ib technology

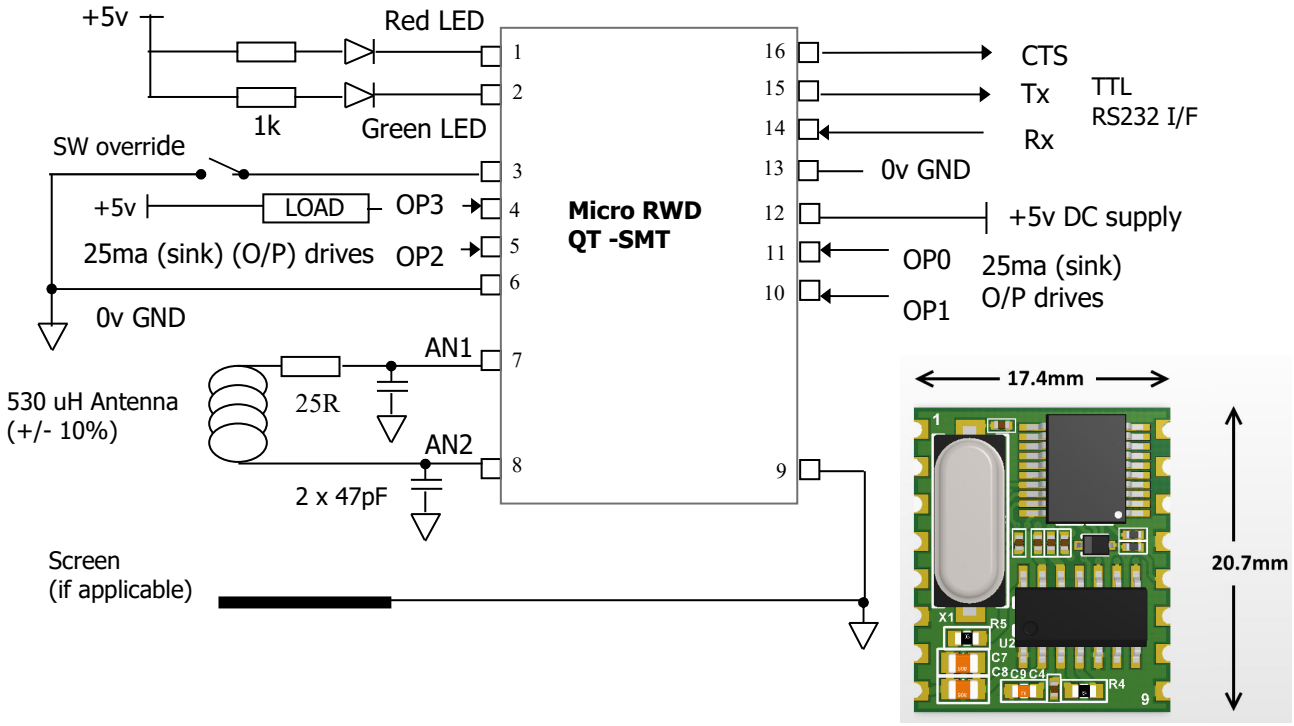
Data Sheet

RWD_QT_LP_SMT.pdf
20 Pages
Last Revised 07/10/16

Micro RWD Quad-Tag SMT (low power) Reader

The MicroRWD QT (Quad-Tag) SMT low-power version is a complete 125kHz reader solution for Hitag 1, Hitag S256/S2048 (Plain Memory mode), Hitag 2 (Password mode), EM400X/4102 and MCRF200I/123 passive RFID transponder types. The module is packaged as a 16-pin low-profile SMT device and only needs a 530 µH antenna coil connected and 5v DC supply to be a fully featured read/write system. The MicroRWD QT LP SMT version behaves in the same manner as the standard reader except that it has an **active, average current consumption of around 150µA (micro Amps)** with 1 second polling rate. As with other RWD modules, all commands and data response are via a simple TTL level RS232 interface. 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.

MicroRWD QT SMT combined Hitag 1/S, Hitag 2, EM400X and MCRF200/123 reader



The MicroRWD 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. The MicroRWD QT SMT version uses the same basic hardware as previous MicroRWD versions but has a larger memory microcontroller to accommodate the software for reading four different tag types. The QT SMT is host interface and command protocol compatible with the individual H1/S, H2, EM400X and MCRF200 reader versions. Functionally, the only difference is that the MicroRWD QT internal EEPROM parameter map has been changed to accommodate all

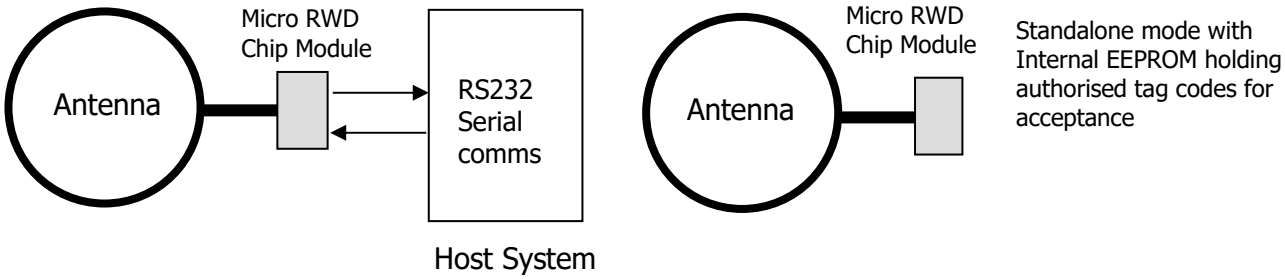
the parameters from all the individual versions. The READER TYPE command code (ASCII "v", 0x76) plus a parameter byte can be used to select the three main transponder types, a parameter in the EEPROM map further selects between EM400X and MC200/123 types.

As with the individual MicroRWD versions, the RWD QT SMT 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 up to 4k bits/second of data transfer and the total time, for example, to read a Hitag 2 four-byte page, including reading of the serial number, selecting the tag and the read operation itself takes less than 100ms.

The MicroRWD QT SMT is ideally suited to battery powered applications; when power (5v DC) is first applied to the module the red and green LED outputs “flash” once to indicate successful power-up. The device can also check for broken or shorted antenna and can even detect very badly tuned antennas, these problems are indicated by the red LED output “flashing” continuously until the fault has been rectified.

The MicroRWD will normally have the red LED output ON until a valid card or tag is brought into the RF field. If the tag is accepted as valid then the green LED output is turned ON (Red OFF) 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.

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 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 internal parameters and perform read/write operations to the tag itself.

2) Standalone mode is where the tag identity codes are checked against a stored list of authorised codes. If an identity code is matched, the output drives and Green LED are enabled. In this case the four byte identity code is taken as the transponder serial number (Page 0) for Hitag 1/S and Hitag 2 or memory bytes 1 - 4 on read-only types, ignoring the most significant first byte (byte 0). Effectively standalone mode occurs when there is no host system communicating with the Micro RWD.

Supported transponder types

The MicroRWD QT is designed to communicate with the following passive RF transponder types:-

1) Hitag 1 read/write transponders configured in R/W Public mode. Setting the HT1 to any other configuration will render them inoperable with this system. Note: Only the HT1 ICS30 02x Hitag silicon is fully supported for WRITE/ READ operations. The earlier HT1 ICS30 01x silicon (made obsolete early 1997) is only partially supported.

2) Hitag S256, S2048 read/write transponders configured in PLAIN MEMORY mode (factory default).

3) Hitag 2 read/write transponders configured in PASSWORD mode. Setting the HT2 transponder to any other configuration will render them inoperable with this system.

4) EM Marin EM4001/H4001 type transponders including H4003, H4102 and compatible read-only tags with the correct header, data and parity bit structure.

5) Microchip Technology MCRF 200-I/123 RF transponders that use direct ASK modulation, Manchester coding and with a data rate of RF/64. The MCRF200 transponder is expected to have the 0x802A header sequence at the start of the memory array.

The operation of the MicroRWD QT with Hitag 1/S, Hitag 2, EM400X and MCRF200/123 transponders is identical to the individual MicroRWD reader versions and their operation is fully described in this document and in the H1prot.PDF, H2prot.PDF, EMprot.PDF and MCprot.PDF documents.

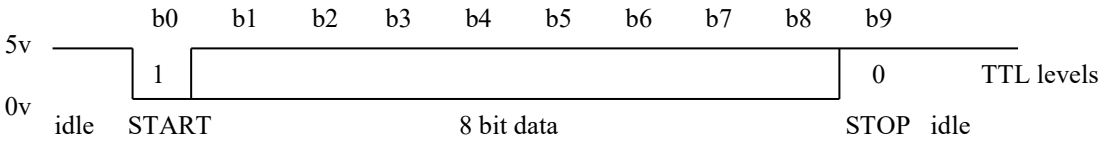
The transponder identification codes described in this text are regarded as the first four bytes (serial number or page 0) of the H1 and H2 memory array or bytes 1 to 4 (least significant four bytes) of the EM400X and MCRF200 memory arrays (ignoring most significant byte 0).

Serial Interface

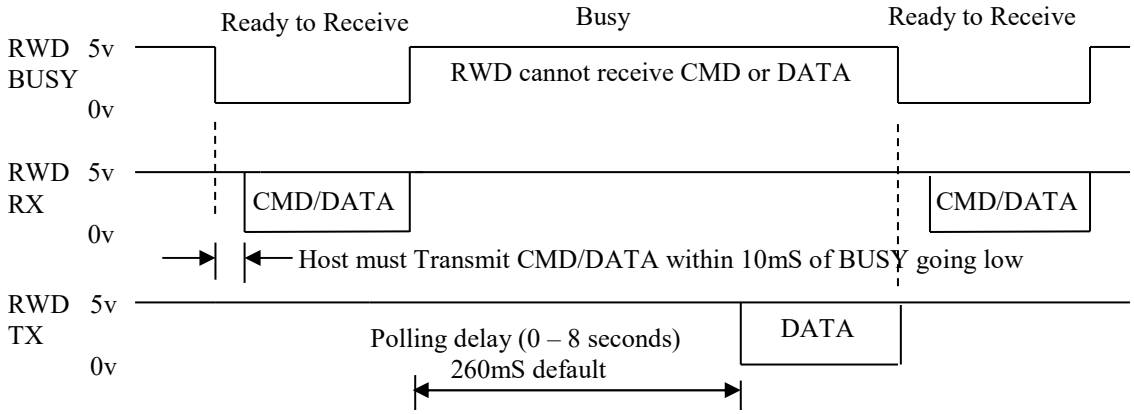
This is a basic implementation of RS232. The Micro RWD does not support buffered interrupt driven input so it must control a BUSY (CTS) line to inhibit communications from the host when it is fully occupied with tag communication. It is assumed that the host (such as a PC) can buffer received data.
Tx,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



Repeated RWD polling cycle and serial communication BUSY protocol



NOTE that the (programmable) polling delay period is skipped if the EEPROM parameter is zero or if there are commands to be processed.

Host Driver software

Communication with the MicroRWD module is via the TTL level RS232 interface (9600 baud, 8 bit, 1 stop bit, no parity) and uses the CTS line for hardware handshaking. The Windows applications (supplied with the Evaluation kit) can be used to communicate with the module or the user can write their own application on a PC or a microcontroller. The following basic communication algorithm should be used:-

Typical host computer "pseudo" driver code

```
if (Green LED ON (pin 2 = 0))                    // Optional check for valid tag in field
{
   if (CTS = 0)          // Wait for CTS = 0 (RWD ready to receive command / data)
   {
            // CTS times out after 10ms so command and all parameters must be sent with no-
            // gaps otherwise CTS times out and goes HIGH.
            // For example, send READ PAGE 1 (0x52 0x01)

            SEND_CMD( );    // Sent command + parameters to RWD

            // RWD sets CTS = 1 after last parameter received. RWD module enters low-
            // power state during (programmable) polling delay then sends reply.

            GET_REPLY( );              // Get Acknowledge byte + data
            // Response to READ command is 0xC0 (no tag) or 0xD6 + four bytes of DATA.
   }
}
```

Command Protocol

The commands are described fully in the following pages. The STATUS, MESSAGE and PROGRAM EEPROM commands are common to all the Reader modes, the structure and reply from commands such as READ PAGE can be different depending on which Reader mode is selected. Generally, command codes (plus optional data bytes) are transmitted to the RWD which replies with an Acknowledge byte (and data bytes if appropriate). The Acknowledge code should be read back by the host and decoded to confirm that the command was received and handled 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)
         |   |   |  Rx OK  (Tag  communication and acknowledgement OK)
         |   |   RS232  error (Host serial communication 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 CO (Hex) would indicate NO valid transponder in the RF field, whereas an acknowledge byte of D6 (Hex) would indicate a correctly matched transponder detected in the field (and no errors).
Note also that only the relevant flags are set after each command as indicated in the protocol documents.

NOTE:

1) The serial communication 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 data.
3) 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.
4) NOTE that only one command sequence is handled at a time.

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)

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:	“b IDE RWD H1 (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.

Reader Type

Command to allow selection of particular MicroRWD “Reader Type”. This command has the same function as writing to parameter byte 17 (0x11) of the internal EEPROM using Program EEPROM command. The Acknowledge byte reply confirms if parameter has been stored correctly.

	B7							B0	
Command:	0	1	1	1	0	1	1	0	(ASCII “v”, 0x76)
Argument1:	X	X	X	X	X	X	N	N	(NN bits = Reader Type selection parameter) 01 = Hitag 2 (0x01) 10 = Hitag 1/S (0x02 – factory default) 11 = EM400X/MC200 (0x03) (00 parameter also selects Hitag 1 version)
Acknowledge:	1	1	X	F	X	X	X	F	(F = Status flags, X = “don’t care” bits)

The “Reader Type” command has been added to the standard command set in order to allow selection of the H1/S, H2 or EM400X Reader modes. This command automatically stores the “Reader Type” parameter in the MicroRWD internal EEPROM (parameter byte 17) to allow the required Reader Type selection from power-up. The standard PROGRAM EEPROM command can also be used to store the parameter byte directly to location 17 to achieve the same result.
When EM400X type is selected, MCRF200/123 transponder type can be further selected as a subset of the main EM400X option. This achieved by storing 00 as the “EM400X/MC200” selection parameter (byte 16) in the internal EEPROM (using Program EEPROM command). Storing 01 as the selection parameter selects main EM400X type (factory default set to 01, EM400X mode).

The selected Reader Type can be verified by sending the MESSAGE command (0x7A = ASCII “z”). The message string returned has a unique ASCII character as the start of the string (“a”, “b” or “c”) and this can be used to confirm Reader mode currently selected.

For example:-

H1 type selected, MESSAGE command reply =
"**b** IDE RWD H1 (SEC_COM V1.xx) DD/MM/YY) Copyright IB Technology (Eccel Technology Ltd)" 0x00

H2 type selected, MESSAGE command reply =
"**a** IDE RWD H2 (SEC_COM V1.xx) DD/MM/YY) Copyright IB Technology (Eccel Technology Ltd)" 0x00

H400X/MC200 type selected, MESSAGE command reply =
"**c** IDE RD H400X/MC200 (SEC_COM V1.xx) DD/MM/YY) Copyright IB Technology (Eccel Technology Ltd)" 0x00

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

Polling delay parameter values (EEPROM location 0):

Parameter 0 value	Polling Delay SLEEP Period
0x00	0 mS
0x10	8 mS
0x20	16 mS
0x30	32 mS
0x40	65 mS
0x50	132 mS
0x60	**262 mS**
0x70	524 mS
0x80	1 second
0x90	2 seconds
0xA0	4 seconds
0xB0	8 seconds

Polling delay and SLEEP skipped

Polling delay can be set from 0 to 8 seconds to give complete control over current consumption and battery life. Note that setting Polling delay = 0x00 skips the SLEEP and power-down operation so polling is as fast as possible (and current consumption is highest). Polling delay is also skipped when there are host commands to be processed.

Byte 0: Polling Delay (SLEEP / Power down) period (Default = 0x60 = approx 260mS)

Byte 1: RF ON/OFF lock byte (0x55 = RF ON, anything else = OFF, normally set to 0x55)
Byte 2: Reserved (internal checksum value) – do not use
Byte 3: H1 Encryption ON/OFF control byte (0x00 = OFF)

Byte 4:) H1 32 bit Encryption Seed (M.S byte)
Byte 5:)
Byte 6:)
Byte 7:) (L.S byte)

Byte 8: H2 PASSWORD_RWD (32 bit password sent to HT2) – default “M”
Byte 9: H2 PASSWORD_RWD “I ”
Byte 10: H2 PASSWORD_RWD “K”
Byte 11: H2 PASSWORD_RWD “R”

Byte 12: Reserved (not used)
Byte 13: H2 PASSWORD_TAG (24 but reply from HT2) - default 0xAA
Byte 14: H2 PASSWORD_TAG "H"
Byte 15: H2 PASSWORD_TAG "T"

Byte 16: EM400X Option Byte, 0x00 = MC200, 0x01 = H400x (default)
Byte 17: Reader Type (0x02 = H1 default)
Byte 18: Reserved (not used)
Byte 19: Reserved (not used)

Start of authorised tag identity 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).
NOTE that identity codes are four bytes long.
Identity codes are taken as Page 0 serial numbers for H1 / H2 types and transponder memory bytes 1 to 4 for EM400X and MCRF200 types, ignoring most significant first byte (byte 0).
List can hold up to 60 (4 byte) identity codes.

Byte 20: 0xFF Empty list
Byte 21: 0xFF
Byte 22: 0xFF
Byte 23: 0xFF

Byte 24: (MSB) Tag identity code
Byte 25:
Byte 26:
Byte 27: (LSB)

Byte 28: (MSB) Tag identity code
Byte 29:
Byte 30:
Byte 31: (LSB)
-
-
Byte 255: Last Internal EEPROM location

Factory Reset

Command to restore Factory default EEPROM values and perform hardware Reset operation. The 0x55 0xAA parameters protect against accidental operation.
After Reset, the Green LED flashes five times indicating the successful loading of the Factory default values.

	B7							B0	
Command:	0	1	0	0	0	1	1	0	(Ascii “F”, 0x46)
Argument1:	0	1	0	1	0	1	0	1	0x55
Argument1:	1	0	1	0	1	0	1	0	0xAA

Reset occurs after the command is processed so there is no Acknowledge byte reply.

Operation of Identity code authorisation list

The Micro RWD QT reader only allows full communication with any of the transponders if an initial level of security has been passed. The system works by firstly reading the tag identity code (serial number), which is the four bytes from page 0 (first page) of H1/S or H2 types and bytes 1 to 4 of the EM400X or MC200 memory arrays ignoring the most significant first byte (byte 0). The Micro RWD internal EEPROM is then checked to see if this serial number is stored in the authorisation list located from byte 20 onwards. If the tag serial number is matched to a stored serial number or the list is empty then the tag has passed the validation test. If the Micro RWD has FF FF FF FF (hex) stored at EEPROM locations 20 to 23 then the list is treated as empty and all tags are accepted.
Full communication is only allowed if this initial security check has been passed (or the Micro RWD authorisation list is empty).

Micro RWD H1/S Protocol

The MicroRWD H1/S Reader mode is a complete read / write and tag acceptance solution for Hitag 1, Hitag S256 and Hitag S2048 RFID transponders (in Plain Memory mode).

Write Tag Page

Command to write 4 bytes of data to HT1 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	N	N	N	N	N	N	(N = HT1 page address 0-63)
Argument2:	D	D	D	D	D	D	D	D	(D = msb data to write to HT1)
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 HT1)
Acknowledge:	1	1	F	F	F	F	F	X	(F = Status flags)

Write Tag Block

Command to write up to 16 bytes of data to HT1 memory. A Block is made up of four pages (each page being 4 bytes of data). If the specified page lies on the block boundary then all 16 bytes (4 pages) can be written. If the specified page is on the block boundary + 1 then 12 bytes (3 pages) can be written.
In this way 16, 12, 8 or 4 bytes of data can be stored on the tag depending on the page number and it's position within the block. If the write was unsuccessful (invalid tag or out of field) then Status flags in acknowledge byte indicate error.

	B7 B0	
Command:	0 1 1 1 0 1 1 1	(ASCII "w", 0x77)
Argument1:	x x N N N N N N	(N = HT1 page address 0-63)
Argument2:	D D D D D D D D	(D = msb data to write to HT1)
Argument3:	D D D D D D D D	(PAGE N DATA)
Argument4:	D D D D D D D D	
Argument5:	D D D D D D D D	(D = lsb data to write to HT1)
|		
|	Up to 16 bytes can be specified depending on page address N	
|	ie. Perform PAGE/4 => if remainder (mod) = 0 then full block (16 bytes)	
|	if remainder = 1 then 12 bytes sent	
|	if remainder = 2 then 8 bytes sent	
|	if remainder = 3 then 4 bytes sent	
V		
Argument14:	D D D D D D D D	(D = msb data to write to HT1)
Argument15:	D D D D D D D D	(PAGE N+3 DATA)
Argument16:	D D D D D D D D	
Argument17:	D D D D D D D D	(D = lsb data to write to HT1)
Acknowledge:	1 1 F F F F F X	(F = Status flags)

Read Tag Page

Command to read 4 bytes of data from HT1 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 N N N N N N	(N = HT1 page address 0-63)
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 read from HT1)
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 read from HT1)

Read Tag Block

Command to read up to 16 bytes of data from HT1 memory. A Block is made up of four pages (each page being 4 bytes of data). If the specified page lies on the block boundary then all 16 bytes (4 pages) can be read. If the specified page is on the block boundary + 1 then 12 bytes (3 pages) can be read. In this way 16, 12, 8 or 4 bytes of data can be retrieved from the tag depending on the page number specified and it's position within the block. If the read was successful, indicated by acknowledge status flags then up to 16 bytes of tag data follow.

	B7							B0	
Command:	0	1	1	1	0	0	1	0	(ASCII "r", 0x72)
Argument1:	x	x	N	N	N	N	N	N	(N = HT1 page address 0-63)
Acknowledge:	1	1	F	F	F	F	F	X	(F = Status flags)

+ up to 16 bytes
Data only follows if read was successful

Reply1:	D	D	D	D	D	D	D	D	(D = msb data read from HT1)
Reply2:	D	D	D	D	D	D	D	D	(PAGE N DATA)
Reply3:	D	D	D	D	D	D	D	D	
Reply4:	D	D	D	D	D	D	D	D	(D = lsb data read from HT1)

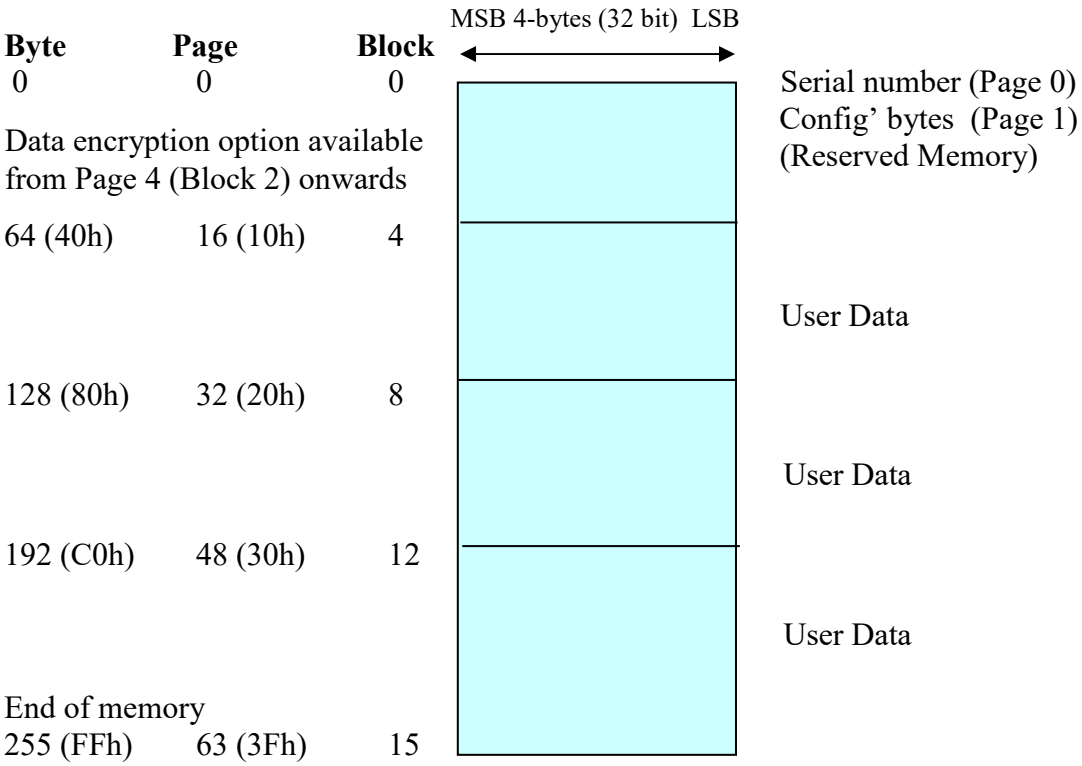
|
| Up to 16 bytes can be specified depending on page address N
| ie. Perform PAGE/4 => if remainder (mod) = 0 then full block (16 bytes)
| if remainder = 1 then 12 bytes read
| if remainder = 2 then 8 bytes read
| if remainder = 3 then 4 bytes read
V

Reply13:	D	D	D	D	D	D	D	D	(D = msb data read from HT1)
Reply14:	D	D	D	D	D	D	D	D	(PAGE N+3 DATA)
Reply15:	D	D	D	D	D	D	D	D	
Reply16:	D	D	D	D	D	D	D	D	(D = lsb data read from HT1)

Encryption Methodology

The Micro RWD H1/S has a data encryption system that allows data to be stored in an encoded form that cannot be read as sensible data by any other Hitag 1 reader system.
The format of the data stored in the transponder memory (apart from the serial number, configuration and other data in Pages 0 - 3) is controlled by the Encryption Control byte in the Micro RWD internal EEPROM. If Encryption Control ON is selected then all data stored in the transponder from page 4 upwards will be encrypted, and if OFF is selected then all data is stored in standard format.
The method of encryption uses a "dynamic algorithm" which effectively makes the encoded data specific to a particular transponder and a set of encryption seed values stored in the Micro RWD internal EEPROM. This not only protects stored information but also prevents cloning of cards or copying of data. Information is encrypted when being stored and decrypted when being read, thereby making the process totally transparent to the user. Another Hitag 1 reader system would read encrypted data as random bytes with no meaning.
Users should program their own encryption seed values to fully customise their system.

Hitag 1 Memory Map

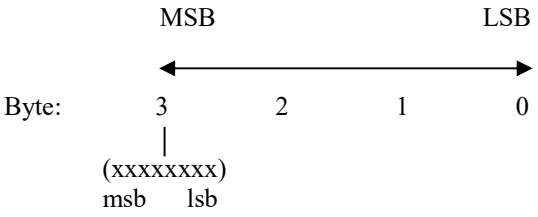


Hitag 1 transponders have Pages 16 to 63 available for user data storage (192 bytes). It is advised not to use the memory locations below page 16 because these are used for configuration bytes and a "Reserved" memory area.

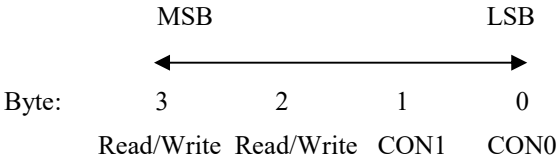
Hitag S transponders configured in PLAIN MEMORY mode have a similar memory map to Hitag 1 except they have available "user data " memory from Page 2 onwards. Hitag S256 transponders therefore have Page 2 – 7 (24 bytes) for user data and Hitag S2048 types have Page 2 - 63 (248 bytes) for user data.

Hitag 1 Serial Number and Configuration Bytes

Page 0 (Serial Number):

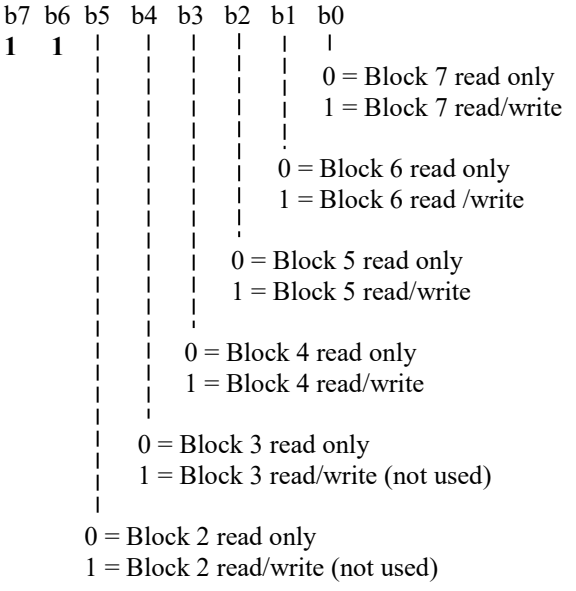


Page 1 (Configuration Bytes):

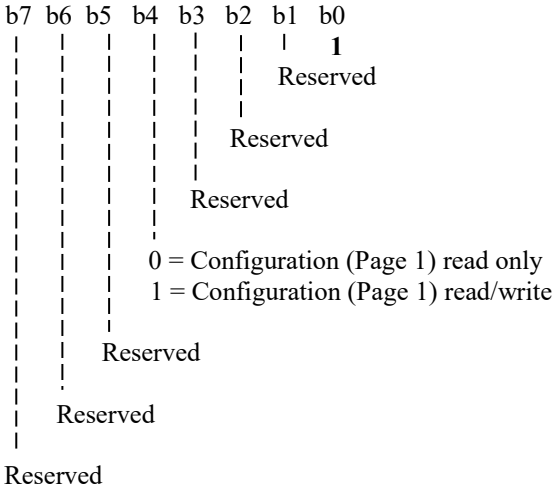


The Hitag 1 configuration bytes control whether the memory blocks are read/write or locked for read only access. Note that bytes 2 and 3 of the configuration page are not used and are currently available for general read/write use.

CON 0 (Page 1, byte 0)



CON 1 (Page 1, byte 1)

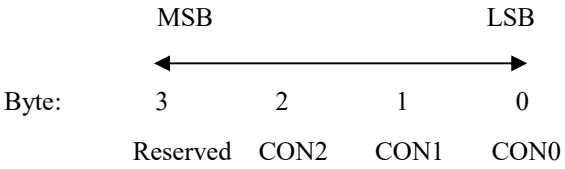


Note that these configuration bits are OTP. Once they are set to read-only the Hitag 1 transponder is hardware protected and they can never be changed.

Note that the "Reserved" bits of Configuration Byte 1 must not be altered. Page 1 must be read first and the bits that can be changed masked on/off before writing back.

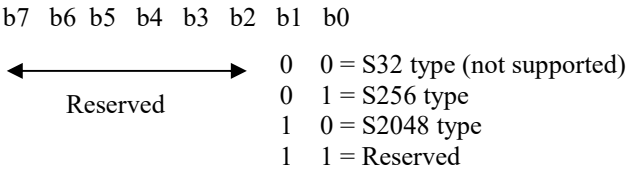
Hitag S Configuration Bytes

Page 1 (Configuration Bytes):

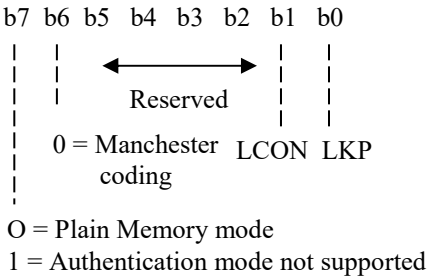


The Hitag S configuration bytes indicate the type of HS transponder and the mode of operation. Please note that the MicroRWD H1/S module only supports Plain Memory mode (default mode as set by Philips). Configuration bytes also control whether the memory blocks are read/write or locked for read only access.

CON 0 (Read-only – Memory Type information)



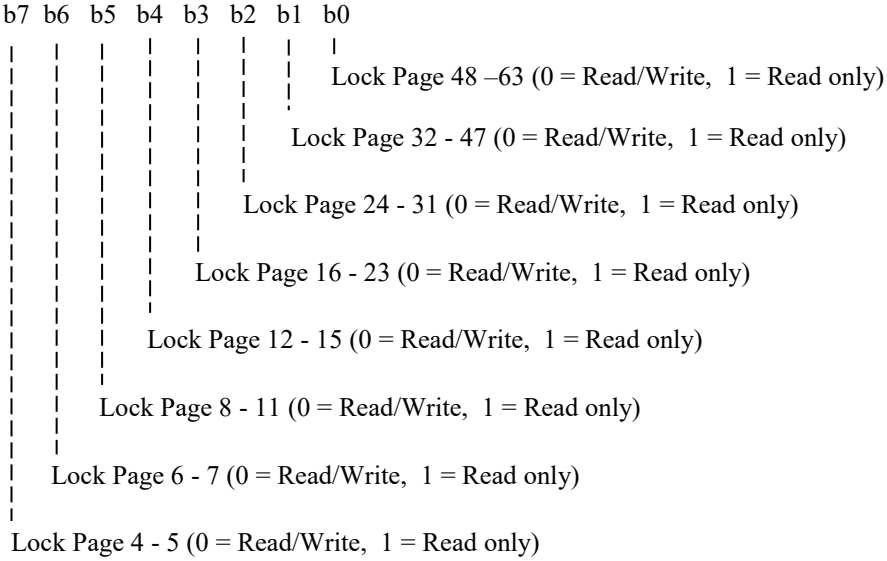
CON 1 (Mode and Lock bits)



LCON bit
(CON1 and CON2 access control):
0 = Read/Write
1 = CON1 read only, CON2 OTP

LKP bit
(Page 2 and Page 3 access control)
0 = Read/Write
1 = Read only.

CON 2 (Memory Lock bits)



Note that CON2 (Memory Lock bits) are OTP (One-Time-Programmable) if LCON = 1
Note also that the "Reserved" bits must not be altered. Page 1 must be read first and the bits that can be changed masked on/off before writing back.

Micro RWD H2 Protocol

The MicroRWD H2 Reader mode a complete read / write and tag acceptance solution for Hitag 2 RFID transponders (in Password mode).

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.

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.

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

Micro RWD (EM) H400x / 4102 Protocol

The MicroRWD H400X Reader mode is a complete reader and tag acceptance solution for EM Marin H4001/H4102 and compatible RFID transponders.

Read H400x Tag

Command to read 5 bytes of data from H400x (40 bit) memory array. If the read was successful, indicated by acknowledge status flags then five 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	x	x	x	(Dummy Page number e.g 00)
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 read from H400x)
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	
Reply5:	D	D	D	D	D	D	D	D	(D = lsb data read from H400x)

Note that for the Read Tag command, if an error flag has been set in the Acknowledge code then there will be NO following data.

Micro RWD MC200 Protocol

The MicroRWD MC200 Reader mode is a complete reader and tag acceptance solution for Microchip Technology MCRF 200-I/123 RFID read-only transponders (configured as RF/64 bit rate, direct ASK, Manchester coded with 0x802A header bytes)

Read MC200 Tag

Command to read 16 bytes of data from MCRF200 (128 bit) memory array. If the read was successful, indicated by acknowledge status flags then 16 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	x	x	x	(Dummy Page number e.g 00)
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 read from MCRF200)
Reply2:	D D D D D D D D	
Reply3:	D D D D D D D D	
Reply15:	D D D D D D D D	
Reply16:	D D D D D D D D	(D = lsb data read from MCRF200)

Note that for the Read Tag command, if an error flag has been set in the Acknowledge code then there will be NO following data.

Micro RWD QT LP (low-power) specification

The MicroRWD QT LOW-POWER version is a complete RFID Reader for 125kHz Hitag1, HitagS, Hitag2, EM4100/4102 and MCRF200/123 cards and tags. The module is pin-compatible and virtually identical in operation to previous version (NOTE differences in EEPROM parameters and the polling delay rates).

However the LOW-POWER version uses a different specification microcontroller offering lower voltage operation and is designed to be powered from four alkaline battery cells. During the Polling Delay period the microcontroller enters SLEEP mode with the RF device in hard power-down mode to reduce the current consumption to a very low level.

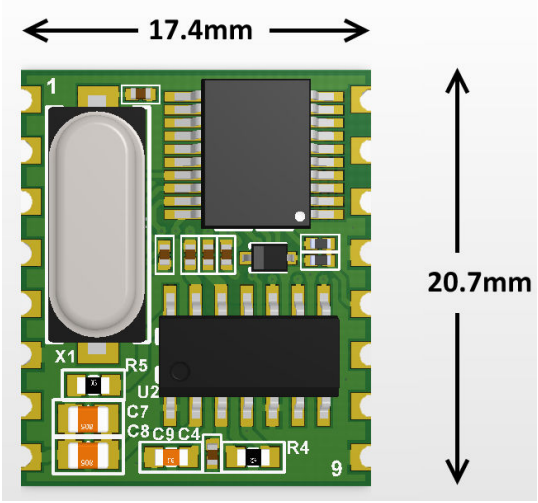
The module wakes up after the polling delay period and the process repeats. The RWD-QT Windows applications can be used to configure the parameters and read/write data.

Parameter	Typical Value
Supply Voltage (performance optimised for 5 volt operation)	4 – 6 volts DC (operation from 4 x alkaline cells)
Operating temperature	-40 deg C to + 85 deg C
AVERAGE current consumption. (1 second polling)	**150 µA (micro Amps)**
Active period for RF AND host communication (each polling cycle).	Up to 40 mS
Peak antenna voltage (optimum tuning)	180 volts peak-to-peak
Peak antenna current (optimum tuning) for short period each polling cycle (up to 10 mS burst)	150 mA
Polling Delay (SLEEP / Power-down mode)	0 to 8 seconds
Current consumption during Polling delay / SLEEP	Less than 20 µA
Current consumption during RF ON each polling cycle	Less than 20mA
Maximum data rate (between card and RWD)	4k baud
Range (dependent on antenna dimensions and tuning)	Up to 150mm
Auxiliary output drives	Up to 25mA
Serial Interface	TTL level RS232
Serial Communication Parameters	9600 baud, 8 data bits, no parity, 1 stop bit protocol with CTS handshake

Basic electrical specification with LEDs pins and auxiliary outputs NOT connected.
Note that the MicroRWD QT SMT low-power version is designed for optimum performance and range at 5-volt operation. Performance will be reduced at maximum and minimum operating voltage.

During the "Polling Delay" SLEEP/Power-down period the logic levels on the RWD pins remain active and so for minimum current consumption, the LEDs and the auxiliary output drives must be disconnected.

Micro RWD QT SMT module dimensions and pinout



PINOUT DESCRIPTION

Pin Name	DIP No.	I/O Type	Buffer Type	Description
LED1	1	O	TTL	Red LED connection. 25ma max sink current
LED2	2	O	TTL	Green LED connection. 25ma max sink current
SW1	3	I	TTL	Manual override for auxiliary outputs
OP3	4	O	TTL	Auxiliary output drive. 25ma max sink current.
OP2	5	O	TTL	Auxiliary output drive. 25ma max sink current.
GND	6	P	-	Ground reference for logic and analogue pins
AN1	7	P	AN	Antenna connection. 1 (connected to antenna coil)
AN2	8	P	AN	Antenna connection 2 (connected to antenna coil)
GND	9	P	-	Ground reference for logic and analogue pins.
OP1	10	O	TTL	Auxiliary output drive. 25ma max sink current.
OP0	11	O	TTL	Auxiliary output drive. 25ma max sink current.
VCC	12	P	-	+5v Positive supply
GND	13	P	-	Ground reference for logic and analogue pins.
RX	14	I	TTL	Serial communication Receive line. 9600 baud, 8 bit, 1 stop, no parity
TX	15	O	TTL	Serial communication Transmit line
CTS	16	O	TTL	Serial communication CTS handshake. RX enabled when CTS low and disabled when high.

(I/O = Input/Output, AN = Antenna output, P = Power, ST = Schmitt Trigger input, TTL = TTL logic I/O)

(Hitag is a trademark of Philips/NXP Semiconductors N.V)
(EM400X is a trademark of EM MICROELECTRONIC-MARIN SA, a company of the SWATCH GROUP)
(MCRF200 is a trademark of Microchip Technology Inc.)

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