ib technology

Data Sheet

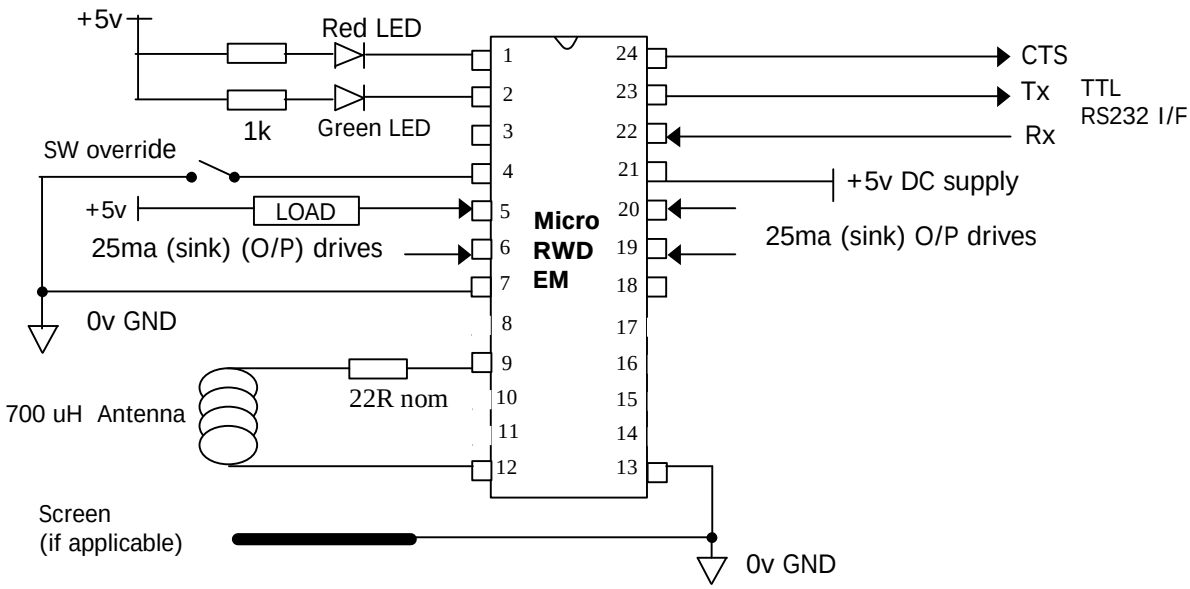
EMPROT.PDF
7 Pages
Last Revised 21/03/06

Micro RWD (EM) H400x Protocol

The MicroRWD H400X version is a complete reader and tag acceptance solution for EM Marin H4001/H4102 derived RF transponders. The solution only needs a 7??uH antenna coil connected and 5v DC supply to be a fully featured reader 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 system features to be customised, configurations changed and data read from the tag to be handled by the host system.

Typical application configuration for Micro RWD module



The H4001 based transponders provide 64 bits of read-only memory. This memory contains a header bit sequence and 40 bits (5 bytes) of user data interspersed with parity bits. Data is only accepted from the H4001 transponder if the memory parity bits are valid. This configuration ensures that the integrity of user data is maintained. The H4001 transponder type is widely used throughout the world in its base form and also in many fully compatible derivative forms.

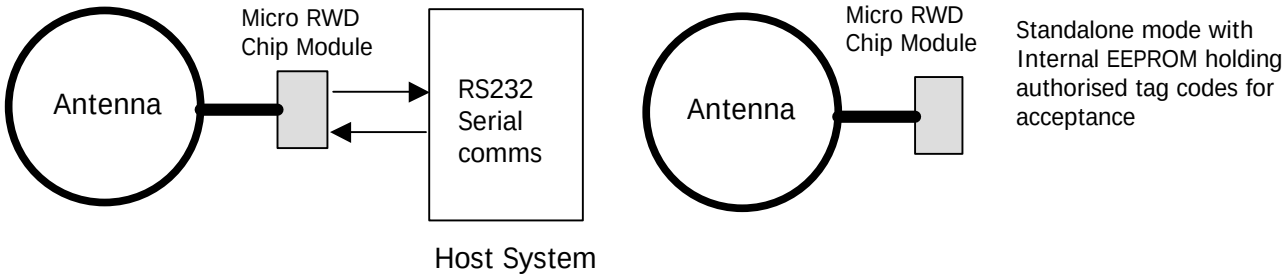
The MicroRWD is essentially a proximity system and a Read range of up to 20cm can be achieved with the same level of reliable communication and EMC resilience.

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 2k bits/second of data transfer and the total time to read the 40 bit data is less than 40ms.

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 very 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.

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 H400X transponder for subsequent read operations. A simple serial protocol allows a host system to communicate with the Micro RWD in order to program new authorised identity codes, change configurations and perform read operations from the tag itself.

2) Standalone mode is where the H400X 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 identity codes are taken as the least significant bytes 1 to 4 of the H400X five byte sequence, The most significant first byte (byte 0) is ignored. This is to allow use of any commercially supplied H400X transponders where least significant bytes are incremented. Effectively standalone mode occurs when there is no host system communicating with the Micro RWD.

Supported transponder types

The Micro RWD H400X version is designed to read data from EM Marin H4001 type transponders including H4003, H4102 (now called EM4001, EM4102) and compatible read-only tags with the correct header, data and parity bit structure. The operation of the Micro RWD and H400X transponders is described in more detail at the end of this document.

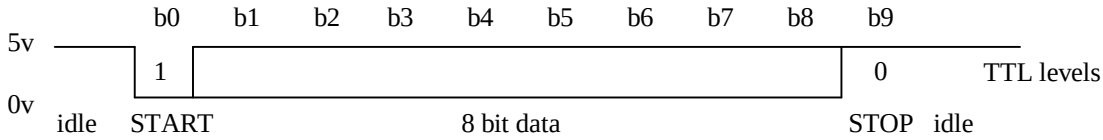
The identification codes described in this text are regarded as bytes 1 to 4 (32 bits) of the five byte (40 bit) memory array, ignoring the most significant first byte (byte 0).

Serial Interface

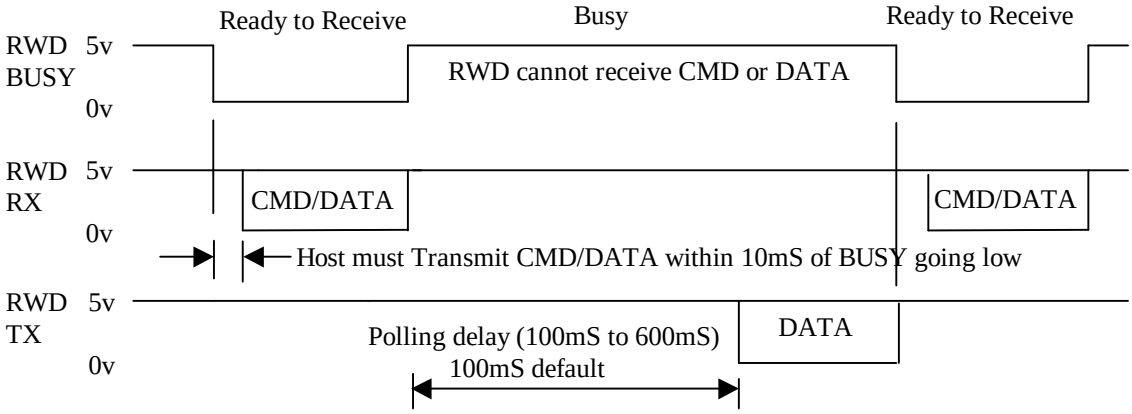
This is a basic implementation of RS232. The Micro RWD does not support buffered interrupt driven input so it must control a BUSY (CTS) line to inhibit communications from the host when it is fully occupied with tag communication. It is assumed that the host (such as a PC) can buffer received data.
Tx,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



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 authentication 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) Tag present.
Note also that only the relevant flags are set after each command as indicated in the following specification.

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	(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.

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	(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	(0x7A)

Reply: “c IDE RD MC200/H400x (SECM200 V1.xx) DD/MM/YY” 0x00

Returned string identifies author, product descriptor, project name, firmware version number 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 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 configuration 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	(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 byte (0x55 = RF ON, anything else = OFF, normally set to 0x55)
Byte 2: Reserved (Checksum)
Byte 3: Reserved

Byte 4: Reserved
Byte 5: Reserved
Byte 6: Reserved
Byte 7: Reserved

Byte 8: Reserved
Byte 9: Reserved
Byte 10: Reserved
Byte 11: Reserved

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).

NOTE that these identity codes are four byte sequences.

The tag identity code is taken as bytes 1 to 4 of H400X five byte sequence, the most significant first byte (byte 0) is ignored. The list can hold up to 60 (4 byte) identity codes.

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 communication with H4001 transponders if an initial level of security has been passed. The system works by reading the tag memory, stripping off the various parity bits to give the five byte user memory. Bytes 1 to 4 of the H4001 five byte sequence are then taken as a four byte serial number (identity code). The most significant byte (byte 0) is ignored. 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 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 12 to 15 then the list is treated as empty and all H4001 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