xff – execution of the operation is correct

Writing the one side of the transponder

Name of command – query	Command code	Parameters
C_PageWrite	0x50	Data1...4, PageAddr

Data1...4 – data for writing
PageAddr – the target page address

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

OperationCode – 0xff execution of the operation is correct

Reading out of the one side of the transponder

Name of command – query	Command code	Parameters
C_PageRead	0x52	PageAddr

PageAddr – the source page address

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

Data1...4 – red-out data
OperationCode – 0xff execution of the operation is correct

Setting the transponder into sleep mode

Name of command – query	Command code	Parameters
C_Halt	0x40	-

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

OperationCode – 0xff execution of the operation is correct

Writing the bit to the I/O port

Name of command – query	Command code	Parameters
C_WritePort	0xE0	PortNr, Bit

PortNr=1,2
Bit=0,1

Name of command – response	Response code	Parameters
A_WritePort	0xE1	OperationCode

OperationCode – 0xff always
After switching on of the supply, both ports operate in the "input" mode.

Reading out the bit from the I/O port

Name of command – query	Command code	Parameters
C_ReadPort	0xE2	PortNr

PortNr=1,2

Name of command – response	Response code	Parameters
A_ReadPort	0xE3	Bit, OperationCode

Bit=00 for the red-out value L
=01 for the red-out value H
OperationCode – 0xff always

Additional commands

Setting the gain of receiving path for the transponder signals

Name of command – query	Command code	Parameters
C_GainSet	0xf0	Gain

Gain – 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	0xf1	OperationCode

OperationCode – 0xff always

Setting the address of the H1M-005-p module RSXXX bus

Name of command – query	Command code	Parameters
C_SlaveAddressSet	0xf2	NewAdr

NewAdr – 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	0xf3	OperationCode

OperationCode – 0xff always

Reading out the software version of the H1M-005-p 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 *FromAddr, unsigned short *ToAddr,  unsigned char Many)
{
int     i,NrBajtu;
 unsigned short C;
       *ToAddr=0;
       for (NrBajtu=1;NrBajtu<=Many;NrBajtu++,FromAddr++)
       {
             C=((*ToAddr>>8)^*FromAddr)<<8;
             for (i=0;i<8;i++)
                   if (C&0x8000) C=(C<<1)^0x1021;
                   else C=C<<1;
             *ToAddr=C^(*ToAddr<<8);
       }

}
```

where:

*FromAddr - is the data first byte flag
Many - informs how many data bytes will be used for calculation
*ToAddr - is the flag for the calculated CRC value

Examples of the Hitag1 transponder operation with the help of H1M-005-p module

Foundations:

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

The typical command frame:

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

The typical response frame:

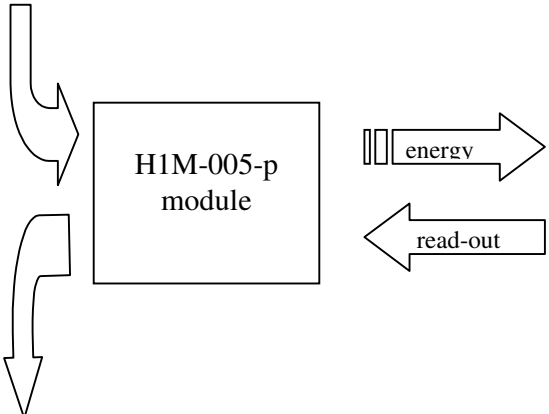
module address	frame length	response	data	operation code	CRCH,CRCL
01	XX	XX	XX	XX	XX XX

Work with high level functions

Example 1 Writing the sector of the transponder

We are to write the page with the 3f address the following data e1 e2 e3 e4 e5 and to check the correctness of that write.
For this purpose you can use two high level functions C_HL_PageWrite and C_HL_PageRead.
We send the sequence to the H1M-005-p module:

module address	frame length	command	data	CRCH,CRCL
ff	0a	A0	e1 e2 e3 e4 3f	9c 5d



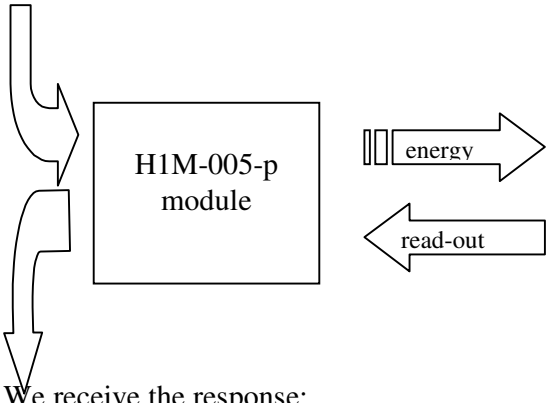
Page No.	HITAG1 transponder memory			
0				
1				
2				
3				
⋮	⋮	⋮	⋮	⋮
3c				
3d				
3e				
3f				

We receive the response:

module address	frame length	response	data	operation code	CRCH,CRCL
01	0a	A1	ID1..4	ff	XX XX

To verify the write correctness, send the sequence:

module address	frame length	command	data	CRCH,CRCL
ff	06	A2	3f	45 a3



Page No.	HITAG1 transponder memory			
0				
1				
2				
3				
⋮	⋮	⋮	⋮	⋮
3c				
3d				
3e				
3f	e1	e2	e3	e4

We receive the response:

module address	frame length	response	data	operation code	CRCH,CRCL
01	0e	A3	ID1...4, e1 e2 e3 e4	ff	XX XX

The data is very same as the written data, which means write is correct.

Work with low level functions

Example 2 Writing the two transponders existing in the field

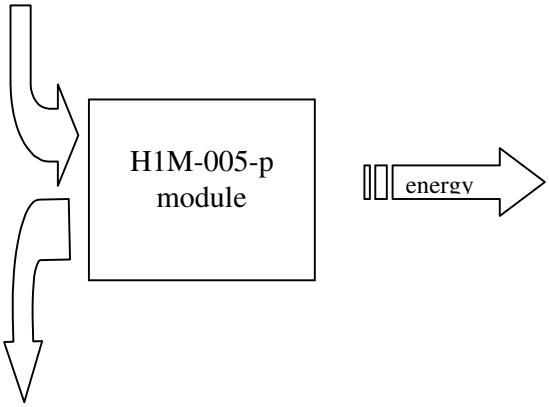
We are to write the sectors with 0x3E address in both of transponders.
For this purpose:

- switch the antenna field on
- select one of the transponders, write the transponder, set the transponder into sleep mode
- select the next transponder, write the transponder, set the transponder into sleep mode
- switch the antenna filed off

For this purpose, you can use the functions: C_TurnOnAntennaPower, C_Select, C_PageWrite, C_Halt and C_TurnOffAntennaPower.

We send the sequence to the H1M-005-p module:

module address	frame length	command	data	CRCH,CRCL
ff	05	10	-	22 a7



Page No.	HITAG1 transponder memory			
0				
1				
2				
3				
⋮	⋮	⋮	⋮	⋮
3c				
3d				
3e				
3f				

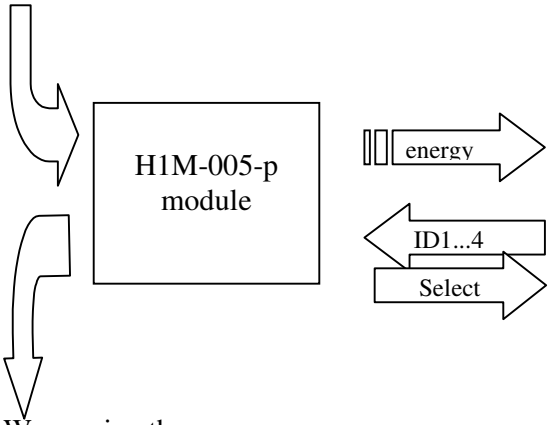
We receive the response:

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

At this moment, the antenna field is switched on.

We select the transponder:

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



Page No.	HITAG1 transponder memory			
0				
1				
2				
3				
⋮	⋮	⋮	⋮	⋮
3c				
3d				
3e				
3f				

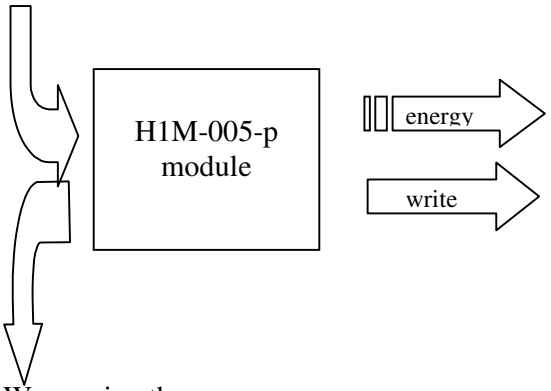
We receive the response:

module address	frame length	response	data	operation code	CRCH,CRCL
01	0A	31	ID1..4	ff	XX XX

We have selected the transponder one of the transponders.

We write data d1 d2 d3 d4 to the sector 3e

module address	frame length	command	data	CRCH,CRCL
ff	0a	50	d1 d2 d3 d4 3e	fd f7



Page No.	HITAG1 transponder memory			
0				
1				
2				
3				
⋮	⋮	⋮	⋮	⋮
3c				
3d				
3e				
3f				

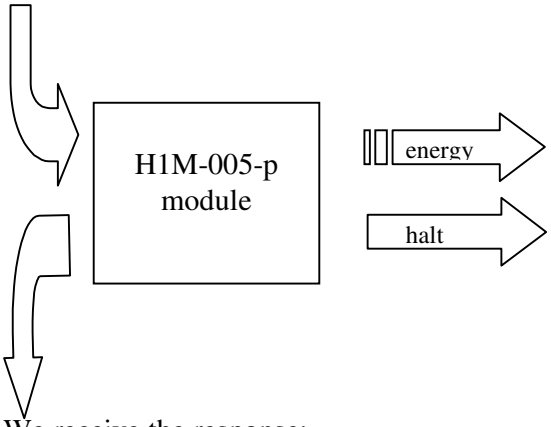
We receive the response:

module address	frame length	response	data	operation code	CRCH,CRCL
01	06	51	-	ff	e7 6a

The transponder is written in.

To select the next transponder the first one should be set into sleep mode.

module address	frame length	command	data	CRCH,CRCL
ff	05	40	-	78 52



Page No.	HITAG1 transponder memory			
0				
1				
2				
3				
⋮	⋮	⋮	⋮	⋮
3c				
3d				
3e				
3f				

We receive the response:

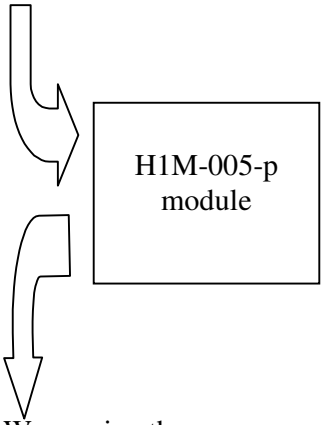
module address	frame length	response	data	operation code	CRCH,CRCL
01	06	41	-	ff	e4 19

The transponder is set into sleep mode.

To select the next transponder the first one should be set into sleep mode (as before).

The last step is switching the antenna field off.

module address	frame length	command	data	CRCH,CRCL
ff	05	12	-	02 e5



Page No.	HITAG1 transponder memory			
0				
1				
2				
3				
⋮	⋮	⋮	⋮	⋮
3c				
3d				
3e				
3f				

We receive the response:

module address	frame length	response	data	operation code	CRCH,CRCL
01	06	13	-	ff	8c c4

Latest news about NETRONIX products is available on website:
http://www.netronix.pl/