PICO MEGA DESIGN LABS

HF 1WATT READER RF MODULE

Pico HF RFID reader series
HF 1 W reader **AID-TMRND-DEV-HF-01**
Reference manual

5th Edition June 2008

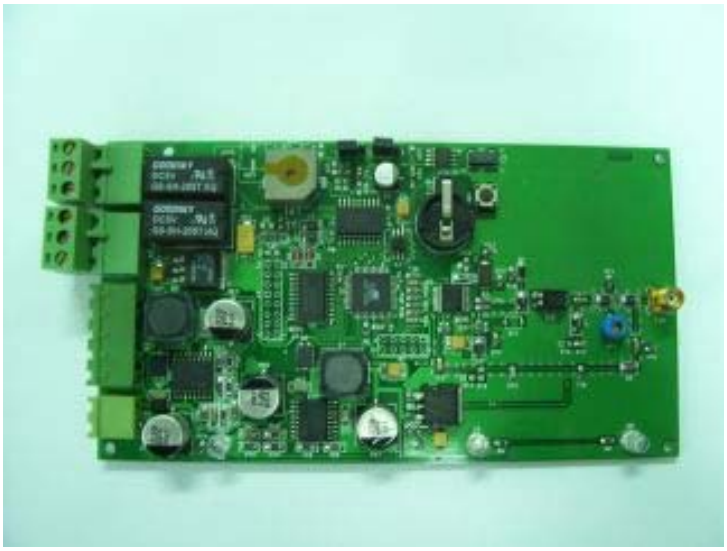
For more information, please contact www.pico-mega.com

Fifth edition - JUNE 2008

This is the fifth edition of the manual, it describes about

Pico High Frequency 1 W Reader **AID-TMRND-DEV-HF-01**

Firmware version 4.2.1.



Pico Mega Design Labs (PMDL) reserves the right to make changes to its products or services or to discontinue any product or service at any time without notice. PMDL provides customer assistance in various technical areas, but does not have full access to data concerning the use and application of customer's solutions. Therefore, PMDL assumes no liability and is not responsible for customer solutions or software design or performance relating to solutions or applications incorporating PMDL products. In addition PMDL assumes no liability and is not responsible for infringement of patents and/or any other intellectual or industrial property rights of third parties, which may result from assistance provided by PMDL. PMDL products are not designed, intended, authorized or warranted to be suitable for life support applications or any other life critical applications that could involve potential risk of death, personal injury or severe property or environmental damage.

Document overview

4.2. a. Configuration Commands

- 4.2.1. Get Firmware Version
- 4.2.2. Check reader status
- 4.2.3. Set baud rate
- 4.2.4. Set clock time
- 4.2.5. Get clock time
- 4.2.6. Set Reader ID
- 4.2.7. Get Reader ID
- 4.2.8. Set / Reset auto visual
- 4.2.9. Activate / Deactivate VAI
- 4.2.10. Write into reader memory
- 4.2.11. Read from reader memory

4.2. b. RF related Commands

- 4.2.12. Read single tag UID
- 4.2.13. Read tags in auto anti-collision mode
- 4.2.14. Write into nth block
- 4.2.15. Read from nth block
- 4.2.16. Write into nth block of particular transponder
- 4.2.17. Read from nth block of particular transponder
- 4.2.18. Write into nth block of particular transponder with password
- 4.2.19. Write AFI
- 4.2.20. Write DSFID
- 4.2.21. Lock any Block / AFI / DSFID
- 4.2.22. Stay quiet
- 4.2.23. Transmitter ON / OFF

4.2. c. Common response to all the RF commands

1. Introduction

1.1. Document description

This document describes about hardware, operational features, commands and response data formats of Pico HF RFID 1W reader, AID-TMRND-DEV-HF-01. This fifth edition of the document is meant for the firmware version 4.1.0.

- All data format in the command frame should be given in hexadecimal format only.
- The hexadecimal value in brackets "[ ]" indicates a control byte (command).
- During the reading of a transponder, it must be ensured that the transponder is located within the detection range of the 1 W Reader during the process.
- 1 W Reader is also referred as Reader in the entire document.

1.2. Abbreviations

AFI	Application Family Identifier
ASK	Amplitude Shift Keying
bps	Bits per second
DSFID	Data Storage Format Identifier
FSK	Frequency Shift Keying
ID	Identification
LRC	Longitudinal Redundancy Check
MHZ	Megahertz
Min	minutes
ms	milliseconds
MSB	Most Significant Byte
Mbit	Megabit
RF	Radio Frequency
RTC	Real Time Clock
Sec	Seconds
UID	Unique Identifier (read only serial number)

2. Hardware Description

2.1. General Description – 1 W Reader

Pico RFID line of 13.56 MHz HF 1 W Reader brings the efficiency in industrial automation, process control, warranty management, etc.

The HF 1 W Reader is based on Texas Instruments RFID technology and operates at 13.56 MHz frequency that is compliance with the ISO/IEC 15693 vicinity card standards. The HF 1 W Reader features include a printed antenna, a Real Time Clock (RTC) and 2 M bits memory.

The reader can be interfaced to a PC via RS232 communication port at a configurable baud rate. Two onboard LED's and a buzzer provides visual and audio interface.

2.2. System Overview

HF 1 W Reader works on the 'Readers-talks-first' principle. As soon as the reader is powered it generates an electromagnetic field around the antenna. Once it receives a command from the PC it sends the corresponding modulated command in the field. The transponder in the vicinity of the RF field converts the electromagnetic field energy to an operational energy and demodulates the command sent by the reader and responds to it accordingly.

2.3. Interfacing PC – Reader

The Reader is interfaced with the PC through RS232 serial port cable. The serial communication occurs at RS232 level using 1 start bit, 8 data bits and 1 stop bit, no parity, no hard ware flow control at a selective baud rate between 300 bps to 57600bps, except 38400 bps. The default baud rate of the reader is 19200 bps. The PC – Reader communication is carried out in data packets.

The communication from the PC to reader is a command and from the reader to PC is a response.

2.4. Functional specifications

Part Number	AID-TMRND-DEV-HF-01
Operating frequency	13.56 MHz
Voltage Rating	16 – 24 VDC
Current Consumption	800 mA (peak)
Transmitter power level	1W (pulsed)
Antenna connection	On board SMA connector
Antenna impedance	50 ohms @ 13.56 MHz
Communication interface	RS232
Baud rate	Configurable from 300 bps to 57600 bps*.
Visual / Audio Interface	Two LED's, a Buzzer
Additional features	Inbuilt Real Time Clock (RTC) Inbuilt Memory of 2 M bits
Operating temperature	-20°C to + 65°C
Storage temperature	-40°C to + 85°C

***The reader does not support the baud rate 38400 bps.**

2.5. Mechanical specifications

The 1 W Reader has a simple mechanical construction where all the components are mounted on the Printed Circuit Board. The PCB also carries the connectors for the power supply and serial cable. The outer dimension and weight of the board is given below.

Dimensions	158(L) x 85(W) x 22(H) all in mm
Weight	250 grams

2.6. Power Supply

The input supply voltage ranging from +16.0 V to 24 V DC can be given to the 1 W Reader. A +15 V DC adapter is supplied along with the reader package. The reader has industrial grade onboard 5VDC low drop regulator and current consumption is 150 mA.

Input Supply voltage	+16 V to +24 V dc power supply
Current consumption	15V @ 800 mA

2.7. Output RF power

RF output power	1 W (+30dBm)

2.8. RF Physical layer

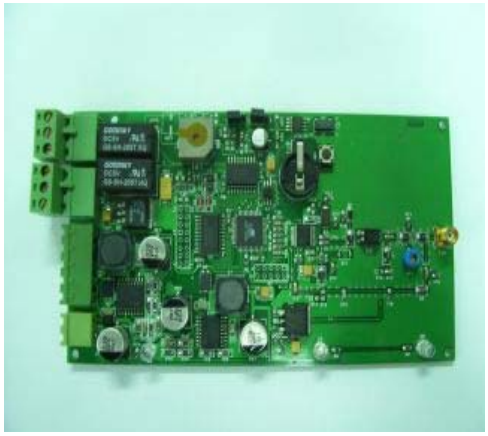
Reader to transponder	10% - 30% (nominally 20%) ASK
Transponder to reader	FSK / High speed data rate

2.9. Antenna parameters

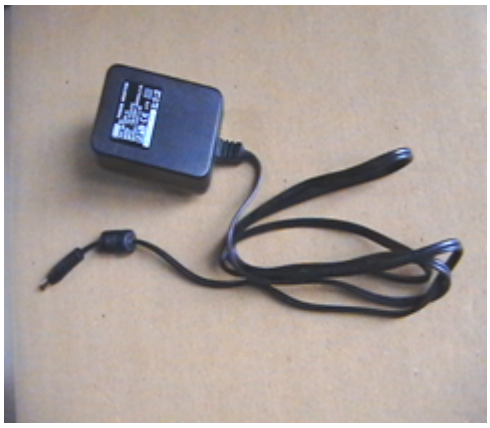
Impedance	50 ohms @ 13.56 MHz
Loaded Q	10 < Q < 30

3. Connection Procedure

3.1. Power Supply Connection procedure



Power supply connector

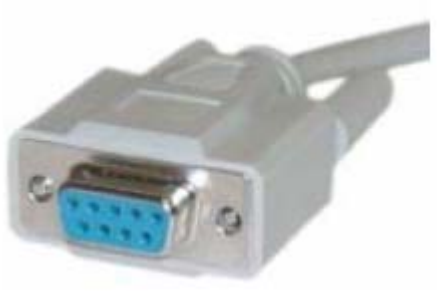


15 volts DC adapter

The reader has an interface connector for power supply. The location of the power supply connector is shown in the above picture. A 15 V DC adapter with 1 A current rating is used to power the reader.

3.2. RS232 serial port interfacing procedure

A RS232 serial cable which has a RS232 DB9 female connector at both ends is used for serial communication.



RS232 DB9 female connector

Data transmission through the serial port is carried out using only 3 pins of the DB9 female connector as shown below.

Pin Number	Signal
DB2	TX
DB3	RX
DB5	GND
DB1,DB4,DB6,DB7,DB8,DB9	NC

The serial port communication setting of the reader is given below.

Baud rate : 19200 bps

Start bit : 1 bit

Data bits : 8 bits

Stop bit : 1 bit

Flow control : None

4. Command and Response format

4.1 Protocol Frame

The Data can be transferred from host to reader and vice versa. The protocol frame is same for the host to reader as well as the Reader to Host transmission.

All bytes transfer occurs with the most significant bit (MSB) first.

1	2	3	4	5	6 … n-3	n-2	n-1	N
Start Byte (0x01)	Device Address	Antenna ID	Data Length	Command Byte	**Protocol Data**	**LRC**	**Separator Byte (0x03)**	Stop Byte (0x04)

Data Format

Start Byte

The start byte of any command is 0x01 (ASCII character 0x01).

Device Address

The reader can be addressed using the user defined reader identification number of one byte length. The default address of the reader is ‘0’. The reader ID ‘0’ is a universal ID for all readers, used particularly for configuring the readers in the distributed network. The reader has ID ‘1’ only will respond to such commands.

Antenna ID

The antenna ID byte denotes antenna number allocated for the antenna. The antenna ID for this reader is fixed as 0x01. The antenna ID will be 0x00 for all the ‘General commands’.

Data Length

The data length byte refers the length of single protocol data frame i.e., the number of bytes in a single command or response.

Command Byte

Command byte performs the function related to the byte. A brief description of the command byte used in various commands is listed below.

Function	Command byte
Get Firmware Version	0xCF
Check Reader Status	0xC0
Set baud rate	0xCD
Set Clock time	0XC5
Get Clock time	0XC6
Set Reader ID	0xC3
Get Reader ID	0xC4
Set/Reset Auto Visual	0xC2
Activate/Deactivate VAR	0xC1
Write reader memory	0xC7
Read reader memory	0xC8
Read Single Tag	0xF3

Function	Command byte
Get Multiple UID	0xF2
Write into nth block	0xF0
Read from nth block	0xF5
Write into nth block of particular transponder	0xF1
Read from nth block of particular transponder	0xF6
Write into nth block of particular transponder with password	0xF7
Write AFI	0xF8
Write DSFID	0xF9
Lock any memory block/ AFI/ DSFID	0xFA
Stay quiet	0xFC
Transmitter ON/OFF	0xF4

Protocol Data

The ‘Protocol Data’ refers to the Data of the command byte.

Separator Byte

The separator byte is 0x03 used by the reader only when sending the response to the ‘Read multiple tags’ command. This byte is used to separate one UID from the other.

Note: The ‘separator byte’ is an optional segment of the protocol frame. Depends on the response data and separator byte may exists zero or many times.

LRC Calculation

The Longitudinal Redundancy Check (LRC) is a one-byte data. LRC is calculated by adding the successive bytes in the command and discarding the carries and then two's complementing the result.

Stop Byte

The stop byte of any command is 0x04 (ASCII character 0x04). Care must be taken by the host to identify the correct 'stop byte' using the 'Data Length' byte.

UID representation

The UID is 8 byte length (64 bits) All UID's starts with 'E0h' as the first byte.

Timing Condition

Before sending the protocol start byte, there must be a minimum of 5 ms delay. The reader's reaction time to any given command is a maximum of 5 ms. The time delay between each character is maximum 1 ms. The host must make use of the 'Data length' byte to identify the correct stop byte(0x04).

For each command the reader will respond within 5 ms except the "Read Multiple UID" command for which the reader takes 300 ms to read all the tags present in the field.

Transponder memory and reader memory addressing methods

The transponder has 2K bits of memory which are organized as 64 blocks. Each block can store 4 characters. When accessing the transponder memory the first block has to be addressed as 0x01 and the 64^{th} block is addressed as 0x64. But when accessing the reader memory the first file, block and page are addressed by 0x00.

4.2 Commands and Responses

4.2. a General commands

4.2.1 Get Firmware Version

The 'Get Firmware Version' command gives the firmware version of the reader. The byte from B2 to B5 denotes firmware version is in ASCII format. B0 & B1 are used for manufacturer's reference.

Host → Reader

1	2	3	4	5	6	7
0x01	DEVICE_ID	0x00	0X07	[0xCF]	LRC	0x04

Reader → Host

1	2	3	4	5	6...11	12	13
0x01	DEVICE_ID	0x00	0x0D	[0xCF]	B0...B5	LRC	0x04

Command example:

Host to reader: 01 01 00 07 CF 28 04
Reader to host: 01 01 00 0D CF 52 34 56 34 32 31 AF 04

The ASCII equivalent of 52 – R
34 – 4
56 – V
34 – 4
32 – 2
31 – 1

So the firmware version is V4.2.1 (R4 is for manufacturer's reference).

4.2.2 Check Reader status

The 'Check reader status' command makes the reader to check whether all the modules are in working condition or not.

Host → Reader

1	2	3	4	5	6	7
0x01	DEVICE_ID	0x00	0X07	[0xC0]	LRC	0x04

Reader → Host

1	2	3	4	5	6	7	8
0x01	DEVICE_ID	0x00	0x08	[0xC0]	Error code	LRC	0x04

In response to the above command, one of the following codes gets displayed.

Code	**Message**
No response	Communication error
0X00	Reader Status GOOD
0X01	RF Error
0X02	Memory Error
0X03	RTC Error

Command example:

Host to reader: 01 01 00 07 C0 37 04
Reader to host: 01 01 00 08 C0 00 36 04

Since error code is zero no error.

4.2.3. Set Baud rate

The ‘Set Baud rate‘ command is used to set the selectable baud rate from 600 bps to 57600 bps except, listed below.

Host → Reader

1	2	3	4	5	6	7	8
0x01	DEVICE_ID	0x00	0x08	[0xCD]	DATA	LRC	0x04

Reader → Host

1	2	3	4	5	6	7	8
0x01	DEVICE_ID	0x00	0x08	[0xCD]	DATA	LRC	0x04

Select the suitable baud rate by giving the appropriate DATA value from the given table.

DATA	**Baudrate**
0x00	57600
0x01	19200
0x02	9600
0x03	4800
0x04	2400
0x05	1200
0x06	600

Command example:

Host to reader: 01 01 00 08 CD 01 28 04
Reader to host: 01 01 00 08 CD 01 28 04

Since the Baud rate DATA is 0x01, the device is set with baud rate of 19200
bps.

4.2.4. Set clock time

The ‘Set clock time’ command sets the clock time in the reader. The time and date should be set for real time based application.

Host → Reader

1	2	3	4	5	6 ... 12	13	14
0x01	DEVICE_ID	0x00	0x0E	[0XC5]	T0...T6	LRC	0x04

Reader → Host

1	2	3	4	5	6...12	13	14
0x01	DEVICE_ID	0x00	0x0E	[0xC5]	T0...T6	LRC	0x04

TIME:

6	7	8	9	10	11	12
T0_Sec	T1_Min	T2_Hour	T3_Day	T4_Date	T5_Month	T6_Year

Note: For T3_day: 0x00-Sun, 0x01-Mon, 0x02-Tue, 0x03-Wed, 0x04-Thu, 0x05-Fri and 0x06-Sat. The time get and set are in hexadecimal mode only. For example to set 27 sec in T0, set the fifth byte as 0x1B (hexadecimal value of 27 is 0x1B).

Command example:

Command is to set time 01:02:13(7 PM) 04 (Thursday) 15:06(June):07(2007).

Host to reader: 01 01 00 0E C5 01 02 13 04 15 06 07 EF 04
Reader to host: 01 01 00 0E C5 01 02 13 04 15 06 07 EF 04

4.2.5. Get Clock Time

The 'Get clock time' command get the current time and date of the reader. You can check the time and date set in the reader using this command.

Host → Reader

1	2	3	4	5	6	7
0x01	DEVICE_ID	0x00	0x07	[0XC6]	LRC	0x04

Reader → Host

1	2	3	4	5	6…12	13	14
0x01	DEVICE_ID	0x00	0x0E	0XC6	T0…T6	LRC	0x04

TIME:

6	7	8	9	10	11	12
T0_Sec	T1_Min	T2_Hour	T3_Day	T4_Date	T5_Month	T6_Year

Note: For T3_day: 0x00-Sun, 0x01-Mon, 0x02-Tue, 0x03-Wed, 0x04-Thu, 0x05-Fri and 0x06-Sat. The time get set and received in hexadecimal mode only.

Command example:

Host to reader: 01 01 00 07 C6 31 04
Reader to host: 01 01 00 0E C6 1E 07 13 04 15 06 07 CC 04

Time from the reader's response is 1E(30 secs): 07(min): 13(5PM)
04(Thursday)
15(date 21): 06(June) : 07 (2007).

4.2.6. Set Reader ID (Not applicable to 1 Watt reader since its ID is fixed as 0x01)

Set reader ID command is used the change the device ID of any reader connected in the network. On the execution of the command the host returns the new ID in the fifth byte. For further commands new DEVICE_ID is taken into account. The default DEVICE_ID of a reader is 0XFF.

. *Host → Reader*

1	2	3	4	5	6	7	8
0x01	DEVICE_ID	0x00	0x08	[0xC3]	DEVICE_ID	LRC	0x04

Reader → Host

1	2	3	4	5	6	7	8
0x01	DEVICE_ID	0x00	0x08	[0xC3]	DEVICE_ID	LRC	0x04

Command example:

This example command is to set reader ID as 0x01, if the current ID is not known, 0x00 can be used instead of the current ID.

Host to reader: 01 00 00 08 C3 01 33 04
Reader to host: 01 00 00 08 C3 01 33 04

If the current ID is known and if its 0x02, to change the reader ID as 0x01,

Host to reader: 01 02 00 08 C3 01 31 04
Reader to host: 01 02 00 08 C3 01 31 04

4.2.7 Get Reader ID

Only one reader must be connected during the execution of this command. The Get Reader ID command reveals the device address of a single reader.

Host → Reader

1	2	3	4	5	6	7
0x01	DEVICE_ID	0x00	0x07	[0xC4]	LRC	0x04

Reader → Host

1	2	3	4	5	6	7	8
0x01	DEVICE_ID	0x00	0x08	[0xC4]	DEVICE_ID	LRC	0x04

Command example:

Host to reader: 01 00 00 07 C4 34 04
Reader to host: 01 00 00 08 C4 01 32 04

From the reader's response, the ID is 0x01. The DEVICE_ID of this command is always 0x00.

4.2.8 Set / Reset Auto visual

Enabling the 'Set / Reset auto visual 'command makes the reader to glow the Green LED for a short interval of time, when a valid RF functions like reading UID and read/write tag memory, etc., is performed by the reader. On disabling the function the red LED gets off. If the 'Auto Visual' feature is enabled it will consume little more time to make the LED glow.

Host → Reader

1	2	3	4	5	6	7	8
0x01	DEVICE_ID	0x00	0x08	[0xC2]	Data	LRC	0x04

Reader → Host

1	2	3	4	5	6	7	8
0x01	DEVICE_ID	0x00	0x08	[0xC2]	Data	LRC	0x04

Data byte

Data	Function
0x00	LED Off
0x01	LED On

Note: Disabling this function will improve the reader response time, in RF functions

Command example:

To activate the auto visual function the Data byte is 0x01.

Host to reader: 01 01 00 08 C2 01 33 04
Reader to host: 01 01 00 08 C2 01 33 04

4.2.9. Activate / Deactivate VAI (Visual and Audio Interface)

The 'Activate / Deactivate VAI'command makes the reader to switch ON / OFF the LED's and buzzer of the Reader. Setting the appropriate bits in the 'VAR - 6th byte' makes the LED and buzzer to get switched ON.

Host → Reader

1	2	3	4	5	6	7	8
0x01	DEVICE_ID	0x00	0x08	[0xC1]	VAR	LRC	0x04

Bit wise connection of components related to VAR byte.

VAR	Component	Status
D7	X	Don't care
D6	X	Don't care
D5	X	Don't care
D4	Relay2	Disconnect
D3	Relay1	Disconnect
D2	Buzzer	Connect
D1	LED2	Connect
D0	LED1	Connect

Reader → Host

1	2	3	4	5	6	7	8	9
0x01	DEVICE_ID	0x00	0x09	[0xC1]	VAR	Data2	LRC	0x04

Note: In the command byte DATA if a invalid bit is set, the response Data2 will have a value with same bit set, otherwise it's 0x00 for indicating 'no error'.

Command example:

This example command is make the LED1 glow, Buzzer to beep, Relay1 to be activated and to switch off the LED2 and Relay2. So the binary pattern of the Data byte should be 0000 1101 = 0x0D.

Host to reader: 01 01 00 08 C1 0D 28 04
Reader to host: 01 01 00 09 C1 0D 00 27 04

4.2.10 Write reader memory

The reader has inbuilt non volatile memory of 2 MBits size. The memory is divided into two files. Each file is divided into two blocks. Each block contains 256 pages whereas each page is 256 Bytes size. The host can access maximum 16 bytes of memory at a time. It is mandatory that all the 16 bytes should be of same page. The 256th page of each block is utilized for system purpose and is not available for the host access.

Host → Reader

1	2	3	4	5	6..9	10...n	n+1	n+2
0x01	DEVICE_ID	0x00	Data length*	[0xC7]	Addr & Length	Bytes to be written	LRC	0x04

Reader → Host

1	2	3	4	5	6..9	10...n	n+1	n+2
0x01	DEVICE_ID	0x00	Data length*	[0xC7]	Addr & Length	Bytes written	LRC	0x04

Addr & Length (6...9)			
File and Block No	Page address	Starting byte address	No of bytes to be written

Data for block specifications

FILE	BLOCK NO
0X00	File 0 and Block 0
0X01	File 0 and Block 1
0X10	File 1 and Block 0
0x11	File 1 and Block 1

*** The 'Data Length' byte is not a fixed one for this command as the number of bytes to be written may vary from 1 to 16.**

Note: The file, block and page address starts with 0x00 unlike the transponder memory address.

Command example:

To write a sentence PICO MEGA in File 1& Block 0 the 6th byte is 0x10. To write the page address 0x00, the seventh byte is 0x00 and the starting address 0x00, so the 8th byte as well 0x00. Ninth byte 0x09 denotes the no of byte in the sentence, ie. in PICO MEGA there are 9 characters including the space(0x20). The hexadecimal values staring from 0x50 to 0x41 are the Hex equivalent of PICO MEGA. The command is Host to reader：`01 01 00 14 C7 10 00 00 09 50 49 43 4F 20 4D 45 47 41 A5 04` Reader to host：`01 01 00 14 C7 10 00 00 09 50 49 43 4F 20 4D 45 47 41 A5 04`

4.2.11 Read reader memory

The reader has inbuilt non volatile memory of 2 MBits size. The memory is divided into two files. Each file is divided into two blocks. Each block contains 256 pages whereas each page is 256 Bytes size. The host can access maximum 16 bytes of memory at a time. It is mandatory that all the 16 bytes should be of same page. The 256th page of each block is utilized for system purpose and is not available for the host access.

Host → Reader

1	2	3	4	5	6..9	10	11
0x01	DEVICE_ID	0x00	0x0B	[0xC8]	Addr & Length	LRC	0x04

Reader → Host

1	2	3	4	5	6..9	10...n	n+1	n+2
0x01	DEVICE_ID	0x00	Data length*	[0xC8]	Addr & Length	Bytes written	LRC	0x04

Addr & Length (6...9)			
File and Block No	Page address	Starting byte address	No of bytes to be accessed

Data for block specifications

FILE	BLOCK NO
0X00	File 0 and Block 0
0X01	File 0 and Block 1
0X10	File 1 and Block 0
0x11	File 1 and Block 1

***The 'Data Length' byte is not a fixed one for this command as the number of bytes to be written may vary from 1 to 16**

Command example:

To read a data from File 1& Block 0 the 6th byte is 0x10. To write the page address 0x00, the seventh byte is 0x00 and the starting address 0x00, so the 8th byte as well 0x00. Ninth byte 0x10 denotes the no of byte (16 in decimal) to be read from the starting address.

The command to read memory

Host to reader： 01 01 00 0B C8 10 00 00 10 0B 04

Reader to host：01 01 00 1B C8 10 00 00 10 50 49 43 4F 20 4D 45 47 41 FF FF FF FF FF FF FF 9D 04

Note that in the 16 bytes read, the first 9 bytes have values for PICO MEGA (starting from 50 to 41) and the rest of the bytes are FF indicates blank memory byte.

4.2. b. RF related Commands

4.2.12. Read Single Tag UID

The 'Read Single Tag UID' command is used to get the UID of a transponder exists in the field. When executing this command the reader assumes that there is only one tag exists in the field.

Host → Reader

1	2	3	4	5	6	7
0x01	DEVICE_ID	ANTENNA_ID	0X07	[0xF3]	LRC	0x04

Reader → Host

1	2	3	4	5	6..13	14	15
0x01	DEVICE_ID	ANTENNA_ID	0x0F	[0xF3]	UID	LRC	0x04

Command example:

Host to reader: `01 01 01 07 F3 03 04`
Reader to host: `01 01 01 0F F3 E0 04 01 00 0A 36 A0 68 CE 04`

The UID of the tag read is E00401000A36A068.

4.2.13. Read Tags in auto anti-collision mode

The 'Read Tags in auto anti-collision mode' command makes the reader to get all the UID's of the transponders exist in the field. The response time of the reader is 400 mS.

Host → Reader

1	2	3	4	5	6	7
0x01	DEVICE_ID	ANTENNA_ID	0X07	[0xF2]	LRC	0x04

Reader → Host

1	2	3	4	5	6..13	14	15	16
0x01	DEVICE_ID	ANTENN_ID	0x10	[0xF2]	UID	LRC	0x03	0x04

Note: A separator byte is sent as the 15th byte in the response to separate the UID's from one another. The reader will send a stop byte 0x04 after the separator byte only with the last UID to indicate the end of the response or it will send the start byte (0x01) if another UID get detected.

Command example:

Host to reader: 01 01 01 07 F2 04 04
Reader to host: 01 01 01 0F F2 E0 04 01 00 08 2F 4C C6 CE 03
01 01 01 0F F2 E0 04 01 00 0A 36 A0 68 CF 03 04

The two UIDs read are E0040100082F4CC6 & E00401000A36A068. Note that a separator
byte 0x03 comes for every UID.

4.2.14. Write to nth block

The 'Write to nth block' command makes the reader to write a 4 byte data into a particular memory block of the transponder.

Host → Reader

1	2	3	4	5	6	7..10	11	12
0x01	DEVICE_ID	ANTENN_ID	0x0C	0xF0	Block Number in Hex	4 Byte Data	LRC	0x04

Reader → Host

1	2	3	4	5	6	7..10	11	12
0x01	DEVICE_ID	ANTENN_ID	0x0C	0xF5	Block Number in Hex	4 Byte Data	LRC	0x04

Note:

(i) The command byte in the response is 0xF5 not 0xF0 as the written data in the block is read once to confirm it.

(ii) The first block address is 0x00.

Command example:

This example command is to write a 4 byte data (ABCD) in 3rd block (0x02 since first block ID is 0x00).

Host to reader: 01 01 01 0C F0 02 41 42 43 44 F5 04
Reader to host: 01 01 01 0C F5 02 41 42 43 44 F0 04

Note that in the response the command byte is 0xF5. 0x41..0x44 are Hex values of
ABCD.

4.2.15. Read from nth block

The 'Read from nth block' command makes the reader to read a 4 byte data from a particular memory block of the transponder.

Host → Reader

1	2	3	4	5	6	7	8
0x01	DEVICE_ID	ANTENNA_ID	0x08	[0xF5]	Block Number in Hex	LRC	0x04

Reader → Host

1	2	3	4	5	6	7..10	11	12
0x01	DEVICE_ID	ANTENN_ID	0x0C	[0xF5]	Block Number in Hex	4 Byte Data	LRC	0x04

Note:

(i) To Read/write data in multiple blocks at a time, do it block by block with a delay of 10 ms.

(ii) The first block address is 0x00.

Command example:

This example command is to from 3rd block (0x02 since first block ID is 0x00).

Host to reader: 01 01 01 08 F5 02 FE 04
Reader to host: 01 01 01 0C F5 02 41 42 43 44 F0 04

0x41..0x44 are Hex values of ABCD.

4.2.16. Write into nth block of particular tag

The 'Write into nth block of a particular tag' command makes the reader to write a 4 byte data into a particular block of a given transponder whose UID is mentioned in the command.

Host → Reader

1	2	3	4	5	6..13	14	15..18	19	20
0x01	DEVICE_ID	ANTENN_ID	0x14	[0xF1]	UID	Block Number in Hex	4 Byte Data	LRC	0x04

Reader → Host

1	2	3	4	5	6..13	14	15..18	19	20
0x01	DEVICE_ID	ANTENN_ID	0x14	[0xF6]	UID	Block Number in Hex	4 Byte Data	LRC	0x04

Note:

(i) The command byte in the response is 0xF6 not 0xF1 as the written data is read once to ensure it.

(ii) The first block address is 0x00.

Command example:

This example command is to write a 4 byte data (EFGH) in 3rd block (0x02 since first block ID is 0x00).

Host to reader: `01 01 01 14 F1 E0 04 01 00 0A 36 A0 68 02 45 46 47 48 AF 04`
Reader to host: `01 01 01 14 F6 E0 04 01 00 0A 36 A0 68 02 45 46 47 48 AA 04`

```
Note that in the response the command byte is 0xF6 not 0xF1.
0x45, 0x46, 0x47 & 0x48 are Hex values of EFGH.
```

4.2.17. Read from nth block of particular tag

The 'Read from nth block of a particular tag' command makes the reader to read a 4 byte data from a particular block of a given transponder whose UID is mentioned in the command.

Host → Reader

1	2	3	4	5	6..13	14	15	16
0x01	DEVICE_ID	ANTENN_ID	0x10	[0xF6]	UID	Block Number in Hex	LRC	0x04

Reader → Host

1	2	3	4	5	6..13	14	15..18	19	20
0x01	DEVICE_ID	ANTENN_ID	0x14	[0xF6]	UID	Block Number in Hex	4 Byte Data	LRC	0x04

(i) The first block address is 0x00.

Command example:

This example command is to from 3rd block (0x02 since first block ID is 0x00).

Host to reader: `01 01 01 10 F6 E0 04 01 00 0A 36 A0 68 02 C8 04`

Reader to host: `01 01 01 14 F6 E0 04 01 00 0A 36 A0 68 02 45 46 47 48 AA 04`

From the response its found that the values in 3rd block of the UID mentioned in the command is `0x45, 0x46, 0x47 & 0x48 which are Hex values of EFGH.`

4.2.18. Write into nth block of particular tag with password

The 'Write into nth block of a particular tag with password' command makes the reader to write a 4 byte data into a particular block of a given transponder, whose UID is mentioned in the command along with a password. This is a custom command for Texas Instruments TI HF-I PRO tags. This command helps in allowing locked EEPROM data memory block to be rewritten if the password to that tag is known to a user.

Host → Reader

1	2	3	4	5	6..13	14..17	18	19..22	23	24
0x01	DEVICE_ID	ANT_ID	0x1F	[0xF7]	UID	Password	Block Number in Hex	4 Byte Data	LRC	0x04

Reader → Host

1	2	3	4	5	6..13	14	15..18	19	20
0x01	DEVICE_ID	ANT_ID	0x1F	[0xF6]	UID	Block Number in Hex	4 Byte Data	LRC	0x04

Note:

(i) The command byte in the response is 0xF6 not 0xF1 as the written data is read once to ensure it.

(ii) The first block address is 0x00.

Command example:

This example command is to write a 4 byte data (EFGH) in 3rd block (0x02 since first block ID is 0x00).

Host to reader : `01 01 01 18 F7 E0 07 C4 D2 E5 C2 42 9C 2A 2A 2A 2A 02 45 46 47 48 28 04`

Reader to host: `01 01 01 14 F6 E0 07 C4 D2 E5 C2 42 9C 02 45 46 47 48 D5 04`

Note that in the command after the UID there are 4 bytes (all 2A) which is the
password of the tag. Password is nothing but the data written and locked in the block 0x0B of Ti's HF-I PRO tags.

In the response the command byte is 0xF6 not 0XF7. 0x45, 0x46, 0x47 & 0x48 are Hex values of EFGH.

4.2.19. Write AFI of particular transponder

The 'Write AFI' command makes the reader to write a single byte data in the AFI block of the tag whose UID is mentioned in the command.

Host → Reader

1	2	3	4	5	6..13	14	15	16
0x01	DEVICE_ID	ANTENNA_ID	0X10	[0xF8]	UID	DATA	LRC	0x04

Reader → Host

1	2	3	4	5	6..13	14	15	16
0x01	DEVICE_ID	ANTENNA_ID	0X10	[0xF8]	UID	DATA	LRC	0x04

Command example:

This example command is to write a byte in the AFI of the tag whose UID is mentioned in the command.
The UID of the card in the command is `E007000001CD4245.`

Host to reader: `01 01 01 10 F8 E0 07 00 00 01 CD 42 45 59 60 04`
Reader to host: `01 01 01 10 F8 E0 07 00 00 01 CD 42 45 59 60 04`

The byte written is 0x59. '5' is written in Most Significant Nibble and '9' is written in Least significant nibble.

4.2.20. Write DSFID of particular transponder

The 'Write DSFID' command makes the reader to write a single byte data in the DSFID block of the tag whose UID is mentioned in the command.

Host → Reader

1	2	3	4	5	6..13	14	15	16
0x01	DEVICE_ID	ANTENNA_ID	0X10	[0xF9]	UID	DATA	LRC	0x04

Reader → Host

1	2	3	4	5	6..13	14	15	16
0x01	DEVICE_ID	ANTENNA_ID	0X10	[0xF9]	UID	DATA	LRC	0x04

Command example:

This example command is to write a byte in the DSFID of the tag whose UID is mentioned in the command.
The UID of the card in the command is E007000001CD4245.

Host to reader: 01 01 01 10 F9 E0 07 00 00 01 CD 42 45 18 A0 04
Reader to host: 01 01 01 10 F9 E0 07 00 00 01 CD 42 45 18 A0 04

The value written in the DSFID is 0x18.

4.2.21. Lock any memory block / AFI / DSFID of particular transponder

The 'Lock any memory block / AFI / DSIFID of particular transponder' command makes the reader to set the lock bit of a particular memory block or AFI or DSFID of the tag whose UID is mentioned in the command. The number of bytes in the command for locking the memory block is two bytes and for locking the AFI and DSFID is one byte.

The DATA1 field denotes whether a memory block or AFI or DSFID is selected for locking. The DATA2 denotes the block number of the selected memory. DATA2 field is not required for AFI and DSFID.

Lock any Memory block

Host → Reader

1	2	3	4	5	6..13	14	15	16	17
0x01	DEVICE_ID	ANTENNA_ID	0X11	[0xFA]	UID	DATA1	DATA2	LRC	0x04

Reader → Host

1	2	3	4	5	6..13	14	15	16	17
0x01	DEVICE_ID	ANTENNA_ID	0X11	[0xFA]	UID	DATA1	DATA2	LRC	0x04

Lock AFI / DSFID

Host → Reader

1	2	3	4	5	6..13	14	15	16
0x01	DEVICE_ID	ANTENNA_ID	0X08	[0xFA]	UID	DATA1	LRC	0x04

Reader → Host

1	2	3	4	5	6..13	6	7	8
0x01	DEVICE_ID	ANTENNA_ID	0X08	[0xFA]	UID	DATA1	LRC	0x04

DATA1 Byte

DATA1	To LOCK
0x00	Memory
0x01	AFI
0x02	DSFID

Command example:

This example command is to lock the AFI of the tag whose UID is mentioned in the command.
The UID of the card in the command is `E007C4D2E5C2429C`.

Host to reader: `01 01 01 10 FA E0 07 C4 D2 E5 C2 42 9C 01 F0 04`
Reader to host: `01 01 01 10 FA E0 07 C4 D2 E5 C2 42 9C 01 F0 04`

Since the byte that comes after the UID is 0x01, the reader will lock the AFI of the card.

To lock the DSFID, the byte that comes after the UID should be 0x02.

To lock a particular block, the byte that comes after the UID should be 0x00 followed by the block number. So the command to lock the block has one more byte. One example is given below.

Host to reader: `01 01 01 10 FA E0 07 C4 D2 E5 C2 42 9C 00 0B E5 04`
Reader to host: `01 01 01 10 FA E0 07 C4 D2 E5 C2 42 9C 00 0B E5 04`

Since the byte that comes after the UID is 0x00, it's a lock block command and the block number is mentioned as 0x0B. On receiving this command the reader will lock the block 0x0B.

4.2.22. Stay quiet

Execution of the 'Stay quiet' command makes the tag with the mentioned UID, to become quiet for the forthcoming RF commands. There will be no response to this command. After the execution of the 'Stay quiet', the tag will not respond to any 'non-addressed' and inventory related commands. However the tag will respond to the request with the matching UID. This property gets lost when the Transmitter is turned OFF or if the Tag is moved out of the RF field.

Host → Reader

1	2	3	4	5	6...13	14	15
0x01	DEVICE_ID	ANTENNA_ID	0X17	[0xFC]	UID	LRC	0x04

Reader → Host

[No response from the reader]

Command example:

This example command is to make the tag whose UID is mentioned in the command, to be quiet. The UID of the card in the command is `E007C4D2E5C2429C`.

Host to reader: `01 01 01 0F FC E0 07 C4 D2 E5 C2 42 9C F0 04`

`(No response from the reader)`

4.2.23. Transmitter ON / OFF

The 'Transmitter ON / OFF' command is used to turn ON / OFF the transmitter of the reader. It means that on receiving this command the reader will turn ON/OFF the generation of 13.56 MHz electromagnetic carrier field at the antenna.

Host → Reader

1	2	3	4	5	6	7	8
0x01	DEVICE_ID	ANTENNA_ID	0X08	[0xF4]	DATA	LRC	0x04

Reader → Host

1	2	3	4	5	6	7	8
0x01	DEVICE_ID	ANTENNA_ID	0X08	[0xF4]	DATA	LRC	0x04

DATA Byte

DATA	Transmitter
0x00	OFF
0x01	ON

Command example:

This example command is to switch ON the transmitter.

Host to reader: 01 01 01 08 F4 01 00 04
Reader to host: 01 01 01 08 F4 01 00 04

Since the byte that comes after the command byte is 0x01 the reader will switch ON the transmitter.

This example command is to switch OFF the transmitter.

Host to reader: 01 01 01 08 F4 00 01 04
Reader to host: 01 01 01 08 F4 00 01 04

Since the byte that comes after the command byte is 0x00 the reader will switch OFF the transmitter.

4.2. c. Common response to all the RF commands

In the RF related commands, when there is no transponder in the field of the reader, the response as below.

Reader → Host

1	2	3	4	5	6	7
0x01	DEVICE_ID	Antenna ID	0X07	[0xFF]	LRC	0x04