ib technology

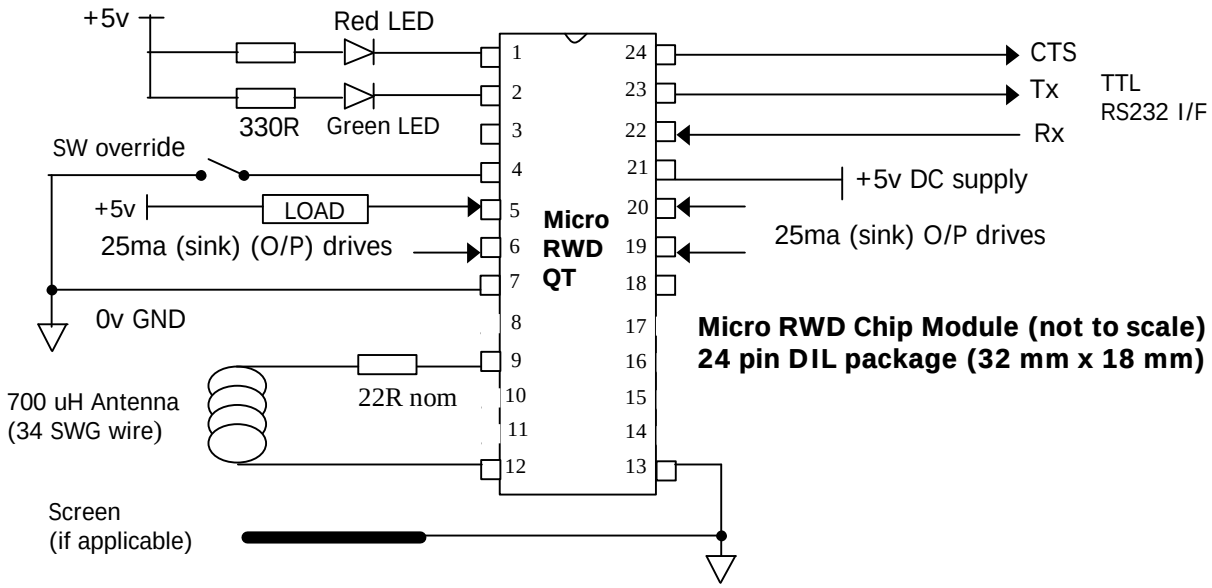
Data Sheet

RWD_QT.pdf
8 Pages
Last Revised 08/05/06

Micro RWD Quad-Tag Reader

The MicroRWD "QT" (Quad-Tag) version is a complete 125kHz reader solution for Hitag 1 (including Hitag S in Plain Memory mode), Hitag 2 (Password mode), EM400X/4102 and MCRF200I/123 passive RFID transponder types. The solution only needs a 700 uH 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.

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



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 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 version is pin-for-pin, host interface and command protocol compatible with the individual H1, H2, EM400X and MCRF200 reader versions. This document should therefore be read in conjunction with the **H1prot.PDF**, **H2prot.PDF**, **EMprot.PDF** and **MCprot.PDF** data sheets. Functionally, the only difference is that the MicroRWD QT internal EEPROM parameter map has been changed to accommodate all the parameters of all the individual versions.

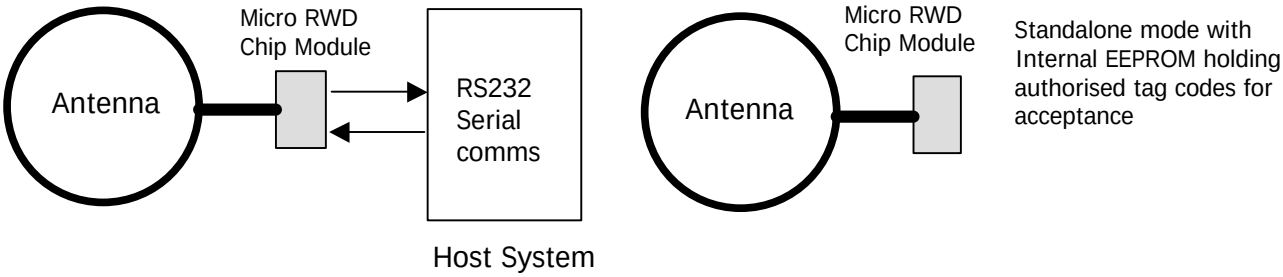
A new command code "v" plus a parameter byte can be used to select the three main transponder types, a parameter in the EEPROM map further selects between EM400X and MC200/123 types.

A with the individual MicroRWD versions, the RWD “QT” 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 can be easily integrated into almost any application; 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 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 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 Manchester modulation 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, Hitag 2, EM400X and MCRF200/123 transponders is identical to the individual MicroRWD reader versions and their operation is described fully in the H1prot.PDF, H2prot.PDF, EMprot.PDF and MCprot.PDF documents.

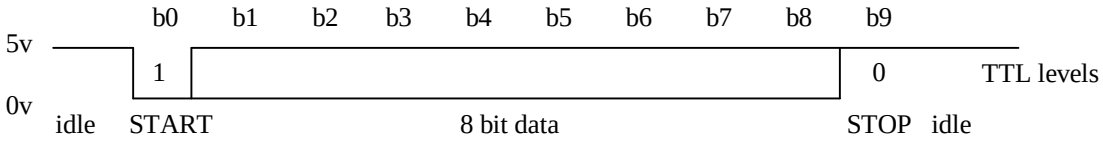
The transponder identification codes described in this text are regarded as the first four bytes (serial number or page 0) of the H1 and H2 memory array or bytes 1 to 4 (least significant four bytes) of the EM400X and MCRF200 memory arrays (ignoring most significant byte 0).

Serial Interface

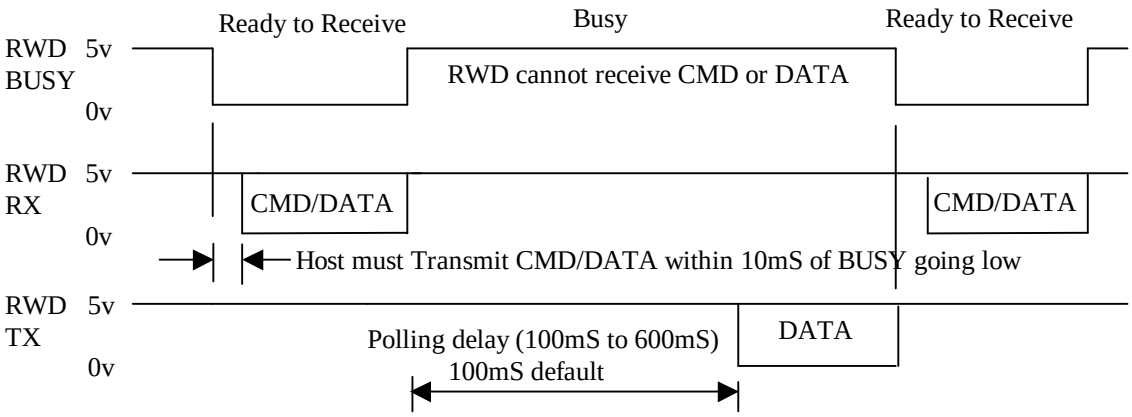
This is a basic implementation of RS232. The Micro RWD does not support buffered interrupt driven input so it must control a BUSY (CTS) line to inhibit communications from the host when it is fully occupied with tag communication. It is assumed that the host (such as a PC) can buffer received data.
Tx,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



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 main commands for the MicroRWD QT version are described in the H1Prot.PDF, H2prot.PDF, EMprot.PDF and MCprot.PDF documents. 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.

The "Reader Type" command has been added to the standard command sets of the individual versions in order to allow selection of the H1, H2 or EM400X transponder types. 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).

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	(0x76 = ASCII v)
Argument1:	X X X X X X N N	(NN bits = Reader Type selection parameter) 01 = Hitag 2 (0x01) 10 = Hitag 1 (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 selected Reader Type can be verified by sending the Report MESSAGE command (0x7A = ASCII z), see individual protocol documents for more information. The message string returned has a unique ASCII character as the start of the string ("a", "b" or "c") and this could be used to confirm Reader Type currently running.

For example:-

H1 type selected, z command reply =
"**b** IDE RWD H1 (SEC_COM V1.xx) DD/MM/YY) IB Technology accepts no liability for the use of this product in any end application" 0x00

H2 type selected, reply =
"**a** IDE RWD H2 (SEC_COM V1.xx) DD/MM/YY) IB Technology accepts no liability for the use of this product in any end application" 0x00

H400X/MC200 type selected, reply =
"**c** IDE RD H400X/MC200 (SEC_COM V1.xx) DD/MM/YY) IB Technology accepts no liability for the use of this product in any end application" 0x00

Internal EEPROM memory map

Byte 0:	Tag Polling Rate (x 2.5ms), (default = 0x14, 20 (dec) approx (50ms)
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

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 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 serial number stored in the Micro RWD 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 through the validation test.

Full communication is only allowed if this initial security check has been passed (or the Micro RWD authorisation list is empty).

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