

Data Sheet

H2PROT.PDF

9 Pages

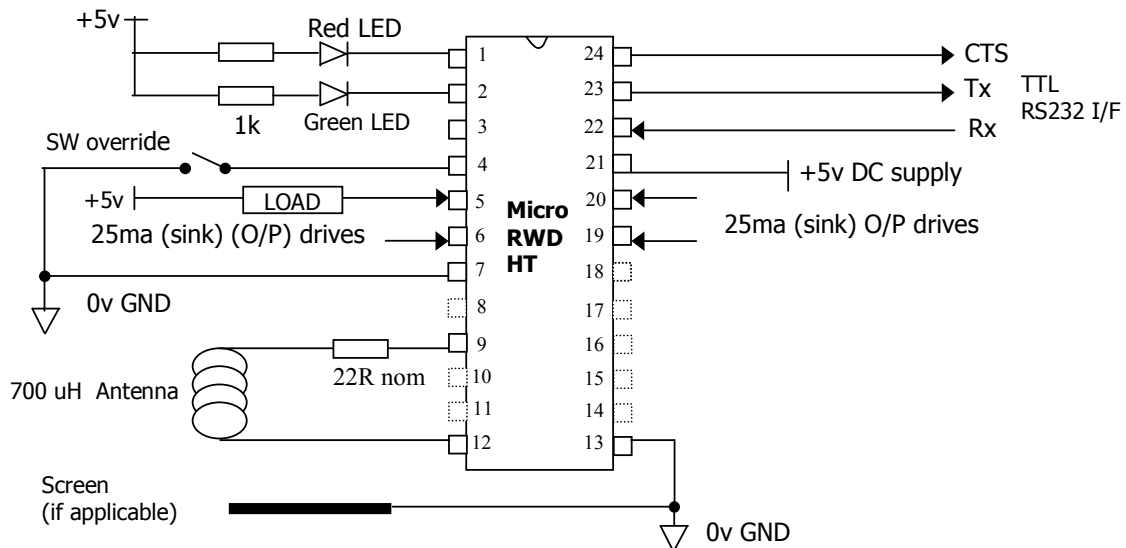
Last Revised 04/11/09

Micro RWD H2 Protocol

The MicroRWD H2 version is a complete reader and tag acceptance solution for Hitag 2 RF transponders. The solution only needs a 700uH antenna coil connected and 5v DC supply to be a fully featured read/write system. The module provides internal EEPROM memory for holding lists of authorised identity codes, a manual override switch facility and has LED drives to give visual indication of acceptance.

The RWD also has a TTL level RS232 interface that allows a host system to communicate with the RWD if necessary, so that system features can be customised, configurations changed and tag read/write data handled by the host system.

Typical application configuration for Micro RWD module



The Hitag 2 transponders provide 256 bits (32 bytes) of read/write EEPROM memory arranged as 8 partitioned 32 bit pages. An area of 128 bits (16 bytes) is open for general user data. The Hitag 2 transponders are configurable for different modes of operation and the MicroRWD H2 version supports the high security PASSWORD mode only. This feature uses two password codes stored both in the H2 transponder and the RWD that are mutually exchanged when a tag is brought into the RF field; the tag is only unlocked for read/write operations if these codes exactly agree.

The use of this Mutual Authentication process, encrypted communications and a pulsed RF field ensures that the MicroRWD H2 reader system is very secure.

ib technology

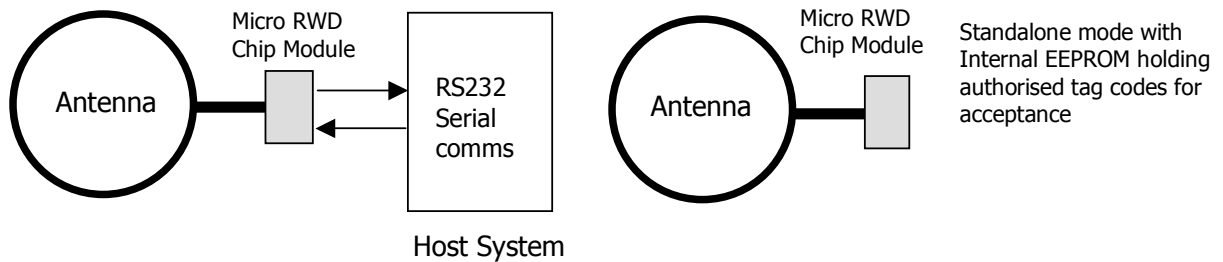
The MicroRWD is essentially a proximity system and a Read/Write range of up to 20cm can be achieved with the same level of reliable communication and EMC resilience. The unique AST (Adaptive Sampling) feature allows the RWD to continually adjust and re-tune the sampling to allow for inductive changes in the RF field, an essential feature for real-world reliability and robust operation. The communication protocol with the tags can achieve 4k bits/second of data transfer and the total time to read a 32-bit page takes less than 50ms.

The MicroRWD can be easily integrated into almost any application; when power (5v DC) is first applied to the board the red and green LEDs flash once to indicate successful power-up. The device can also check for broken or shorted antenna and can even detect badly tuned antennas; these problems are indicated by the red LED flashing continuously until the fault has been rectified.

The MicroRWD will normally have the red LED lit until a valid card or tag is brought into the RF field. If the tag is accepted as valid then the green LED is lit and the output drivers (OP0, OP1, OP2, OP3) are switched on. These outputs can be connected together to give up to 100ma of drive current for operating a relay etc. In addition, a switch input is provided for overriding the tag reading operation and switching the output drives directly.

(Hitag 2 is a trademark of Philips/NXP Semiconductors NV)

The Micro RWD has two basic modes of operation:-



Remote mode (connected to a host computer or microcontroller) and Standalone mode.

- 1) Remote mode involves connecting to a host serial interface. This is where the stored list of authorised identity codes can be empty, effectively authorising any HT2 transponder for subsequent read/write operations. A simple serial protocol allows a host system to communicate with the Micro RWD in order to program new authorised identity codes, change passwords and perform read/write operations to the tag itself.
- 2) Standalone mode is where the HT2 tag identity codes (serial number) are checked against a stored list of authorised codes. If an identity code is matched, the output drives and Green LED are enabled. Effectively standalone mode occurs when there is no host system communicating with the Micro RWD.

Supported transponder types

The Micro RWD H2 version is designed to communicate with Hitag 2 transponders configured in PASSWORD mode. Setting the HT2 transponder to any other configuration will render them inoperable with this system. The operation of the Micro RWD and Hitag 2 transponders is described in more detail at the end of this document.

The identification codes described in this text are regarded as the first four bytes (serial number or page 0) of the tag memory array.

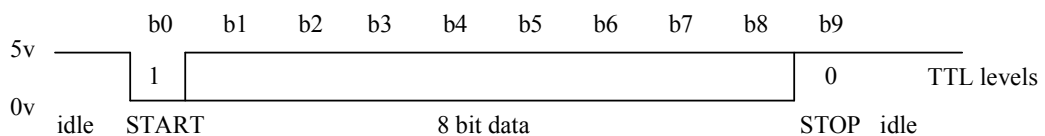
Serial Interface

This is a basic implementation of RS232. The Micro RWD does not support buffered interrupt driven input so it must control a BUSY (CTS) line to inhibit communications from the host when it is fully occupied with tag communication. It is assumed that the host (such as a PC) can buffer received data.

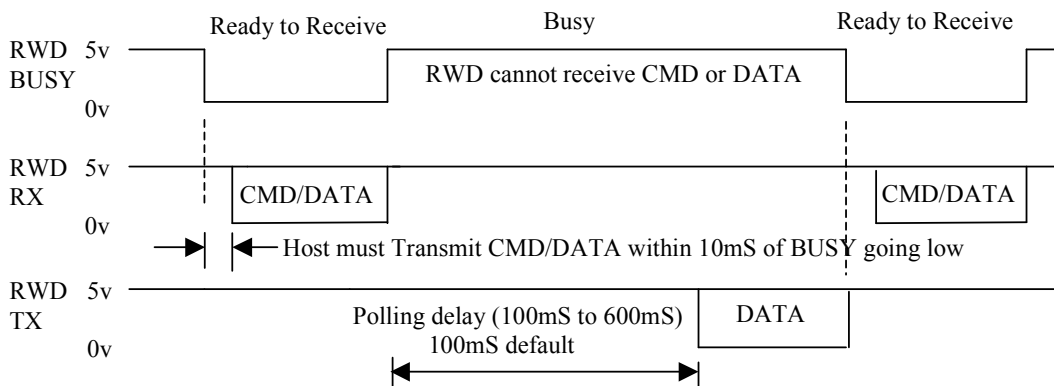
Tx, Rx and RTS signals from the Micro RWD are all TTL level and can be converted to +/-10v RS232 levels using an inverting level converter device such as the MAX202 (note the inversion of the TTL levels).

The serial communication system and protocol allows for a 10ms 'window' every Tag polling cycle indicated by the BUSY line being low. During this 'window' the host must assert the first start bit and start transmitting data. The BUSY goes high again 10ms after the last stop bit is received. NOTE that only one command sequence is handled at a time.

Transmitted or Received data byte, 9600 baud, 8 bit, 1 stop, No parity (104uS per bit)



RWD tag polling cycle and serial communication BUSY protocol



Command Protocol

The following commands are supported. The corresponding acknowledge code should be read back by the host and decoded to confirm that the command was received and actioned correctly. The serial bit protocol is 9600 baud, 8 bits, 1 stop, no parity (lsb transmitted first).

The status flags returned in the Acknowledge byte are as follows:

b7	b6	b5	b4	b3	b2	b1	b0	
1	1	1	1	1	1	1	1	
								EEPROM error (Internal EEPROM write error)
								Tag OK (Tag identity code matched to list and Password exchange successful)
								Rx OK (Tag communications and acknowledgement OK)
								RS232 error (Host serial communications error)
								RELAY Enabled flag
								HTRC (or Antenna fault) error flag

Note that bits 6 and 7 are fixed 1's so that an acknowledge code of D6 (Hex) would generally indicate no errors with a matched (or authorised) HT2 Tag present. Note also that only the relevant flags are set after each command as indicated in the following specification.

Write Tag

Command to write 4 bytes of data to HT2 32 bit page. If the write was unsuccessful (invalid tag or out of field) then Status flags in acknowledge byte indicate error.

	B7		B0						
Command:	0	1	0	1	0	1	1	1	(ASCII "W", 0x57)
Argument1:	x	x	x	x	x	N	N	N	(N = HT2 page address 0-7)
Argument2:	D	D	D	D	D	D	D	D	(D = msb data to write to HT2)
Argument3:	D	D	D	D	D	D	D	D	
Argument4:	D	D	D	D	D	D	D	D	
Argument5:	D	D	D	D	D	D	D	D	(D = lsb data to write to HT2)
Acknowledge:	1	1	F	F	F	F	F	X	(F = Status flags)

Note that PASSWORD exchange occurs for WRITE command.

If no tag present then acknowledge / status byte reply is 0xC0

If tag present but RWD PASSWORD check fails then acknowledge byte reply is 0xC0.

If tag present but TAG PASSWORD check fails then acknowledge byte reply is 0xC4.

If tag present and both PASSWORDS match then acknowledge reply is 0xD6.

Read Tag

Command to read 4 bytes of data from HT2 32 bit page. If the read was successful, indicated by acknowledge status flags then four bytes of tag data follow.

	B7		B0						
Command:	0	1	0	1	0	0	1	0	(ASCII "R", 0x52)
Argument1:	x	x	x	x	x	N	N	N	(N = HT2 page address 0-7)
Acknowledge:	1	1	F	F	F	F	F	X	(F = Status flags)

Data only follows if read was successful

Reply1:	D	D	D	D	D	D	D	D	(D = msb data to write to HT2)
Reply2:	D	D	D	D	D	D	D	D	
Reply3:	D	D	D	D	D	D	D	D	
Reply4:	D	D	D	D	D	D	D	D	(D = lsb data to write to HT2)

Note that PASSWORD exchange occurs for READ command.

If no tag present then acknowledge / status byte reply is 0xC0

If tag present but RWD PASSWORD check fails then acknowledge byte reply is 0xC0.

If tag present but TAG PASSWORD check fails then acknowledge byte reply is 0xC4.

If tag present and both PASSWORDS match then acknowledge reply is 0xD6 followed by 4-bytes of data.

Tag STATUS

Command to return Tag status. The acknowledge byte flags indicate general Tag status.

	B7		B0						
Command:	0	1	0	1	0	0	1	1	(ASCII "S", 0x53)
Acknowledge:	1	1	F	F	F	F	F	X	(F = Status flags)

Card UID

Command to return card status and UID (Unique Identifier or Serial number).

The acknowledge byte flags indicate general Tag status.

	B7		B0						
Command:	0	1	0	1	0	1	0	1	(ASCII "U", 0x55)
Acknowledge:	1	1	F	F	F	F	F	X	(F = Status flags)

Data only follows if card was selected OK with no errors detected.

Reply1:	D	D	D	D	D	D	D	D	(D =MS Byte of UID/Serial number from card)
Reply2:	D	D	D	D	D	D	D	D	
Reply3:	D	D	D	D	D	D	D	D	
Reply4:	D	D	D	D	D	D	D	D	(D =LS Byte of UID/Serial number from card)

Note that the CARD UID command works independently of the PASSWORD mode. The PASSWORD authentication only occurs for READ/WRITE operations.

Message

Command to return product and firmware identifier string to host.

	B7	B0	
Command:	0 1 1 1 1 0 1 0		(ASCII "z", 0x7A)
Reply:	"a IDE RWD H2 (SECx V1.xx) DD/MM/YY" 0x00		

Returned string identifies author, product descriptor, project name, firmware version no. and date of last software change. Note that the string is always NULL terminated. The string begins with a unique lower case character that can be used to identify a particular version of Micro RWD.

NOTE:

- 1) The serial communications uses hardware handshaking to inhibit the host from sending the Micro RWD commands while Tag interrogation is in progress.
- 2) Following the Read Tag command, if an error flag has been set in the Acknowledge code then there will be NO following data.
- 3) The serial communications system and protocol allows for a 10ms 'window' every Tag polling cycle indicated by the BUSY line being low. During this 'window' the host must assert the first start bit and start transmitting data. The BUSY goes high again 10ms after the last stop bit is received.
- 4) Only one command sequence is handled at a time.

Program EEPROM

The Micro RWD has some internal EEPROM for storing system parameters such as passwords and authorised identity codes. This command sequence allows individual bytes of the EEPROM to be programmed with new data. Note that due to the fundamental nature of these system parameters, incorrect data may render the system temporarily inoperable.

	B7	B0	
Command:	0 1 0 1 0 0 0 0		(ASCII "P", 0x50)
Argument1:	N N N N N N N N		(N = EEPROM memory location 0- 255)
Argument2:	D D D D D D D D		(D = data to write to EEPROM)
Acknowledge:	1 1 X F X X X F		(F = Status flags)

Internal EEPROM memory map

Byte 0: Tag Polling Rate (x 2.5ms)
Byte 1: RF ON/OFF lock (0x55 = ON, anything else = OFF, normally set to 0x55)
Byte 2: Reserved (Checksum)
Byte 3: Reserved
Byte 4: PASSWORD_RWD "M" (Sent to HT2)
Byte 5: PASSWORD_RWD "I"
Byte 6: PASSWORD_RWD "K"
Byte 7: PASSWORD_RWD "R"
Byte 8: Reserved
Byte 9: PASSWORD_TAG 0xAA (Reply from HT2)
Byte 10: PASSWORD_TAG "H"
Byte 11: PASSWORD_TAG "T"

Start of authorised tag codes. List is terminated with FF FF FF FF sequence.

List is regarded as empty (all identity codes valid) if first code sequence in list is (FF FF FF FF).

List can hold up to 60 identity codes (serial numbers).

Byte 12: 0xFF Empty list
Byte 13: 0xFF
Byte 14: 0xFF
Byte 15: 0xFF

Byte 16: (MSB) Tag identity code
Byte 17:
Byte 18:
Byte 19: (LSB)

Byte 20: (MSB) Tag identity code
Byte 21:
Byte 22:
Byte 23: (LSB)

-
-
-
-

Byte 255: Last Internal EEPROM location

Method of Operation

The Micro RWD reader only allows full Read/Write access to the Hitag 2 transponders if TWO levels of security have both succeeded. During the initial communication with the H2 tag the serial number (identity code) is acquired (4-bytes from H2 page 0). The Micro RWD internal EEPROM is then checked to see if this serial number is stored in the authorisation list located from byte 12 onwards. If the tag serial number is matched or the list is empty then the tag has passed the first security check (If the Micro RWD has 0xFF FF FF FF stored at EEPROM locations 12 to 15 then the list is treated as empty and all Hitag 2 tags are accepted through the first security level).

The serial number can be accessed at this stage using the CARD UID command.

For READ and WRITE commands a second security check is automatically performed by mutually exchanging two Passwords between the RWD and the Hitag2 tag. If the PASSWORD exchange operation is successful then memory access is allowed and the READ and WRITE commands can proceed.

The first password is four bytes long (32 bits) and is called the "RWD PASSWORD" which is located at page 1 in the tag memory. The second password is three bytes long (24 bits) and is called the "TAG PASSWORD". It is located at page 3 in the tag from the second to the forth byte, the first byte in page 3 is the tag configuration byte which controls the basic mode of operation. This should be left as 06 (hex) until the system is fully understood. The configuration byte bit definitions are described at the end of this document.

The RWD and TAG PASSWORDS are also stored in the Micro RWD EEPROM to allow the reader to verify the tag, and the tag to mutually verify the reader.

For READ and WRITE commands the Micro RWD reader sends the RWD PASSWORD to the H2 tag first, which then checks this code against it's own RWD PASSWORD. If they agree then the H2 tag sends it's TAG PASSWORD to the reader which then checks the code against it's stored TAG PASSWORD. If they agree then the second security level has been passed and the READ/WRITE commands can proceed. The use of these two levels of security makes the Hitag 2 tags very suitable for secure data storage or for RF identification applications such as locks and access control.

Hitag 2 Memory Map (PASSWORD mode)

The memory of the Hitag 2 transponder consists of 256 bits of very low power EEPROM memory which is organised into 8 pages of 32 bits (4 bytes) each.

Page No.	Content (32 bit words/ 4 bytes)
0	Serial number
1	Password RWD (Default = "MIKR" = 4D 49 4B 52 hex)
2	Reserved
3	8 bit Configuration, 24 bit Password TAG (Default = 06 AA 48 54 hex)
4	Read/Write page
5	Read/Write page
6	Read/Write page
7	Read/Write page

Hitag 2 Configuration Byte

The 8 bit configuration byte located at the start of page 3 defines the basic mode of the Hitag 2 transponder and whether certain parts of it's memory are locked or open for Read/Write operations. Note that the MicroRWD H2 only supports PASSWORD mode and can communicate with Hitag 2 tags with the **configuration byte = 0x06** (or 0x46 with configuration and TAG Password locked).

CONFIGURATION OR PASSWORDS MUST NOT BE CHANGED UNLESS THE OPERATION OF THE HITAG 2 TRANSPONDER IS UNDERSTOOD.

Configuration Byte (Page 3, byte 0)

b7	b6	b5	b4	b3	b2	b1	b0
				0	1	1	0
				0 = Page 6 and 7 read/write			
				1 = Page 6 and 7 read only			
				0 = Page 4 and 5 read/write			
				1 = Page 4 and 5 read only			
				0 = Page 3 read/write			
				1 = Page 3 read only, Configuration and TAG Password FIXED , THIS BIT IS OTP			
				0 = Page 1 an 2 read/write			
				1 = Page 1 no read/no write, Page 2 (RWD Password) read only, THIS BIT IS OTP			

No responsibility is taken for the method of integration or final use of Micro RWD

More information on the Micro RWD and other products can be found at the Internet web site:

<http://www.ibtechnology.co.uk>

Or alternatively contact IB Technology by email at:

sales@ibtechnology.co.uk