

Chapter 3 • Power & Communication Configuration

This chapter describes the electrical options, power requirements and communication configuration of the HF-0405 Series RFID Controller.

Power Requirements

To function properly, the HF-0405 must be powered by a power supply capable of providing voltages of 10 to 30 volts DC, with an Operating Range of 180mA and a Surge Current of 250mA.

Refer to [Appendix B](#) for power supplies offered by Escort Memory Systems.



Warning about “Hotplugging”



Never connect or disconnect the HF-0405 while the power is on. This is sometimes referred to as “Hotplugging”. Turn power off prior to plugging or unplugging the controller. Reapply power only after the unit is reconnected.



Serial Interface Options

There are three distinct versions of the HF-0405 RFID Controller. Each version provides supports for one specific serial interface requirement. Prior to purchasing one or more HF-0405 Series RFID Controllers, determine which of the three serial interface protocols your Host and RFID application will require.

HF-0405 Model Numbers and Supported Serial Interface Protocols

HF-0405 Model Number	Supported Serial Interface	Usage	Recommended Maximum Cable Length
HF-0405-232-01	RS232	Point-to-Point Host/Controller	15 Meters
HF-0405-422-01	RS422	Point-to-Point Host/Controller	50 Meters
HF-0405-485-01	RS485	Subnet16™ Multidrop bus architecture, support for up to 16 connection nodes through HF-Gateway Controller.	1000 Meters



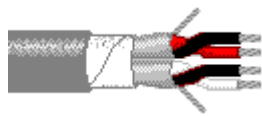
RS232 Interface Connection



In a point-to-point configuration where the distance from the Host to the HF-0405 is less than 15 meters, it is possible to connect the two through an RS232 serial interface connection.

The recommended cable medium for RS232 communication is produced by Belden, part number 9941. This cable is non-paired, 22 AWG stranded (7x30) tinned copper with S-R PVC insulation. Specifications for Belden cables can be found at WWW.BELDEN.COM.

RS422 Interface Connection



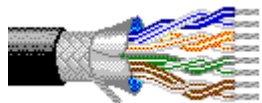
RS422 will support cable lengths up to 50m for point-to-point Host/Controller connections (provided adequate gauge cabling is used for power and signals).

In installations where long cable runs must be used, or in electrically noisy environments, RS422 is the communications standard of choice for point-to-point serial communications. The recommended cable medium is Belden part number 3084A, or Belden part number 3082A.

With a maximum Baud Rate of 38.4kBaud, it is generally unnecessary to terminate the RS422 terminals to match the impedance of the cable. This provides a functional impedance match at all baud rates up to 38.4KBaud, the maximum rate supported by the HF-0405 RFID Controller.

The RS422 receiver within the HF-0405 RFID Controller has failsafe protection circuitry which eliminates the need for any pull-up or pull-down resistors on the RS422 lines.

RS485 Interface Connection



RS485 supports Subnet16™ Multidrop bus architecture and protocol, allowing for up to 16 connection nodes on one bus connected through a Subnet16 Gateway.

The HF-0405-485 uses an M12 (12mm Eurofast) Male 5-pin connector.

Making Connections

Connect the HF-0405 to the appropriate serial interface on the Host: **RS232, RS422 or RS485.**

Connecting the HF-0405 to the Host

1. Connect the female end of your M12 serial communications cable to the male plug on the HF-0405.
2. Connect the other end of the serial communications cable to your Host's COM1 port (RS232 or RS422 compatible).
3. Note COM1 default settings of *9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control.* Make modifications if needed.
4. Connect your power supply connector to the HF-0405.
5. Turn on the power supply, LEDs on unit should illuminate.

COM Port Configuration

In normal use for reading and writing to RFID tags, communications with the HF-0405 RFID Controller can be accomplished via the COM1 serial communications port on the Host computer. The COM 1 communications interface can be accessed by both point-to-point and addressed serial communications protocols.

For point-to-point serial communication, the HF-0405 RFID Controller supports RS232 and RS422 as the standard protocols. For multiplexed communications (where more than one RFID controller will be used), RS485 (Ethernet) is an available option. Both RS232 and RS422 interfaces are optically isolated. The RS422 interface is especially suited for long cable lengths, and for noisy environments.

Applications that require long cable runs should be configured to avoid creating data transmission delays of over 200 milliseconds between the Host and controller.

COM Port Parameter Options

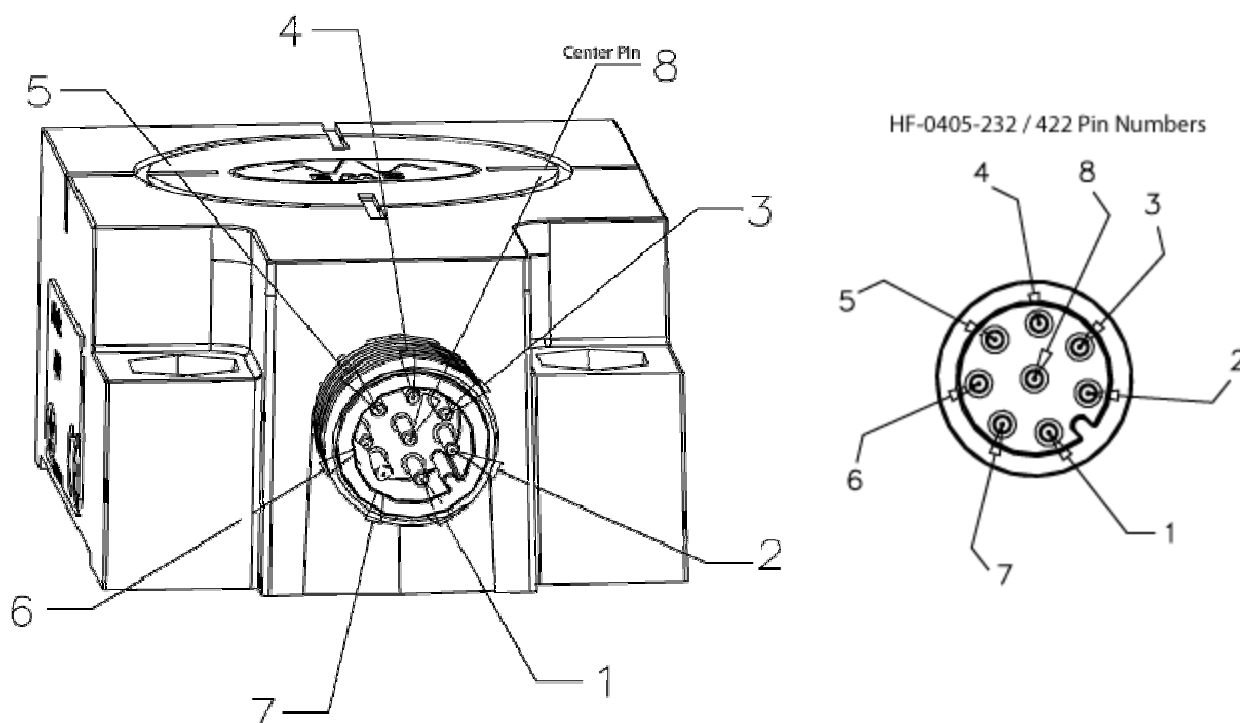
COM 1 Options and Default Settings

Configuration Parameter	Available Choices	Default Setting
Baud Rate (in BPS)	1200, 2400, 4800, 9600, 19200, 38400	9600
Data Bits	7, 8	8
Stop Bits	0, 1	1
Parity	Even, Odd, None	None
Handshake	None, Xon/Xoff	None



Pinouts

HF-0405-232/422 Pinouts



RS232 - Pin Descriptions

1. 24V DC PWR
2. 0V (Power GND)
3. N.C.
4. N.C.
5. N.C.
6. RX
7. TX
8. Shield (Communication GND)

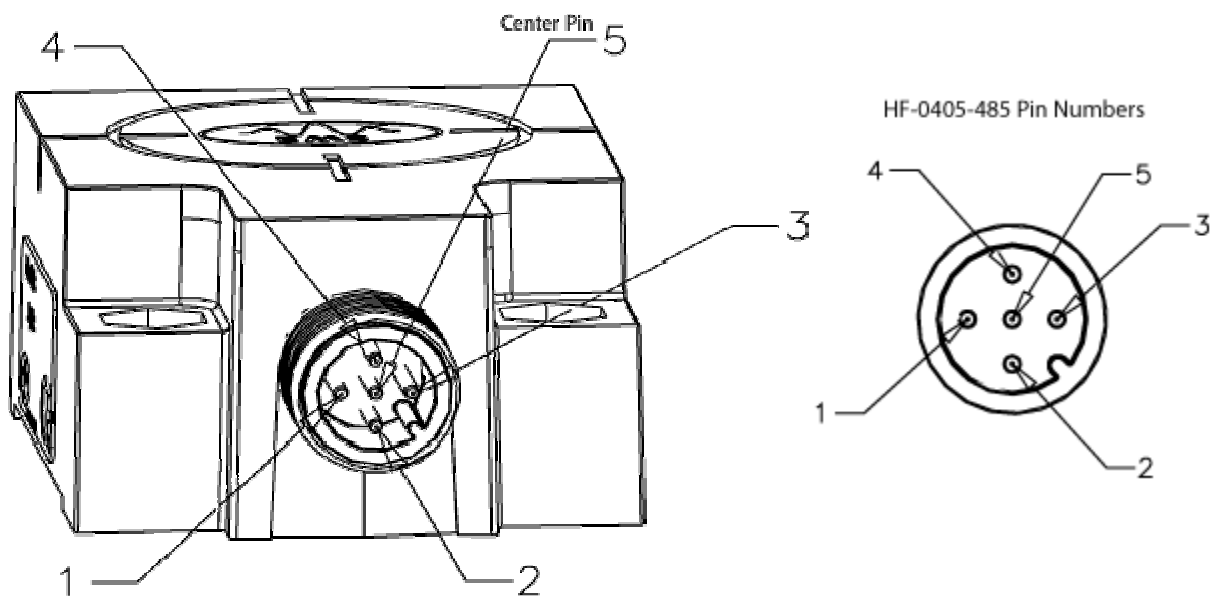
RS422 - Pin Descriptions

1. 24V DC PWR
2. 0V (Power GND)
3. TX+
4. TX-
5. RX+
6. RX-
7. TX232
8. Shield (Communication GND)

N.C. = Not Connected



HF-0405-485 Pinouts



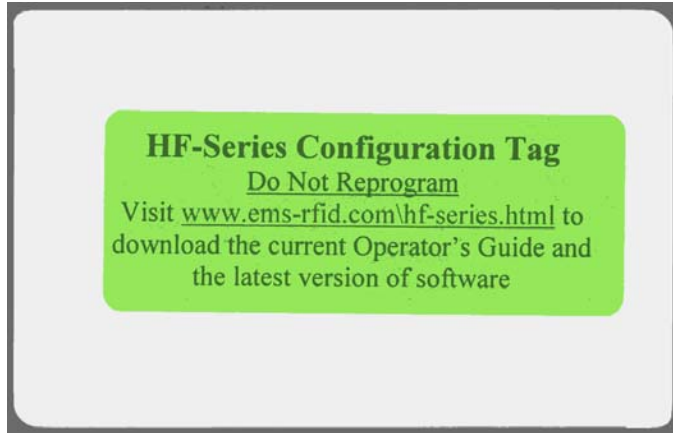
RS485 - Pin Descriptions

1. Shield (Communication GND)
2. 24V DC PWR
3. 0V (Power GND)
4. TX/RX+
5. TX/RX-

The Configuration Tag

Configuration Tag Overview

In the past, RFID controllers had multiple jumpers and dip switches which were used to set configuration parameters. The HF-0405 Controllers have no switches and are software configurable via commands. In the event that serial communication parameters are improperly assigned, recycle power to the RFID controller and place the configuration card in the RF field. When power returns to the controller, factory default settings will be reset.



The Configuration Tag is unique for every HF-0405 Controller and contains specific manufacturing data which can be valuable in troubleshooting a system. The configuration tag is a 112-byte ISO 15693 compliant tag that has much of the memory locked at the factory to prevent important data from being overwritten. As noted above, this tag can also be used to restore factory defaults in the event that serial communications become programmed to an unknown state. It is recommended to write the product serial number on the tag and store it in a safe place.

For testing and demonstration purposes, certain addresses have not been locked and can be written to. For the HF-0405-485-01 controller, this configuration tag can be used to manually set Subnet16™ node addresses.

Configuration Tag Memory Map

The HF-0405 Configuration Tag is a 112-byte tag, where the first 16-bytes (addresses 00 - 15) are used to store factory default settings and specific product ID information. Some of the remaining memory is used in the manufacturing process to record production and test data.

Using the Configuration

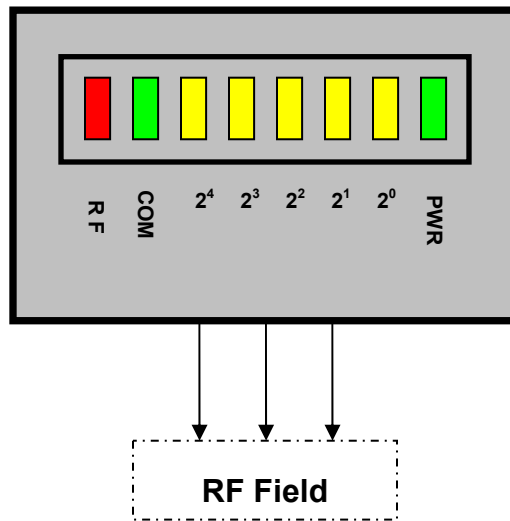
To restore factory default settings to the HF-0405 follow the steps below.

Chapter 4 • LED Status

This chapter describes the functions of the LEDs on the HF-0405 and explains their error condition messages.


The HF-0405 Series RFID Controllers have eight LEDs. The LEDs are conveniently located on the top panel of the HF-0405 and display everything from RF and COM activity to tag presence, diagnostic information and power status.


Normal LED Operation Functions




LED Color	Red	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Green
Function	RF Activity	COM Activity	Node 2 ⁴ (16)	Node 2 ³ (8)	Node 2 ² (4)	Node 2 ¹ (2)	Node 2 ⁰ (1)	Power On


LED Descriptions

 **RF LED**, Color is Red: the RF LED will turn on when RF power is being transmitted from the antenna and stays on during entire RF operation. By default, this occurs each time an RF command is being executed.

 **COM LED**, Color is Green: the COM LED indicates that data is being sent or received. On receipt of a command, the COM LED will begin flashing on and off rapidly. After the controller issues the command response, the COM LED flashing will halt.

When a continuous read command is sent, the COM LED will stay on and will turn off briefly only while data is being read or written to a tag.

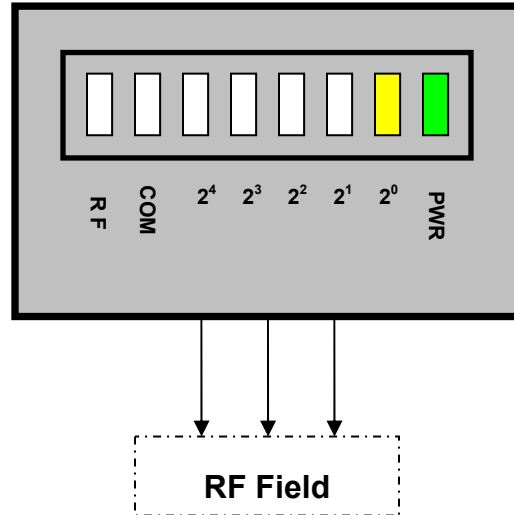
 **Node Address LEDs**, Colors are Yellow: Weighted by powers of 2, these five LEDs indicate the serial communications type for HF-0405-232 and HF-0405-422 models. For the HF-0405-485 model, the five yellow LEDs are used to indicate the current Subnet16 address of the HF-0405-485 model (See below).

 **Power LED**, Color is Green: Power LED will remain on while power is applied to the HF-0405.



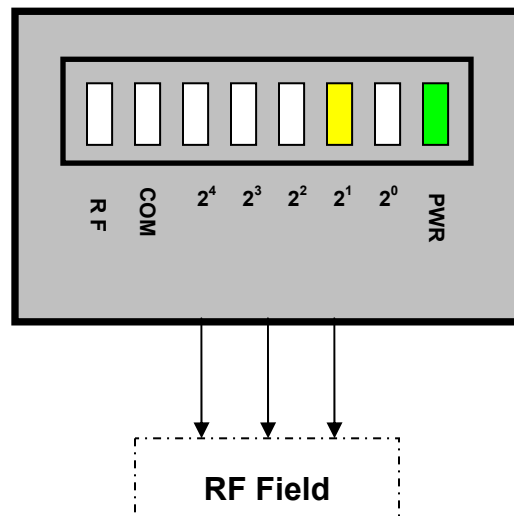
HF-0405-232 LED Status

On the HF-0405-232 model, the yellow LED 2^0 should be on steady state to indicate RS232 mode.



HF-0405-422 LED Status

On the HF-0405-422 model, the yellow LED 2^1 should be on steady state to indicate RS422 mode.

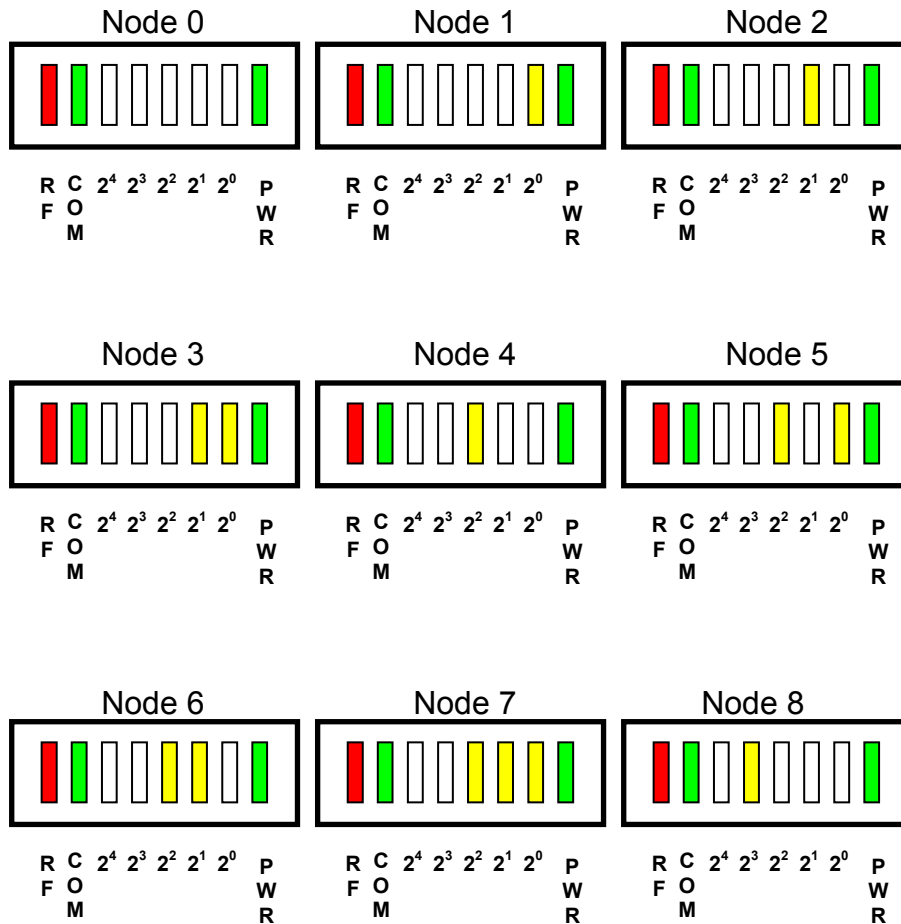


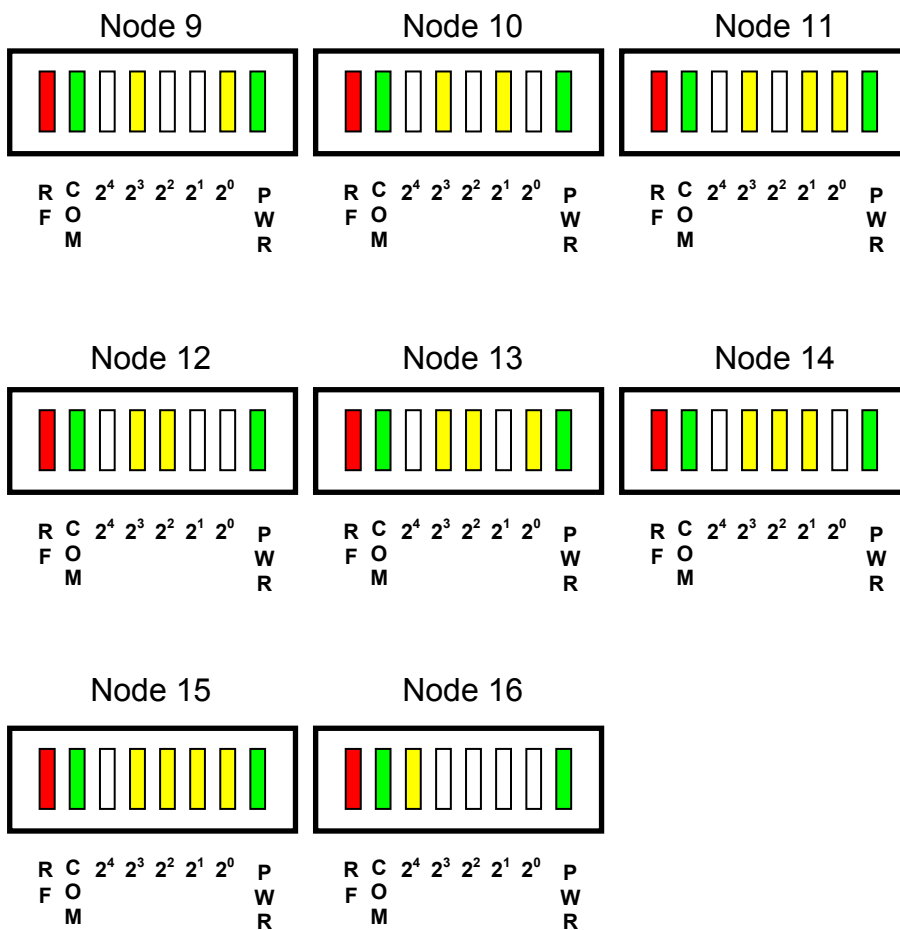
HF-0405-485 LED Status

The five yellow LEDs on the HF-0405-485 indicate Subnet16 node address (used in conjunction with Escort Memory Systems' Subnet16 Gateway or Subnet16 Hub). Weighted by powers of 2, the yellow LEDs indicate (in binary) the current Subnet16 node address assigned to the HF-0405-485. For example: $2^0 = 0x01$ (node 1), $2^1 = 0x02$ (node 2), $2^2 = 0x04$ (node 4), $2^3 = 0x08$ (node 8), $2^4 = 0x10$ (node 16). There are 16 functional Subnet16 node addresses (1 – 16).

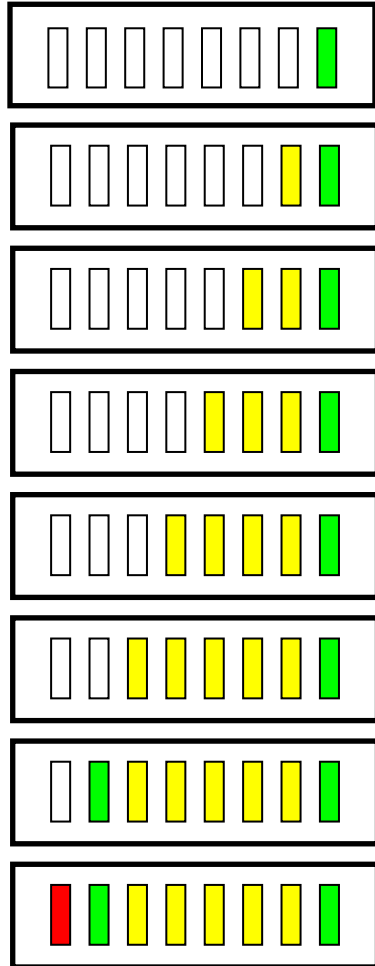
The HF-0405-485 is shipped with the default address of node 0. After it has been recognized by the Subnet16 Gateway or Hub, it will be assigned the next available Subnet16 node address (1 through 16). For configuring the node address or resetting the node address using the configuration card, see [Chapter 3 – the Configuration Tag](#).

Subnet16 Node Addresses for the HF-0405-485

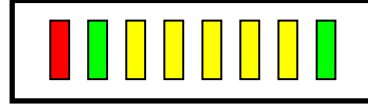




Special LED Operation Functions

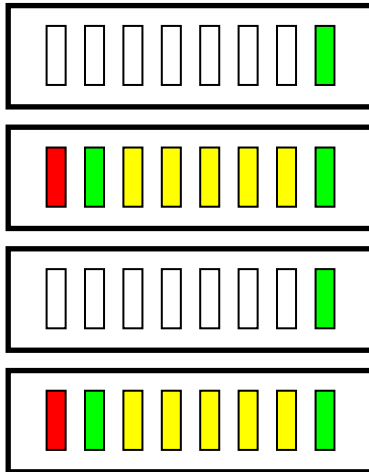


Updating Firmware (Part 1)

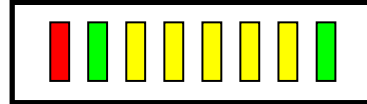


With the PWR LED on the right, the LEDs will illuminate one at a time sequentially from right to left to indicate that the firmware update file is being copied to internal memory.

The LEDs will repeat this R to L sequence until the controller has completely received the firmware update file.



Updating Firmware (Part 2)



After the update file has been copied to internal memory, the LEDs will blink on and off repeatedly during which time the update file is being written to flash memory.

Warning: do not cancel or abort this operation, do not unplug or remove power from the controller until this procedure is completed.

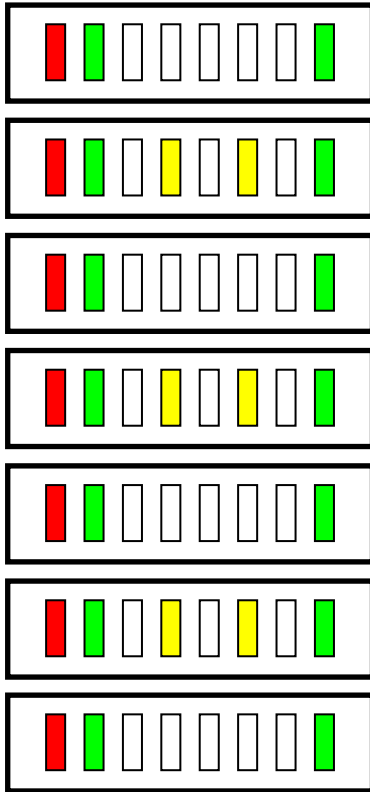


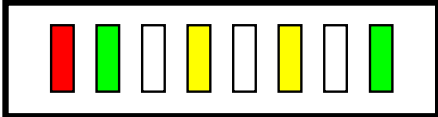
Caution: do not stop, cancel or abort the firmware update operation, **AND** do not unplug or remove power from the controller under any circumstance until part 2 of this procedure is completed.



Error Conditions

When an RFID operation error occurs, other than a Command Timeout, the red RF LED and one or more yellow LEDs will flash in unison. The yellow LEDs represent the error code in binary. The COM LED will stay on to help orient the binary LED positions. The yellow LEDs will continue to flash the error code until a valid command is received. If an unrecoverable error occurs, the LEDs will continuously flash the error code until the controller has been reset.





This example depicts Error 10.

When an error occurs, the COM LED will stay on to help orient the binary LED positions. The power LED should always be on when power is applied to the HF-0405.

Please see [Chapter 7](#), for a list of error codes and their descriptions.

Chapter 5 • Communication Protocols

This chapter contains an overview of the protocols used by the HF-0405 to communicate with the Host and describes how to use them to issue RFID commands.

Communication Overview

When an RFID command is issued, the Host computer instructs the RFID controller to perform a given task. After performing that task, the RFID controller will usually reply back with a Command Response message indicating the status or results of the attempted command. This response indicates whether the command was successfully completed or if the RFID controller failed to complete the command.

ABx Command Protocols

To understand and execute RFID commands, the HF-0405 and the Host must be able to communicate using the same language. The language that they use to communicate RFID commands is referred to as the Command Protocol. The type of Command Protocol that is used is known as the ABx Command Protocol, of which there are three variations. The three versions of the ABx Command Protocol that are supported by the HF-0405 RFID Controller are:

- [ABx Fast \(default\)](#)
- [ABx ASCII](#)
- [ABx Standard](#)

The **ABx Fast** command protocol is a single byte-based packet structure that permits the execution of RFID commands while requiring the transfer of fewer total bytes than ABx Standard. This is the default command protocol for the HF-0405. It can be used with or without a checksum byte.

The **ABx ASCII** command protocol also uses a single byte-based format that permits the execution of RFID commands using a seven-bit ASCII character set. This can be useful in applications reading data bytes with values from 0x00 - 0xFF or where software flow control is required. ABx ASCII will prevent data from interrupting communications when a control character is received. This protocol can also be used with or without a checksum.

The **ABx Standard** command protocol uses a 2-byte, word-based format that shares a common syntax and with most existing RFID systems produced by Escort Memory Systems. This protocol offers legacy support, which may be required by existing PLC applications that only support a 2-byte word packet format. If your application requires compatibility with existing or legacy RFID devices from Escort Memory Systems, use ABx Standard. ABx Standard does not support the use of a checksum byte.

By default, the HF-0405 is configured to use **ABx Fast (No Checksum)**. ABx Fast (as the name suggests) is the faster and more efficient of the three ABx protocols, offering increased communication speed and error immunity. The “No Checksum”



option is chosen for its ease of use. However, we encourage the use of checksums for most applications.

ABx Command Structures

In its simplest form, ABx commands are comprised of a header, a number of parameters, and a command terminator. The structure of every ABx command will, at the very least, contain these basic elements.

[Command Header - Command Parameters - Command Terminator]

In ABx Fast and ABx ASCII, each command begins with the 2-byte header 0x0202 and ends with the one-byte terminator 0x03. In ABx Standard, every command begins with the one-byte header "0xAA," and ends with the two-byte terminator "0xFFFF". See the table below for further clarification.

ABx Protocols Headers and Terminators

ABx Protocol	Header	Terminator
ABx Fast	0x0202	0x03
ABx ASCII	0x0202 <STX><STX>	0x03 <ETX>
ABx Standard	0xAA	0xFFFF

When a command is issued from the Host, the RFID controller stores the incoming data packet in a buffer while it scans the data for a start character (0x0202 or 0xAA). When a start character is found, it checks for the proper terminator (0x03, <ETX> or 0xFFFF). Having identified a potentially valid command string, the controller will verify the format of the data and either perform the requested function or generate an error message.

ABx Response Structures

After receiving and/or performing a command, the HF-0405 will issue a *Command Response* message back to the Host. Similar in structure to ABx commands, an ABx Command Response contains a header, a number of response values, and a response terminator.

The response structure for all three ABx protocols consists of these same basic elements:

[Response Header - Response Values - Response Terminator]

For all three ABx protocols, the response header and response terminator will be the same as their command header and command terminator counterparts.



ABx Command Parameters

ABx commands have specific parameters that may be modified depending on your application. Some of the typical Command Parameters include: Command Size, Packet Length, Command Timeout and Starting Address.



A long timeout value does not necessarily mean that a command will take any longer to execute. This value only represents the period of time that the controller will attempt to execute the command.

Command Timeout

Most ABx commands require the setting of a Timeout Value that is used to limit the length of time that the HF-0405 will attempt to complete a specified operation.

The Timeout Value is measured in increments of 1 millisecond, with a maximum value of 65,534 (0xFFFFE) milliseconds, or slightly more than one minute.

For most ABx commands, the absolute minimum Timeout Value which can be issued to the controller is 1 millisecond. However, we recommend 2000 milliseconds as the shortest timeout value to use.

The HF-0405 does support a limited number of commands that will allow a Timeout Value of 0, in which case the controller will try indefinitely to complete the issued command. However, for the most part, a timeout value of 0 will cause the controller to generate an error message. (See [Chapter 6](#) for specific details regarding each ABx command).

During Write commands, the tag must remain in the field until either the command completes successfully, or the Timeout period has expired. If a Write command is initiated with a tag in the antenna's active field and then the tag leaves the field before the command has completed or times out, data may be lost or corrupted. It is recommended that you use the longest Timeout Value permitted by your application.

Command Size

ABx Fast and ABx ASCII commands require that the byte length of the Command Size be included as a parameter in the Command Data Packet.

To calculate the Command Size, add the number of total bytes within the Command Data Packet while excluding the Header, Command Size, Checksum (if present) and Terminator.

Another method for identifying the length of the Command Size is to add the number of bytes of all Command Parameters located between (but not including) the Command Size parameter and the Terminator or Checksum, if present (the Command Size remains the same with or without a Checksum). The combined total is a 2-byte value indicating the Command Size.



Checksum Options

ABx Fast and ABx ASCII commands permit the use of an optional checksum byte. Checksums are used to verify the integrity of the data being transmitted. To enable the use of a checksum value, use the RFID Demonstration Utility and select *ABx Fast with Checksum* or *ABx ASCII with Checksum* when starting the program.

The checksum is calculated by adding all byte values in the Command Data Packet (less the header, checksum and terminator), and then subtracting the total byte sum from 0xFF. Therefore, when the byte values of each parameter from Command Size to Checksum are added together, the byte value sum will be 0xFF.

ABx Fast/ASCII Checksum Example

The following is an example of an ABx Fast or ABx ASCII command using a checksum.

Field	Header	Command Size	Command ID	Timeout	Checksum	Terminator
Contents	0x0202	0x0003	0x01	0x07D0	0x24	0x03
Used to Calculate Checksum	n/a	0x00 0x03	0x01	0x07 0xD0	n/a	n/a

$$0x00 + 0x03 + 0x01 + 0x07 + 0xD0 = 0xDB$$

Thus, the equation: $0xFF - 0xDB = 0x24$



ABx Fast Command Protocol

The default command protocol used by the HF-0405 is **ABx Fast (Without Checksum)**. This protocol differs from ABx Standard in that the smallest addressable data element is one byte, rather than the 2-byte “word” structure of ABx Standard. However, ABx Fast commands and responses do contain two-byte words that indicate the size and length of various Command Parameters. ABx Fast also supports the use of a one-byte optional Checksum.

ABx Fast - Command Packet Structure

Field	Header	Command Size	Command ID	Start Address	Read / Write Address Length	Timeout	Data Value Byte	Checksum	Terminator
Content	0x0202	2-byte value indicating packet length in bytes - excluding header, command size, checksum and terminator.	1-byte value for Command ID Number	2-byte value to identify the read/write starting address.	2-byte value to identify the number of addresses to be read or written to.	2-byte value indicating Timeout Value (0x0001 to 0xFFFE in msec).	1-byte value for fill character or other command specific data.	1-byte optional Checksum	1-byte terminator 0x03



ABx Fast – Response Packet Structure

Field	Header	Response Size	Command ID	Start Address	Read / Write Address Length	Timeout	Data Value Byte	Checksum	Terminator
Content	0x0202	2-byte value indicating packet length in bytes - excluding header, command size, checksum and terminator.	1-byte value for Command ID Number	2-byte value to identify the read/write starting address.	2-byte value to identify the number of addresses to be read or written to.	2-byte value indicating Timeout Value (0x0001 to 0xFFFE in msec).	1-byte value for fill character or other response specific data.	1-byte optional Checksum	1-byte terminator 0x03



ABx ASCII Command Protocol

The ABx ASCII command protocol is based on the ABx Fast command protocol, however, ABx ASCII goes one step further by converting command hex values into printable ASCII characters. In another words, hex values displayed in an ABx Fast command are transmitted as separate ASCII characters in ABx ASCII.

ABx ASCII uses the ASCII equivalent of ABx Fast's 2-byte header and 1-Byte terminator (that are always [STX (0x02) STX (0x02)] and [ETX (0x03)] respectively).

The values of all other fields are displayed as ASCII hex notation. The permitted values are the numbers **0-9** and the capital letters **A-F**. The characters 0-9 and A-F equal the Hex values 0x30 thru 0x39, and 0x41 thru 0x46.

ABx ASCII also supports the use of Xon/Xoff handshaking; ABx Fast and ABx Standard do not.

See [Appendix C](#), for a list of ASCII characters and their corresponding Hex and Decimal values.

ABx ASCII Character Values

In ABx ASCII, the hex value 0xAB (decimal 171) is transmitted as the 2-character string **AB**. For example, the 2 bytes "0x41" and "0x42" are equivalent to the ASCII characters '**A**' and '**B**'.

If you refer back to the ABx Fast section earlier in this chapter, you will notice that you can structure ABx ASCII commands by using ASCII characters to represent each digit of a hex value, excluding header and terminator which are already ASCII characters (<STX> and <ETX>).

ABx ASCII Command and Response Size

The ABx ASCII command protocol requires that a 2-byte value indicating the length of the Command Size be included in the command packet. The Command Size is calculated by adding the byte values of all parameters and data values located between the Command Size parameter and Checksum (if used) or Terminator. The Command Size includes the Command ID value and parameters such as address definitions for tag Read/Writes. The Command Size remains the same with, or without a checksum. In ABx ASCII, the Command Size and Response Size is the combined number of Hex bytes, not the number of ASCII characters used to represent the hex values.



ABx ASCII - Command Packet Structure

The ABX ASCII protocol is based on the following minimal command packet structure. Depending on the command issued and your Checksum setting, the Data Byte and Checksum fields may not be present.

Field	Header	Command Size	Command ID	Data Byte Value	Checksum	Terminator
Number of ASCII Characters	2	4	2	1	2	1
Content	<STX><STX> (0x02, 0x02)	Packet length in bytes - excluding header, command size, checksum and terminator	Command ID Number	1-byte value for fill value or other command specific data.	Optional Checksum	<ETX> (0x03)



ABx ASCII - Command Example

ABx ASCII Command 04 – Tag Fill Example

In this example, the RFID controller is directed to fill a number of address locations with a specific data value byte, beginning at a specified starting address location. When Block Size = 0, the HF-0405 will fill the tag until it reaches the end of available memory. This command is similar to the ABx Fast version of the command.

Header	Command Size	Command ID	Start Address	Fill Length	Timeout	Data Value Byte	Checksum	Terminator
<STX><STX>	Packet length in bytes - excluding header, command size, checksum and terminator, displayed as a four character ASCII value (0x0008 for this command).	<0x30> <0x34> (04)	4 character ASCII value for the starting tag address	4 character ASCII value for the length of the fill in number of bytes	4 character ASCII value for timeout in 1 msec units. (0x1E - 0xFFFE)	2 character ASCII value for 1 byte of fill.	2 character ASCII value for optional checksum	<ETX>



ABx ASCII - Response Structure

After a successful operation, the controller will send back a response. The response may not include the Data Byte Value or Checksum fields (depending on the Command ID and your Checksum settings). However, if a Checksum is enabled, it will always be returned in the Command Response.

Field	Header	Response Size	Command Echo	Data Byte Value	Checksum	Terminator
Number of ASCII Characters	2	4	2	2	2	1
Content	<STX><STX> (0x02, 0x02)	Packet length in bytes - excluding header, command size, checksum and terminator	Command Echo	Response Data	Optional Checksum	<ETX> (0x03)

ABx ASCII - Error Response Structure

If the HF-0405 encounters an error during operation it will generate an error response that follows this structure:

Field	Header	Response Size	Error Flag	Error Code	Checksum	Terminator
Number of ASCII Characters	2	4	1	1	2	1
Content	<STX><STX> (0x02, 0x02)	Packet length in bytes - excluding header, command size, checksum and terminator	0xFF (indicates that an error occurred)	1-byte Hex error code (see error code table for details)	Optional Checksum	<ETX> (0x03)



ABx ASCII Error Response Example

A block write fail error response might appear as the following ASCII character string:

```
Code sample: <STX><STX>0006FF0643<ETX>
```

However, in Hex, the same error response would appear as:

```
Code Sample: 0x02 0x02 0x30 0x30 0x03 0x32 0x46 0x46  
0x30 0x36 0x46 0x38 0x03
```



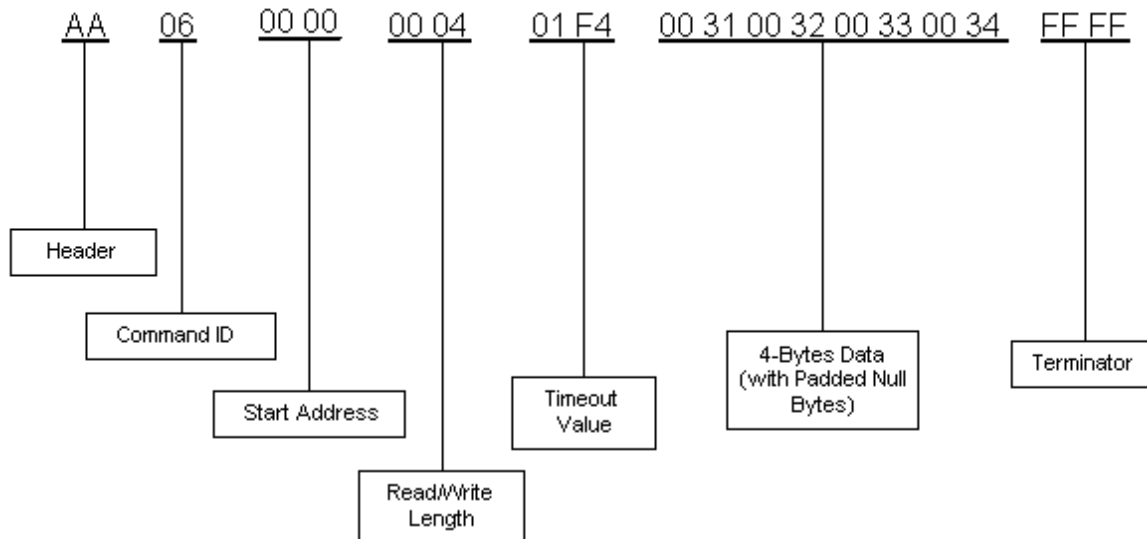
ABx Standard Command Protocol

ABx Standard is a binary, 2-byte, word oriented protocol where data is transmitted in 2-byte increments, the Most Significant Byte (MSB) and the Least Significant Byte (LSB). In a serial transmission, the MSB is transmitted first. Note that the MSB is sometimes called the High Byte and the LSB is sometimes called the Low Byte.

The ABx Standard protocol uses double bytes (or one “word”) of data as its’ primary element for transmitting and receiving information. In transmission, the first byte or MSB of a word is the first character to come out of the Host’s COM port followed by the LSB.

Usually, the first data word sent to the controller contain the Header and Command ID number, followed by parameters such as read length, write length, timeout and starting address. Whatever the combination of commands and data you enter, at no time can the complete array string, including terminator word, exceed 50 words.

ABx Standard Command Format Defined



ABx Standard - Command Packet Structure

Field	Header	Command ID	Start Address	Address Length in Bytes	Timeout	Data Value Byte	Terminator
Number of Bytes	1	1	2	2	2	2	2
Content	0xAA is always the MSB of the first word of an ABx Standard command.	The Command ID is always the LSB of the first word.	2-byte value for the address of the first byte of tag memory to be accessed.	2-byte value indicating the number of contiguous bytes to be accessed.	2 byte timeout value between 0x0001 and 0xFFFFE (1 and 65,534 msecs)	Contains data which will be written to the tag. Data is included in the LSB	0xFFFF

ABx Standard - Command Example

The example below depicts the packet structure of the ABx Standard Command and Response messages for Command 08 (Tag Search). In this example, the RFID Controller is instructed to search for a tag in the RF field. A timeout of 2 seconds (0x07D0) is set for the completion of this operation.

Command from Host

Field	Perform Command 08 (MSB/LSB)	Timeout Value (2 seconds) (MSB/LSB)	Terminator (MSB/LSB)
Content	0xAA 0x08	0x07D0	0xFFFF

Code Sample: AA 08 07 D0 FF FF

Response from Controller

Field	Command Echo (MSB/LSB)	Terminator (MSB/LSB)
Content	0xAA 0x08	0xFFFF

Code Sample: AA 08 FF FF

Chapter 6 • RFID Commands

For the most part, RFID commands can be divided into **two** primary categories:

- 1. Controller Operation Commands**

Controller Operation Commands are used to manually set or modify the HF-0405's internal configuration.

- 2. Tag Operation Commands**

Tag Operation Commands require the presence of an RFID tag in the RF field and can be further sub-divided into *Read* and *Write* commands.

RFID Command Table

The table below contains a list of RFID commands supported by the HF-0405 RFID Controller.

Command ID Number	Command Name
04	Tag Fill
05	Read Data
06	Write Data
07	Read Tag Serial Number
08	Tag Search
0D	Start/Stop Continuous Read
0A	Set RS232/422 Baud Rate
36	Send Controller Configuration
37	Read Controller Configuration
38	Read Controller ID Number
A1	Reset Controller



Command 04 (0x04): Tag Fill

DESCRIPTION

Fill an RFID tag with a one byte value over multiple contiguous addresses.

DISCUSSION

This command is commonly used to clear contiguous segments of a tag's memory. It writes a one byte value repeatedly across a specified range of tag addresses.

The fill function requires one data value byte, a starting address, and a fill length. It will then proceed to fill the tag with the data value byte, starting at the specified start address for the specified number of consecutive bytes.

When Fill Length is set to 0, the controller will write fill data from the start address to the end of the tag's memory. The timeout value is measured in 1 msec increments and can have a value of 0x01 to 0xFFFE (65,534 msec). When the timeout is set to 0, the controller will return a syntax error. If the Fill Length extends beyond the last byte in the tag, the controller will also return an error.

Command 04 (Fill Tag) - ABx Fast Command Structure

Command from Host

Field	Header	Command Size	Command ID	Start Address	Fill Length	Timeout Value	Data Value Byte	Checksum	Terminator
Content	0x0202	2-byte value for command packet length in Bytes excluding header, command size, checksum and terminator	Command ID number in Hex (0x04)	2-Byte value for the starting tag address	2-Byte value for the length of the fill	2-Byte value for timeout measured in 1 msec units. (0x1E – 0xFFFE)	1-byte value for the data byte to be used as fill	Optional Checksum	0x03



Response from Controller

Field	Header	Response Size	Command Echo	Checksum	Terminator
Content	0x0202	2-byte value indicating response packet length in bytes excluding header, response size, checksum and terminator	Command ID number in Hex (0x04)	Optional Checksum	0x03

Command 04 (Fill Tag) - ABx Fast Command Example

This example instructs the HF-0405 to write the ASCII character 'A' (0x41) to the entire tag starting at address 0x0000. A timeout of 2 seconds (0x07D0) is set for the completion of the command.

Command from Host

Field	Header	Command Size	Command ID	Start Address	Fill Length	Timeout	Data Value Byte	Checksum	Terminator
Content	0x0202	0x0008	0x04	0x0000	0x0000	0x07D0	0x41	optional	0x03

Code Sample: 02 02 00 08 04 00 00 00 00 07 D0 41 03

Response from Controller

Field	Header	Response Size	Command Echo	Checksum	Terminator
Content	0x0202	0x0001	0x04	optional	0x03

Code Sample: 02 02 00 01 04 03



Command 04 (Fill Tag) – ABx Standard Command Structure

Field	Command	Start Address	Fill Length	Timeout	Data Value Byte	Terminator
Content	0xAA followed by Command ID number in Hex (0x04).	2-byte value indicating tag address where fill will start	2-byte value indicating the total number of tag addresses to be filled	2-byte value indicating timeout value measured in 1 msec units (0x01 – 0xFFFE)	1-byte value for the data byte to be used as fill	0xFFFF

Command 04 (Fill Tag) - ABx Standard Command Example

In this example, the goal is to write the ASCII value 'A' (0x41) to the entire range of tag memory starting at byte address 00. A timeout of 2 seconds (0x07D0) is set for the completion of the command.

Command from Host

Field	Perform Command 04 (MSB/LSB)	Start Address = 0x0000 (MSB/LSB)	Fill Length = 0 for all (MSB/LSB)	Timeout Value (MSB/LSB)	Data Byte Value (MSB/LSB)	Terminator (MSB/LSB)
Content	0xAA 0x04	0x00 0x05	0x00 0x00	0x07 0xD0	0x00 0x41	0xFF 0xFF

Code Sample: AA 04 00 00 00 00 07 D0 00 41 FF FF

Response from Controller

Field	Command 04 Echo (MSB/LSB)	Terminator (MSB/LSB)
Content	0xAA 0x04	0xFF 0xFF

Code Sample: AA 04 FF FF



Command 05 (0x05): Read Data

DESCRIPTION

Read data from contiguous (sequential) areas of the RFID tag's read/write memory.

DISCUSSION

The Read Data command is used to read bytes from contiguous areas of tag memory. This command consists of the Header and Command ID number, a Start Address and Read Length, followed by the message Terminator.

The minimum read length is 1 byte. The maximum is the entire read/write address space of the tag. The Timeout Value is measured in 1 msec increments and can have a value of 0x0001 to 0xFFFE (1 to 65,534 msec). When the Timeout is set to 0, the controller will return a syntax error. If the read range exceeds the last tag address, the controller will return an invalid format error.

In ABx Standard, data read from the tag is returned in the LSB (Least Significant Byte) only. The MSB (Most Significant Byte) will always be 0x00.

Command 05 (Read Data) - ABx Fast Command Structure

Field	Header	Command Size	Command ID	Start Address	Read Length	Timeout	Checksum	Terminator
Content	0x0202	2-byte value indicating packet length in bytes excluding header, command size, checksum and terminator	1-byte Command ID in Hex (0x05)	2-byte value for the starting read address	2-byte value for the length of the read (in number of bytes)	2-byte value for Timeout measured in 1 msec units. (0x01 – 0xFFFE)	Optional Checksum	0x03



Command 05 (Read Data) - ABx Fast Command Example

This example instructs the controller to read 4 bytes of data from the tag starting at address 0x0000. A timeout of 2 seconds (0x07D0 = 2000 x 1 msec increments) is set for the completion of the Read Data command.

Command from Host

Field	Header	Command Size	Command ID	Start Address	Read Length	Timeout	Checksum	Terminator
Content	0x0202	0x0007	0x05	0x0000	0x0004	0x07D0	optional	0x03

Code Sample: 02 02 00 07 05 00 00 00 04 07 D0 03

Response from Controller

Field	Header	Response Size	Command Echo	Data from address 0x0000	Data from address 0x0001	Data from address 0x0002	Data from address 0x0003	Checksum	Terminator
Content	0x0202	0x0005	0x05	0x05	0xAA	0xE7	0x0A	optional	0x03

Code Sample: 02 02 00 05 05 05 AA E7 0A 03

Data Read From Addresses 0x0000-0x0003 = 05 AA E7 0A



Command 05 (Read Data) - ABx Standard Command Structure

Field	Header & Command ID	Start Address	Read Length	Timeout	Terminator
Content	0xAA followed by Command ID number in Hex (0x05)	2-byte value for tag address where the fill will start	2-byte value for the number of bytes to be read	Timeout value measured in 1 msec units (0x001E – 0xFFFE)	0xFFFF

Command 05 (Read Data) - ABx Standard Command Example

The goal of this example is to read 10 bytes of data from the tag starting at address 00. A timeout of 2 seconds (0x07D0 = 2000 x 1 msec increments) is set for the completion of the Block Read.

Command from Host

Field	Perform Command 05 (MSB/LSB)	Start Byte Address (MSB/LSB)	Read Length (MSB/LSB)	Timeout (MSB/LSB)	Terminator (MSB/LSB)
Content	0xAA 0x05	0x00 0x01	0x00 0x08	0x07 0xD0	0xFF 0xFF

Code Sample: AA 05 00 01 00 08 07 D0 FF FF

Response from Controller

Field	Command Echo (MSB/LSB)	Read Data x N Bytes (MSB/LSB)	Terminator
Content	0xAA 0x05	varies	0xFF 0xFF

Code Sample: AA 05 (Read Data x N-bytes) FF FF

Command 06 ▣ (0x06): Write Data

DESCRIPTION

Write data to an RFID tag.

DISCUSSION

This command is used to write segments of data to contiguous addresses of tag memory. It is capable of transferring up to 100 bytes of data from the Host with one command. The Write Data command consists of a header, the Command ID, the Start Address of the Write, followed by the data value stream to be written to the RFID tag. The timeout value is measured in 1 msec increments and can have a value of 0x0001 to 0xFFFFE (65,534 msec). If the timeout is set to 0, the controller will return a syntax error. If the write range exceeds the last tag address, the controller will return an error message. The controller will also return an error if the write length is 0.

Command 06 (Write Data) - ABx Fast Command Structure

Field	Header	Command Size	Command ID	Start Address	Write Length	Timeout	Data Value Bytes	Checksum	Terminator
Content	0x0202	2-byte value for packet length in Bytes excluding header, command size, checksum and terminator	0x06	2-byte value for the starting tag address	2-byte value for the number of addresses that will be written to.	2-byte value for timeout measured in 1 msec units. (0x1E – 0xFFFFE)	1-byte data byte value to be written to tag	Optional Checksum	0x03



Command 06 (Write Data) – ABx Fast Command Example

This example writes 4 Bytes of data to the tag starting at address 0x0000. A timeout of 2 seconds (0x07D0 = 2000 x 1 msec increments) is set for the completion of the Block Write.

Command from Host

Field	Header	Command Size	Command ID	Start Address	Write Length	Timeout
Content	0x0202	0x000B	0x06	0x0000	0x0004	0x07D0

Data to write to address 0x0000	Data to write to address 0x0001	Data to write to address 0x0002	Data to write to address 0x0003	Checksum	Terminator
0x52	0x46	0x49	0x44	0xEE	0x03

Code Sample: 02 02 00 0B 06 00 00 00 04 07 D0 52 46 49 44 EE 03

Response from Controller

Field	Header	Response Size	Command Echo	Checksum	Terminator
Content	0x0202	0x0001	0x06	0xF8	0x03

Code Sample: 02 02 00 01 06 F8 03



Command 06 (Write Data) – ABx Standard Command Structure

For ABx Standard, data to be written to the tag is contained in the LSB of the Data Byte Value, and the MSB is always 0x00.

Field	Header and Command ID	Start Address	Write Length	Timeout	Data Byte Value	Terminator
Content	0xAA followed by Command ID number in Hex (0x06)	2-byte value for the tag address where the write will start	2-byte value for the number of tag addresses to be written to	Timeout value measured in 1 msec units (0x001E – 0xFFFE)	2-byte value for the data to be written to the tag	0xFFFF

Command 06 (Write Data) – ABx Standard Command Example

In this example, the RFID controller will write 4 bytes of data to the tag starting at address 0x0020. A timeout of 2 seconds (0x07D0 = 2000 msec) is set for the completion of the Block Write.

Command from Host

Field	Perform Command 06	Start Address = 0x0020	Write Length = 4 Bytes (0x0004)	Timeout	Write Data 1 = 0x52	Write Data 2 = 0x46	Write Data 3 = 0x49	Write Data 4 = 0x44	Terminator
Content (MSB/LSB)	AA 06	00 20	00 04	07 D0	00 52	00 46	00 49	00 44	FF FF

Code Sample: AA 06 00 20 00 04 07 D0 00 52 00 46 00 49 00 44 FF FF

Response from Controller

Field	Command Echo	Terminator
Content (MSB/LSB)	AA 06	FF FF

Code Sample: AA 05 FF FF



Command 07 (0x07): Read Tag ID (SN)

DESCRIPTION

This command retrieves the eight-byte tag ID or serial number.

DISCUSSION

Each ISO 14443 and ISO 15693 compliant tag has a unique 8 byte ID or serial number. By using just eight bytes, manufacturers can generate over 280 trillion possible serial numbers. Once a tag is given an ID or serial number it can not be changed and is not part of the available read/write address space of a tag. The timeout value is measured in 1 msec increments and can have a value of 0x001E to 0xFFFE (30 - 65,534 msec).

Command 07 (Read Tag SN) – ABx Fast Command Structure

Field	Header	Command Size	Command ID	Timeout	Checksum	Terminator
Content	0x0202	2-byte value for packet length in bytes excluding header, command size, checksum and terminator (0x0003 for this command).	0x07	2-Byte value for timeout measured in 1 msec units. (0x1E – 0xFFFE)	Optional Checksum	0x03



Command 07 (Read Tag ID) – ABx Fast Command Example

This example will wait until a tag is in range and then reads the 8-byte ID or serial number. In this example the serial number is F272030000104E0.

Command from Host

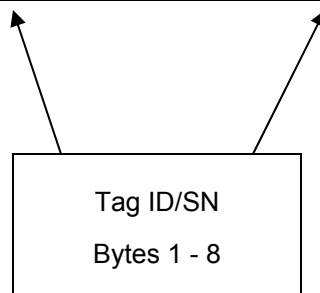
Field	Header	Command Size	Command ID	Timeout	Checksum	Terminator
Content	0x0202	0x0003	0x07	0x07D0 (2 seconds)	0x1E	0x03

Code Sample: 02 02 00 03 07 07 D0 1E 03

Response from Controller

Field	Header	Response Size	Command Echo	ID/SN Bytes 1-8	Checksum	Terminator
Content	0x0202	0x0009	0x07	0xF2 0x72 0x03 0x00 0x00 0x01 0x04 0xE0	0xA3	0x03

Code Sample: 02 02 00 09 07 **F2 72 03 00 00 01 04 E0** A3 03



Command 07 (Read Tag ID) – ABx Standard Command Structure

When running this command, the tag ID or serial number is returned in the LSB only, with 0x00 as the MSB.

Field	Command	Timeout	Message Terminator
Content	0xAA followed by Command ID number in Hex (0x07)	Timeout value measured in 1 msec units (0x001E – 0xFFFFE)	0xFFFF

Command 07 (Read Tag ID) – ABx Standard Command Example

In this example, the command instructs the RFID controller to read the 8-byte ID or serial number. In this example the Tag ID/SN is **E2963C2B**.

Command from Host

Field	Header & Command ID (MSB/LSB)	Timeout Value	Message Terminator
Content	0xAA 0x07	0x07 0xD0	0xFF 0xFF

Code Sample: AA 07 07 D0 FF FF

Response from Controller

Field	Header & Command Echo (MSB/LSB)	SN Byte 1	SN Byte 2	SN Byte 3	SN Byte 4	SN Byte 5
Content	AA 07	00	E2	00	96	00

SN Byte 6	SN Byte 7	SN Byte 8	Terminator (MSB/LSB)
3C	00	2B	FF FF

Code Sample: AA 07 00 E2 00 96 00 3C 00 2B FF FF



Command 08 ■ (0x08): Tag Search

DESCRIPTION

This command instructs the RFID Controller to search for a tag in the RF field.

DISCUSSION

This command will instruct the controller to search for the presence of a tag within range of the antenna. If the controller finds a tag it will return a command echo to the host. The timeout value is measured in 1 msec increments and can have a value of 0x001E to 0xFFFE (30 to 65,534 msec). When the timeout is set to 0, the controller will return a syntax error. If no tag is present, it will return an error message.

Command 08 (Tag Search) – ABx Fast Command Structure

Field	Header	Command Size	Command ID	Timeout	Checksum	Terminator
Content	0x0202	2-byte value for packet length in bytes excluding header, command size, checksum and terminator	0x08	2-byte value for timeout measured in 1 msec units (0x0001 – 0xFFFE).	Optional Checksum	0x03



Command 08 (Tag Search) – ABx Fast Command Example

This example checks for any RFID tag within range of the antenna. A timeout of 2 seconds (0x07D0 = 2000 msec) is set for the completion of the Tag Search.

Command from Host

Field	Header	Command Size	Command ID	Timeout	Checksum	Terminator
Content	0x0202	0x0003	0x08	0x07D0	0x1D	0x03

Code Sample: 02 02 00 03 08 07 D0 1D 03

Response from Controller

Field	Header	Response Size	Command Echo	Checksum	Terminator
Content	0x0202	0x0001	0x08	0xF6	0x03

Code Sample: 02 02 00 01 08 F6 03



Command 08 (Tag Search) – ABx Standard Command Structure

Field	Header & Command ID	Timeout Value	Terminator
Content	0xAA followed by Command ID number in Hex (0x08)	Timeout value measured in 1 msec units (0x0001 – 0xFFFE)	0xFF 0xFF

Command 08 (Tag Search) – ABx Standard Command Example

This example has the RFID Controller check for a tag in the RF field. A timeout of 2 seconds (0x07D0) is set for the completion of the Tag Search.

Command from Host

Field	Header & Command ID (MSB/LSB)	Timeout Value (MSB/LSB)	Terminator (MSB/LSB)
Content	0xAA 0x08	0x07 0xD0	0xFF 0xFF

Code Sample: AA 08 07 D0 FF FF

Response from Controller

Field	Header & Command Echo (MSB/LSB)	Terminator (MSB/LSB)
Content	0xAA 0x08	0xFF 0xFF

Code Sample: AA 08 FF FF



Command 0D ■ (0x0D): Start/Stop Continuous Read

DESCRIPTION

This command instructs the controller to start (or stop) Continuous Read mode.

DISCUSSION

The Start/Stop Continuous Read command contains three parameters:

- Start Address
- Read Length
- Delay Between Duplicate Decodes

When the HF-0405 is in Continuous Read Mode, it will constantly emit RF energy in an attempt to read any tag that comes into range of the antenna. When a tag enters the antenna field, it is immediately read and the data is passed to the Host. The controller will continue to read the tag but will not re-send the same data to the Host until the tag has moved outside the RF field for a specified time period. This parameter is known as the **Delay Between Duplicate Decodes**, which prevents redundant data transmissions when the controller is in Continuous Read mode.

Start Address

The Start Address is a 2 byte value indicating the tag's beginning address location for the read.

Read Length

The Read Length parameter switches the RFID Controller into (or out of) Continuous Read mode. An entry of 1 (0x01) will set the controller into Continuous Read mode. A read length value of 0 (0x00) will turn Continuous Read mode off.

Delay Between Duplicate Decodes

After Continuous Read mode is initiated, any tag that comes within range of the antenna will be read and the requested data from the tag will be sent to the host. The delay parameter represents the number of seconds that a tag must remain out of RF range before it can be re-read for a second time. This delay is implemented to enable the operator to limit the volume of information sent by the controller.

The Delay Between Duplicate Decodes parameter can have a value of 0 to 60 seconds. When the Delay Between Identical Decodes is set to 0, the controller will continuously read AND transmit tag data to the host. This can flood the buffers and cause communication errors and data loss. If the controller receives other commands from the host, it will execute them and then resume Continuous Block Read mode.



Continuous Read Mode LED Behavior

LED	Behavior	Description
PWR	ON	The controller is powered and functioning.
COM	BLINKING	A tag has entered the RF field.
RF	ON	A tag has been read and is still in the field.
RF	OFF	A previously read tag has been out of range for the specified time.

**Command 0D (Start/Stop Continuous Read) – ABx
Fast Command Structure**

Field	Header	Command Size	Command ID	Start Address	Read Length	Delay Between Duplicate Decodes	Checksum	Terminator
Content	0x0202	2-byte value for packet length in bytes excluding header, command size, checksum and terminator bytes.	0x0D	2-byte value for the start address of the read	2-byte value for number of bytes to be read	Delay value measured in 1 second units	Optional Checksum	0x03



Command 0D (Start/Stop Continuous Read) – ABx Fast Command Example

This example places the controller in Continuous Read mode and reads 8 Bytes of data from the tag starting at address 0x0001. A delay between identical reads of 2 seconds (0x0002 = 2 x 1 second increments) is set.

Command from Host

Field	Header	Command Size	Command ID	Start Address	Read Length	Delay Between Duplicate Decodes	Checksum	Terminator
Content	0x0202	0x0006	0x0D	0x0001	0x0008	0x02	0xE1	0x03

Code Sample: 02 02 00 06 0D 00 01 02 E1 03

Response from Controller

Field	Header	Response Size	Command Echo	Checksum	Terminator
Content	0x0202	0x0001	0x0D	0xE1	0x03

Code Sample: 02 02 00 01 0D E1 03



Command 0D (Start/Stop Continuous Read) – ABx Standard Command Structure

Field	Header & Command ID	Start Address	Read Length	Delay Between Identical Decodes	Terminator
Content	0xAA followed by Command ID number in Hex (0x0D)	2 byte value for the start address of the read	2 byte value for the number of bytes to be read.	Time the tag must be out of RF field before controller will transmit data again from same tag. Value is expressed in 1 second units.	0xFFFF

Command 0D (Start/Stop Continuous Read) – ABx Standard Command Example

This example places the controller in Continuous Read mode and reads 8 bytes of data from the tag starting at address 0x0001. The delay between identical reads is set to 2 seconds (in this example 0x0002 = 2 seconds).

Starting Continuous Read Mode

Command from Host

Field	Perform Command 0D (MSB/LSB)	Start Address (MSB/LSB)	Read Length (8 Bytes) (MSB/LSB)	Delay Between Identical Decodes (2 seconds) (MSB/LSB)	Terminator (MSB/LSB)
Content	0xAA 0x0D	0x00 0x01	0x00 0x08	0x00 0x02	0xFF 0xFF

Code Sample: AA 0D 00 01 00 08 00 02 FF FF

Response from Controller

The controller will first return an acknowledgment of the command followed by a response containing read data when a tag enters the antenna field.

Field	Command Echo (MSB/LSB)	Read Data Bytes 1-8 (MSB/LSB)	Terminator (MSB/LSB)
Content	0xAA 0x0D	0x00 0x52 0x00 0x46 0x00 0x49 0x00 0x44 0x00 0x41 0x00 0x20 0x00 0x54 0x00 0x61	0xFF 0xFF

Code Sample: AA 0D 00 52 00 46 00 49 00 44 00 41 00 20 00 54 00 61 FF FF

Stopping Continuous Read Mode

To exit out of Continuous Read mode, re-issue Command 0D with the read length variable set to 0 (0x00 0x00), as shown below.

Command from Host

Field	Perform Command 0D (MSB/LSB)	Start address (MSB/LSB)	Read Length (0 Bytes = ends continuous read mode) (MSB/LSB)	Delay Between Duplicate Decodes (2 seconds) (MSB/LSB)	Terminator (MSB/LSB)
Content	0xAA 0x0D	0x00 0x01	0x00 0x00	0x00 0x02	0xFF 0xFF

Code Sample: AA 0D 00 01 00 00 00 02 FF FF

Response from Controller

Field	Command Echo (MSB/LSB)	Terminator (MSB/LSB)
Content	0xAA 0x0D	0xFF 0xFF

Code Sample: AA 0D FF FF



Command 0A ■ (0x0A): Set RS232/422 Baud Rate

DESCRIPTION

This command controls the Baud Rate of the serial communications protocol for Serial Port COM 1.

DISCUSSION

This command is used to change the Baud Rate from the default of 9600bps. After this command has been initiated, communications with the RFID Controller will cease until the Host has re-established communications at the new rate. The following baud rates can be set using the corresponding hex value in the command.

Baud Rate Variables

MSB	LSB	Comments
00	0C	1200
00	30	4800
00	60	9600 (default setting)
00	C0	19200
01	80	38400
02	40	57600
04	80	115200



Command 0A (Set Baud Rate) – Command Example

This example changes the baud rate to 19200.

Command from Host

Field	Perform Command 0A (MSB/LSB)	Change Baud Rate to 19200 (MSB/LSB)	Terminator (MSB/LSB)
Content	0x00 0x0A	0x00 0xC0	0xFF 0xFF

Interface Type	Hex Value
RS232	00E8
RS422	01A6

Baud Rate	Hex Value
300	012C
600	0258
1200	04B0
2400	0960
4800	12C0
9600	2580
19200	4B00

Parity	Hex Value
None	0001
Even	0002
Odd	0003

Data Bits	Hex Value
8	0008
7	0007

Stop Bits	Hex Value
1	0001
2	0002

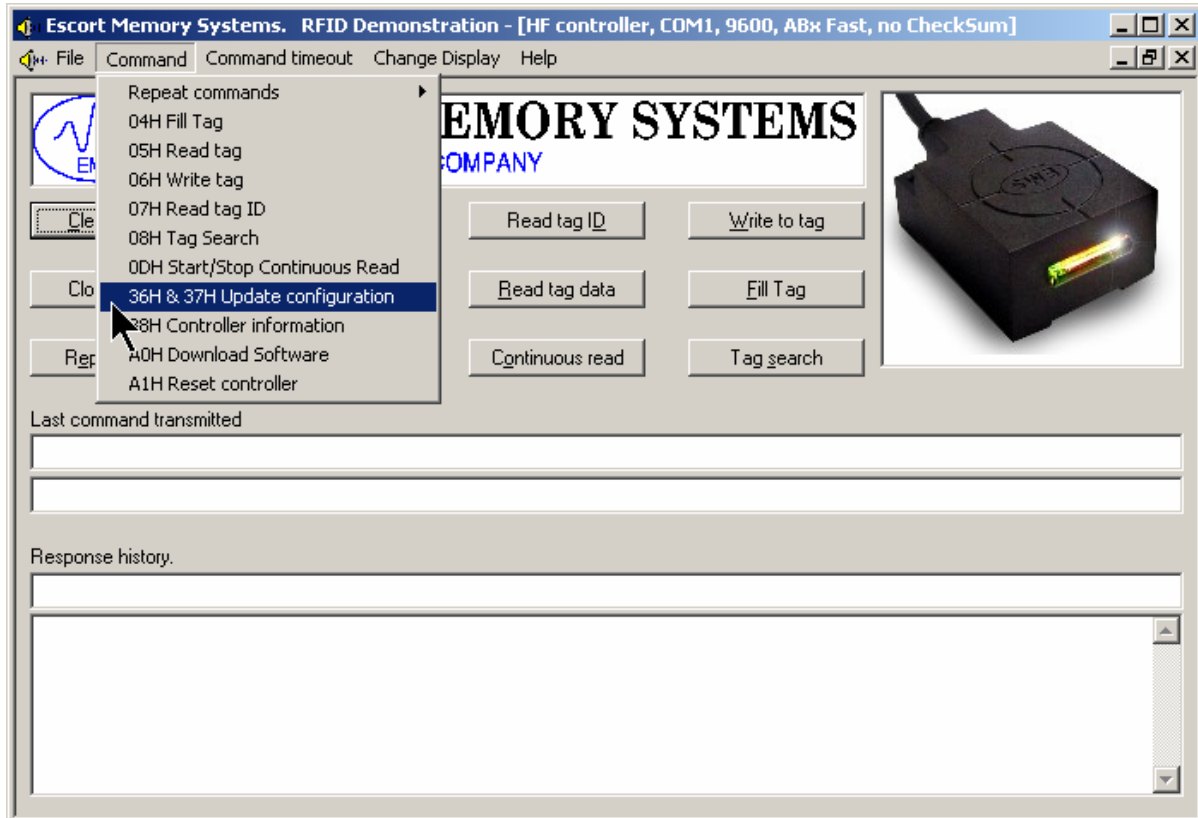


Command 36 ■ (0x36): Send Controller Configuration

Use the RFID Demonstration Utility to run Commands 36, 37, 38 and A1. The RFID Demonstration Utility can be downloaded from:

<http://www.ems-rfid.com/hf-series.html>.

After installing and starting the utility, click COMMAND and select 36H from the drop down menu.



The following configuration box will appear.

At this screen you can change the following settings:

- Tag Type
- Command Protocol
- Baud Rate

When you are done making changes click “SEND SETTINGS”. The new settings will be sent to the HF-0405 controller.

Command Code Sample:

```
02 02 00 18 36 00 00 00 00 00 00 00 01 00 60 00 00 00 01 00
00 41 08 00 00 00 00 03
```

Response Code Sample:

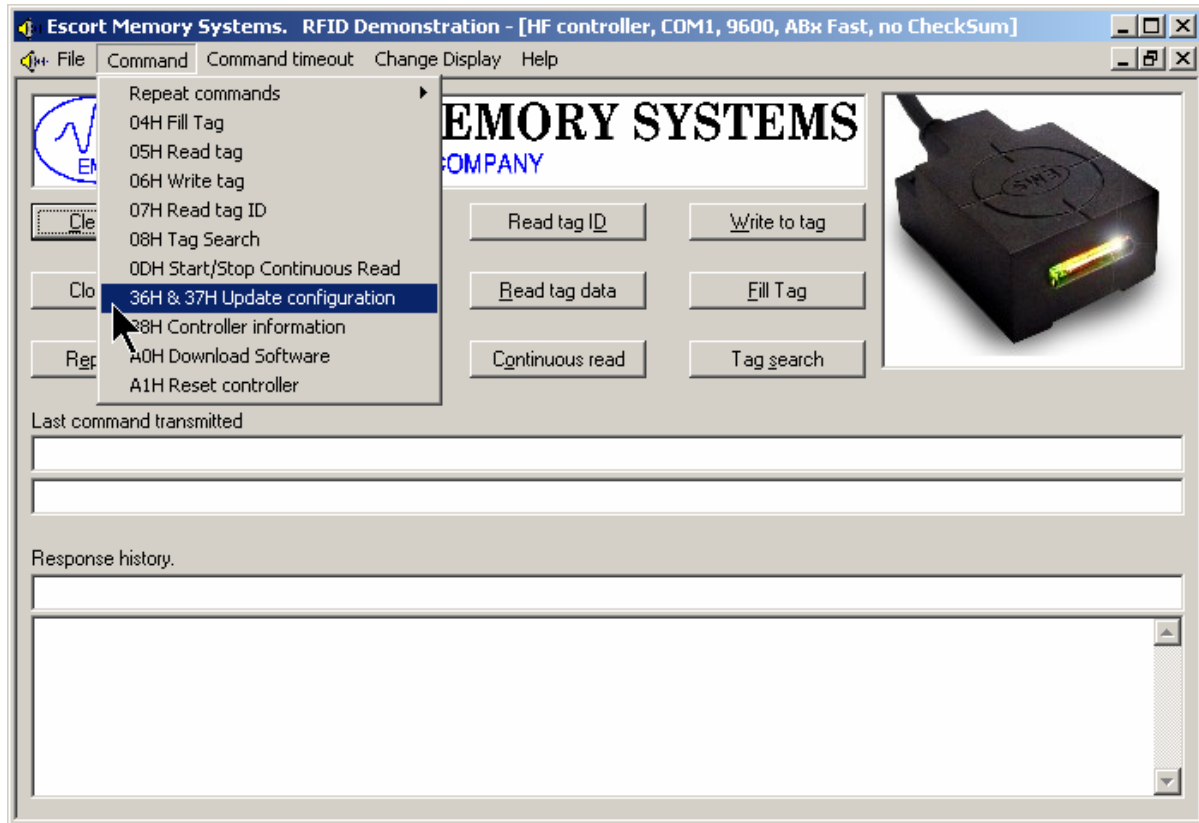
```
02 02 00 01 36 03
```



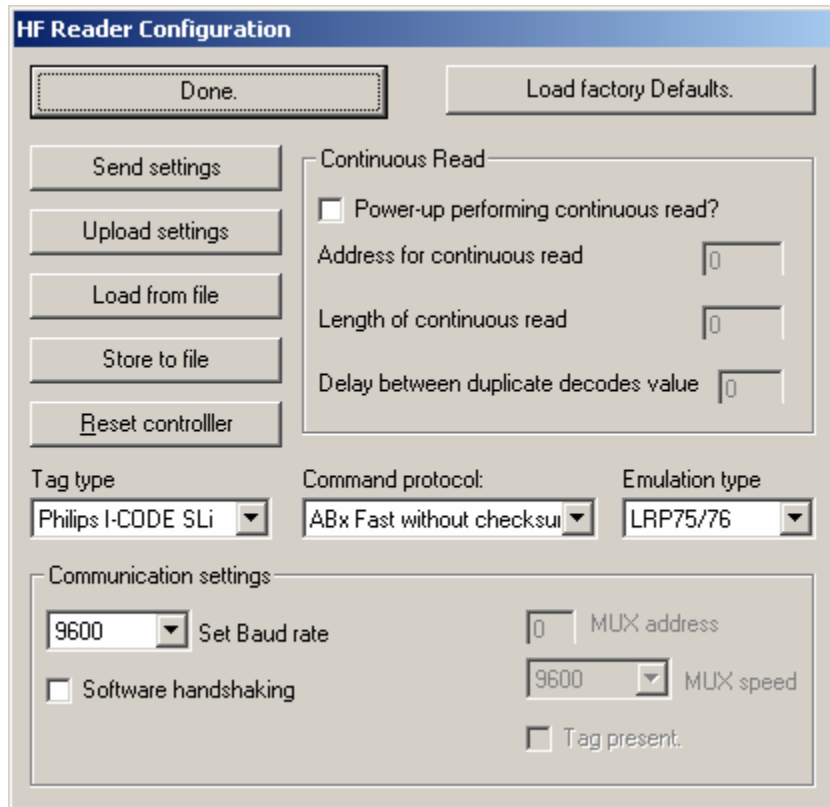
Command 37 ■ (0x37): Read Controller Configuration

Use the RFID Demonstration Utility to run Command 37.

After starting the utility, click COMMAND and select 37H from the drop down menu.



The following configuration box will appear.



The image shows a software dialog box titled "HF Reader Configuration". It contains several sections:

- Buttons:** "Done.", "Load factory Defaults.", "Send settings", "Upload settings", "Load from file", "Store to file", and "Reset controller".
- Continuous Read Section:**
 - Power-up performing continuous read?
 - Address for continuous read: [0]
 - Length of continuous read: [0]
 - Delay between duplicate decodes value: [0]
- Configuration Fields:**
 - Tag type: Philips I-CODE SLi
 - Command protocol: ABx Fast without checksum
 - Emulation type: LRP75/76
- Communication settings Section:**
 - Set Baud rate: 9600
 - MUX address: [0]
 - MUX speed: 9600
 - Software handshaking
 - Tag present.

At this screen click "UPLOAD SETTINGS". The current settings from the controller will be uploaded to the RFID Demonstration Utility.

Command Code Sample:

```
02 02 00 02 37 01 03
```

Response Code Sample:

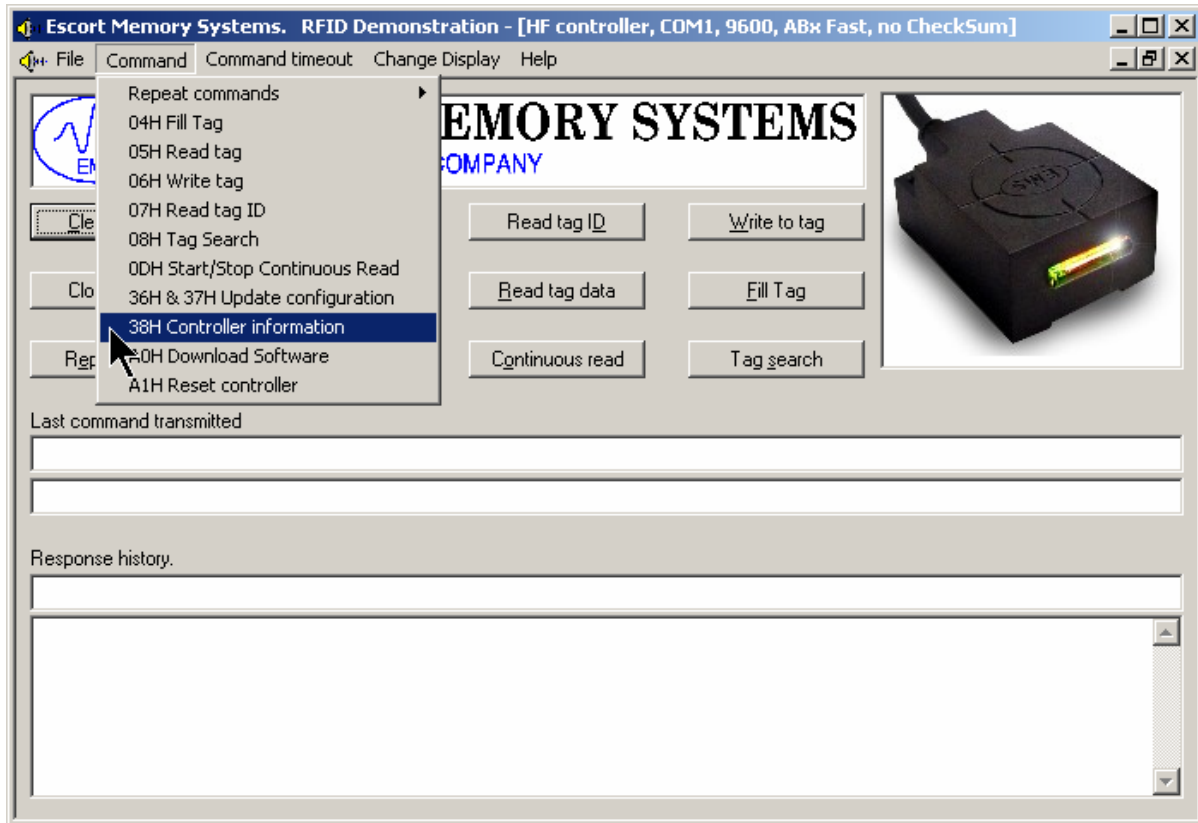
```
02 02 00 14 37 00 00 00 00 00 00 00 00 01 00 60 00 00 00 01 00
00 54 05 03
```



Command 38 ■ (0x38): Read Controller SN

Use the RFID Demonstration Utility to run Command 38. This command is used to read the RFID Controller hardware serial number.

After starting the utility, click COMMAND and select 38H from the drop down menu.



The RFID Demonstration Utility will return information similar to the following:

Read reader/writers information response:

```
Reader/writer type: 1
Version:          0.0T.5
HRDWR VER:       01
Block 0, 1, and 2 CRC: 986E
Block 3, and 4 CRC: 986E
RC632 ID:        30FFFF0F04
RC632 RFU:       000000
RC632 Serial Number: 05E19644
```



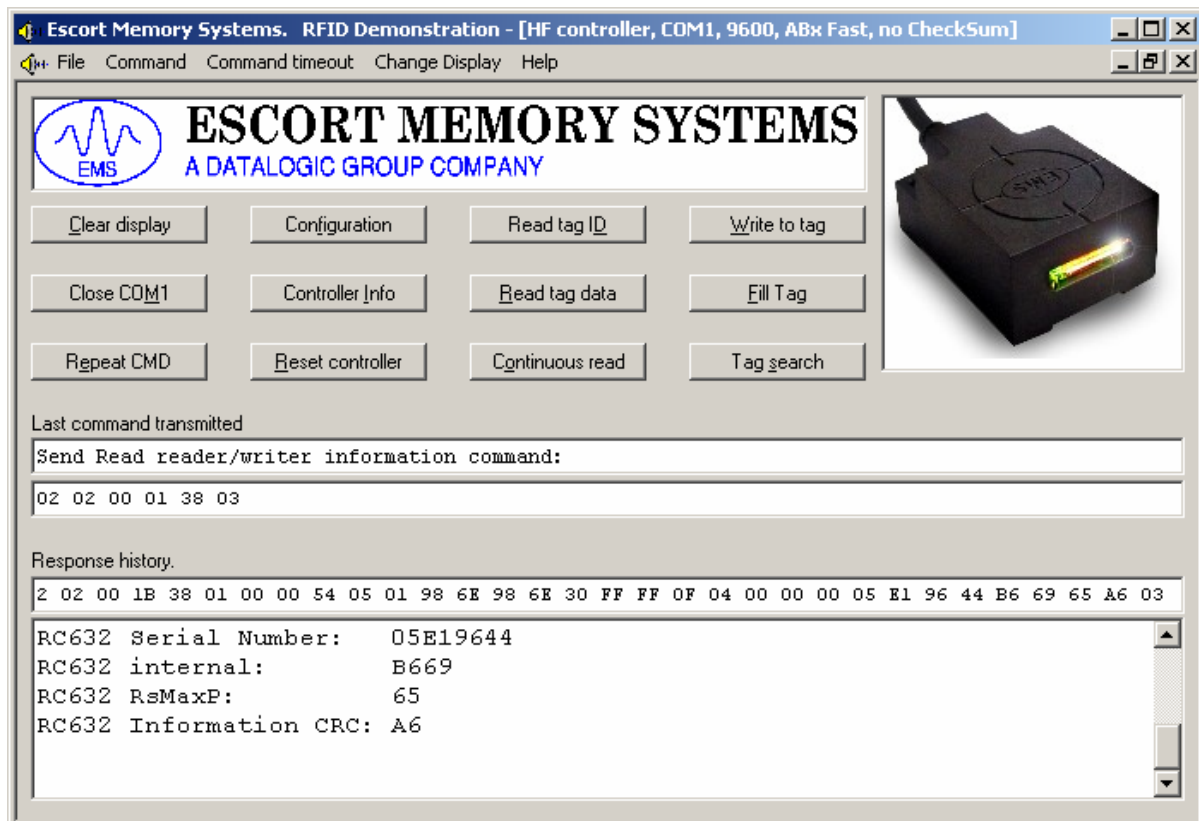
RC632 internal: B669

RC632 RsMaxP: 65

RC632 Information CRC: A6

Command Code Sample: 02 02 00 01 38 03

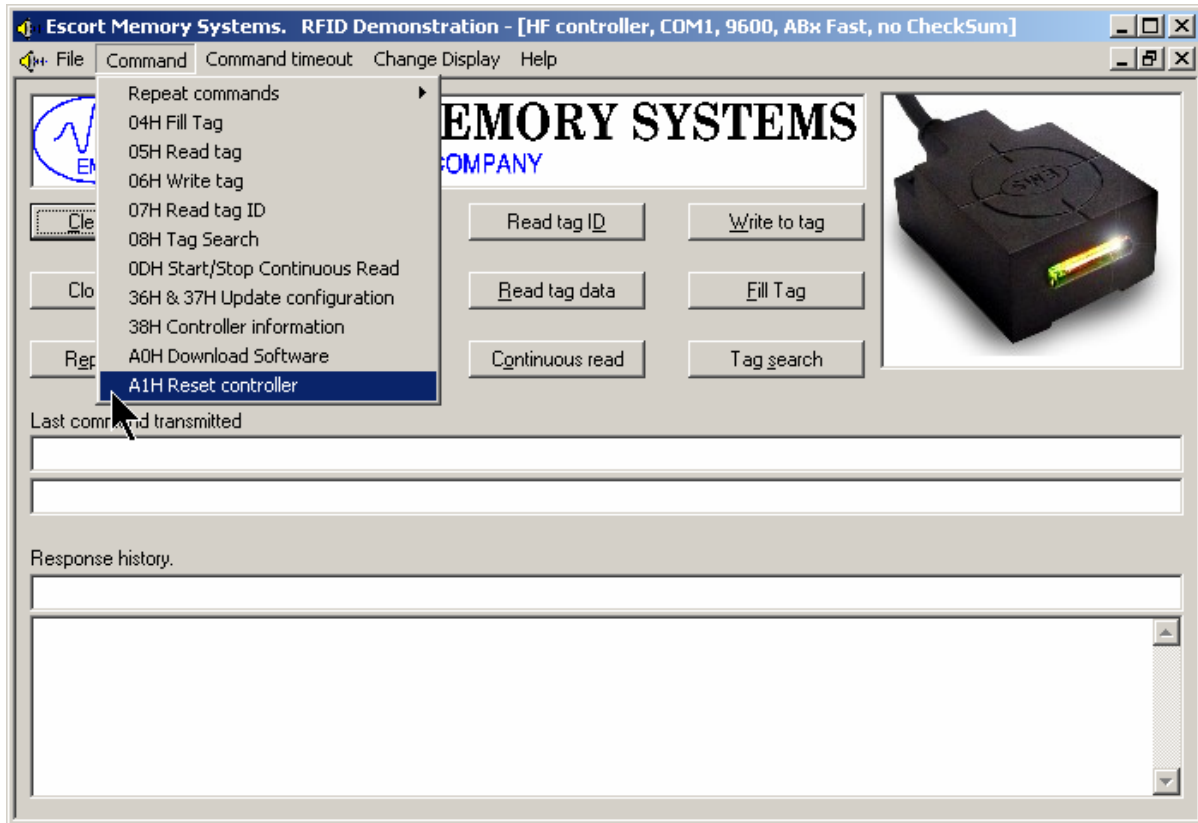
Response Code Sample: 02 02 00 1B 38 01 00 00 54 05 01 98 6E
98 6E 30 FF FF 0F 04 00 00 00 05 E1 96 44 B6 69 65 A6 03



Command A1 (0xA1): Reset Controller

Use the RFID Demonstration Utility to run Command A1. This command is used to reset the RFID Controller.

After starting the utility, click COMMAND and select A1H from the drop down menu.



The controller will be reset to factory default settings.

```
Command Code Sample: 02 02 00 01 A1 03
```

```
Response Code Sample; 02 02 00 01 A1 03
```



Chapter 7 • ABx Error Codes

The RFID controller will return an error code (in Hex) if it encounters a fault during operation. ABx errors are caused, primarily by improperly entering command parameter syntax. Entering an incorrect length value, for example, will generate an error.

If the controller is powered down and loses its internal configuration, simply executing any command could generate errors. When a non-contiguous read or write command is issued to the controller, yet no such address was pre-configured, an error will result. This error occurs when the user does not configure the controller with the list of non-contiguous read/write addresses.

In ABx Standard, the error code will be returned in the LSB of the second register of the response.

The table below lists ABx error codes and their descriptions.

ABx Error Code Table

Error Code	Description
0x01	Non-contiguous Read has failed
0x02	Non-contiguous Write has failed
0x03	Non-contiguous Read/Write Configuration has failed
0x04	Fill Operation has failed
0x05	Block Read has failed
0x06	Block Write has failed
0x07	Block Write security error
0x08	Search Tag Operation failed
0x19	Protected Address violation
0x20	Non-contiguous Read/Write attempted without Pre-Configuration
0x21	Input Command does not match pre-defined format (syntax error)



ABx Fast Error Response Structure

The structure of an ABx Fast error response is shown below (where XX is a 1-byte value indicating the error that occurred).

Field	Header	Response Size MSB	Response Size LSB	Error Flag	Error Code	Checksum	Terminator
Content	0x0202	0x00	0x02	0xFF	0XX	optional	0x03

ABx FAST ERROR RESPONSE EXAMPLE

A Block Write fail (error code 0x06) message would appear (in Hex) as the following:

Code Sample: 0202 0002 FF06 F803



ABx ASCII Error Response Structure

The Structure of an ABx ASCII error response is shown below.

Field	Header	Response Size	Error Flag	Error Code	Checksum	Terminator
Number of ASCII Characters	2	4	2	2	2	1
Contents	<STX><STX> (0x02, 0x02)	Packet length in bytes excluding the header, response size, checksum and terminator bytes	0xFF	1-byte Hex error code	Optional Checksum	<ETX> 0x03

ABx ASCII ERROR RESPONSE EXAMPLE

A Block Write fail (error code 0x06) message would appear as the ASCII character string:

```
Code Sample: <STX><STX>0002FF06F8<ETX>
```

In Hex, the same error is displayed as the following string:

```
Code Sample: 0x02, 0x02, 0x30, 0x30, 0x30, 0x32, 0x46, 0x46, 0x30, 0x36, 0x46, 0x38, 0x03
```



ABx Standard Error Response Structure

The Structure of the ABx Standard error response from the RFID Controller is shown below.

Field	Command Error Header	Command Error Header	Error Code	Error Code	Message Terminator	Message Terminator
	MSB	LSB	MSB	LSB	MSB	LSB
Content	0xAA	0xFF	0x00	(Error Code Value in Hex)	0xFF	0xFF

ABx STANDARD ERROR RESPONSE EXAMPLE

A Block Write fail (error code 0x06) response would appear as the following:

Field	Command Error Header	Command Error Header	Error Code	Error Code	Message Terminator	Message Terminator
	MSB	LSB	MSB	LSB	MSB	LSB
Content	0xAA	0xFF	0x00	0x06	0xFF	0xFF

Code Sample: AA FF 00 06 FF FF



Chapter 8 • Troubleshooting

This chapter is designed to help if you are having difficulties using the HF-0405.

HF-0405 Troubleshooting Table

Problem Symptom	Possible Reason	Resolution
Controller LEDs not functioning		Check power
Unable to read tag		Check proximity to controller, Try different tag
Etc.		Etc.

Contact Technical Support

Hours of Operation

7am-5pm PST

Escort Memory Systems

Technical Support Department

170 Technology Circle

Scotts Valley, CA 95066 U.S.A

- Phone: 831.438.7000 Ext. 259 or Ext. 257
- Toll Free: 800.626.3993
- Fax: 831.438.5768
- Email: tech_support@ems-rfid.com



Appendix A • Specifications

HF-0405 Data Sheet

- Low Cost 13.56MHz RFID Controller with Integrated Antenna
- Small Form Factor 40mm x 56mm x 25mm
- Reads/Writes ISO 14443A/B, ISO 15693 and ICODE 1 RIFD tags (LRP/HMS-series compatible)
- RS232 or RS422 Point to Point Serial Interfaces or RS485 MUX32 protocol
- IP67 Rated
- Fully Encapsulated Electronics
- 7 LED Status Indicator Lights
- Downward Compatible with HMS827, HMS828, LRP75 and LRP76 products
- Flash Memory for Software Upgrades
- Unique Serial Number ID on Every Controller
- Software Configurable
- FCC/CE/ARIB T-82 Agency Compliance Certification (Pending)



Technical Specifications

- Read/Write Range Up To: 100mm (ISO 15693) / 50mm (ISO 14433) with ISO Card Tags
- Supply Voltage: 12-24VDC $\pm 10\%$; 150mA@24VDC (3.60W)
- 26.5kBaud/106kBaud Air Protocols with CRC Error Detection
- RS232/RS422 Baud Rates: 9600, 19.2k, 38.4k, 57.6k, 115.2k
- RS485 Baud Rate: 9600 or 115.2k
- 7 Discrete LED Indicators: Power, Serial Communication, RF Activity, MUX Address, System Diagnostics and Controller Status
- Connector: M12 Circular Male IP67 (8-pin for RS232/422; 5-pin for RS485)
- Physical Dimensions: 40mm x 56mm x 25mm
- Internal Antenna Dimensions: 36mm x 36mm
- Operating Temperature: -20° to 50°C (-4° to 122°F)
- Storage Temperature: -40° to 85°C (-40° to 185°)
- Humidity 100%
- Protection Class IP67
- Shock Resistance IEC 68-2-27 Test EA 30g; 11msecs; 3 Shocks Each Axis
- Vibration Resistance IEC 68-2-6 Test FC 1.5mm; 10 to 55Hz; 2 Hours Each Axis.



Appendix B • Models and Accessories

HF-0405-232-01

Stock Code	Quantity	Description
00-3000	1.00	Configuration Tag for HF-0405-232 ICODE SLI,54MM X 86MM
20-1940	2.00	Screw, (M4-20 PPH SS 18-8\302)
20-5918	2.00	Hex Nut, (M4 SS 18-8\302)
14-3137	1.00	Mounting Bracket for HF-0405, NORYL, BLACK GTX830

HF-0405-422-01

Stock Code	Quantity	Description
00-3001	1.00	Configuration Tag for HF-0405-422 ICODE SLI,54MM X 86MM
20-1940	2.00	Screw, (M4-20 PPH SS 18-8\302)
20-5918	2.00	Hex Nut, (M4 SS 18-8\302)
14-3137	1.00	Mounting Bracket for HF-0405, NORYL, BLACK GTX830

HF-0405-485-01

Stock Code	Quantity	Description
00-3002	1.00	Configuration Tag for HF-0405-485 ICODE SLI,54MM X 86MM
20-1940	2.00	Screw, (M4-20 PPH SS 18-8\302)
20-5918	2.00	Hex Nut, (M4 SS 18-8\302)
14-3137	1.00	Mounting Bracket for HF-0405, NORYL, BLACK GTX830



HF-0405 Compatible Accessories

Tags

Escort Memory Systems designs and manufactures several lines of RFID tags and transponders. In particular, the LRP and HMS series passive read/write RFID tags perform well with HF-0405 controllers. Our HMS tags are tuned slightly off frequency which improves the inductive coupling characteristics of the tag.

Cables

RS485 cables, connectors, Subnet16, Trunk line and Drop-T parts and accessories are available.

Current rating for cables:

- ThinNet will support 6.4A
- ThickNet will support 17.6A power and ground; 13.6A for data.
- 12mm connectors will support 3A.

Power Supplies

EMS offers universal power supplies with 24V DC output.



Appendix C • ASCII Chart

ASCII or Control Character	Decimal Value	Hex Value	ASCII or Control Character	Decimal Value	Hex Value	ASCII or Control Character	Decimal Value	Hex Value	ASCII or Control Character	Decimal Value	Hex Value
NUL	0	0	(Space)	32	20	@	64	40	'	96	60
SOH	1	1	!	33	21	A	65	41	a	97	61
STX	2	2	"	34	22	B	66	42	b	98	62
ETX	3	3	#	35	23	C	67	43	c	99	63
EOT	4	4	\$	36	24	D	68	44	d	100	64
ENQ	5	5	%	37	25	E	69	45	e	101	65
ACK	6	6	&	38	26	F	70	46	f	102	66
BEL	7	7	'	39	27	G	71	47	g	103	67
BS	8	8	(40	28	H	72	48	h	104	68
HT	9	9)	41	29	I	73	49	i	105	69
LF	10	A	*	42	2A	J	74	4A	j	106	6A
VT	11	B	+	43	2B	K	75	4B	k	107	6B
FF	12	C	,	44	2C	L	76	4C	l	108	6C
CR	13	D	-	45	2D	M	77	4D	m	109	6D
SO	14	E	.	46	2E	N	78	4E	n	110	6E
SI	15	F	/	47	2F	O	79	4F	o	111	6F
DLE	16	10	0	48	30	P	80	50	p	112	70
DC1	17	11	1	49	31	Q	81	51	q	113	71
DC2	18	12	2	50	32	R	82	52	r	114	72
DC3	19	13	3	51	33	S	83	53	s	115	73
DC4	20	14	4	52	34	T	84	54	t	116	74
NAK	21	15	5	53	35	U	85	55	u	117	75
SYN	22	16	6	54	36	V	86	56	v	118	76
ETB	23	17	7	55	37	W	87	57	w	119	77
CAN	24	18	8	56	38	X	88	58	x	120	78
EM	25	19	9	57	39	Y	89	59	y	121	79
SUB	26	1A	:	58	3A	Z	90	5A	z	122	7A
ESC	27	1B	;	59	3B	[91	5B	{	123	7B
FS	28	1C	<	60	3C	\	92	5C		124	7C
GS	29	1D	=	61	3D]	93	5D	}	125	7D
RS	30	1E	>	62	3E	^	94	5E	~	126	7E
US	31	1F	?	63	3F	_	95	5F			



Appendix D • RFID Terminology & Definitions

TERM	DEFINITION
Active Tag	An RF tag (transponder) which is partly or completely battery-powered. Batteries may be replaceable or sealed internally.
Addressability	The ability to address bits, fields, pages, files or other areas of memory in a transponder.
Alignment	An indication of the orientation of the transponder, relative to the controller antenna (this is sometimes referred to as the coupling).
Alphanumeric	Denoting that information contains alphabet characters and numeric characters. For example: A1234C9. A string of alphanumeric data can also contain other printable characters such as punctuation marks.
Antenna	The antenna is the part of the controller that radiates RF energy to, and receives energy from the transponder.
ASCII	American Standard Code for Information Interchange. A computer code consisting of 128 alphanumeric and control characters, each encoded with 7 bits, used for the exchange of information between computer devices.
ASCII Protocol	This is a simple protocol that you can use to send ASCII character commands to the controller. It is possible to use a standard terminal emulator program to send ASCII commands. The ASCII full-duplex protocol can only be used with RS232 or RS422.
Asynchronous Transmission	A method of data transmission that doesn't require timing information in addition to data. The beginnings and ends of characters, or blocks of characters, are indicated by start and stop bits.
Baud	The rate at which a data channel transfers bits of information. The rate is measured in Bits Per Second (BPS).
Binary	A numbering system in which numbers are expressed as combinations of digits 0 and 1, based on powers of 2. In computing these can be represented electrically as 'on' or 'off'.



TERM	DEFINITION
Binary Coded Decimal	A number in binary code always written in groups of four bits, each group representing one digit of the number, for example 0011 1001 is 39.
Byte	Eight bits of data (0x00 01 02 03 04 05 06 07)
Capacity	A measure of the maximum amount of information that can be stored in a transponder. The amount may be a few bits or bytes assessable to the user, or may include addresses reserved to the manufacturer.
Capture Field/Area/Zone	The region of the electromagnetic field, generated by the antenna, in which transponders will operate.
Checksum (CSUM)	An addition to the contents of a block of data. This code can then be checked before and after transmission to determine whether the data has been corrupted or lost (see also: CRC).
Continuous Read	A mode of operation, in which the controller repeatedly attempts to issue a specific command (at set time intervals).
ASCII Control Characters	The ASCII character set is made up of all the possible combinations that can be made with 7 bits of information. Many of these bit patterns are mapped against recognizable characters which can be displayed on a screen or printer, while others are defined as control characters, whose functions are to control devices such as printers (see Appendix C: ASCII Chart).
CRC	Cyclic Redundancy Check
Data Transfer Rate	The number of characters that can be transferred within a given time.
Download	The process of transferring controller configuration data from host PC to the RFID controller.

TERM	DEFINITION
Frequency	<p>The number of times a signal executes a complete excursion through its maximum and minimum values and returns to the same value (cycles).</p> <ul style="list-style-type: none"> • LF Low Frequency 30 kHz to 300 kHz • MF Medium Frequency 300 kHz to 3 MHz • HF High Frequency 3 MHz to 30 MHz • VHF Very High Frequency 30 MHz to 300 MHz • UHF Ultra High frequency 300 MHz to 3 GHz
Handshaking	<p>A mechanism for the regulation of the flow of data between devices. For example: Handshaking can be used to prevent a controller from temporarily overwhelming the host with Command Response data.</p>
Hexadecimal (Hex)	<p>A method of numerically representing data based on the number 16. Hex notation uses the numbers 0 to 9 and letters A to F (where the decimal number 10 is represented in hexadecimal as 'A'). In this guide Hex values are preceded by 0x, as in “<i>address 0xFFFE</i>” (it is also considered correct to append Hex values with a lower case h, as in “<i>interrupt 20h</i>”).</p>
Host Computer	<p>The computer that issues commands to and receives responses from the RFID controller.</p>
In Field Reporting	<p>A mode of operation in which the controller reports a transponder ID on entering the field and will not return further reports of that transponder until a prescribed time interval has elapsed.</p>
Interface	<p>An electrical or physical standard for the interconnection of devices.</p>
Interrogator	<p>Synonymous with RFID controller.</p>
ISM	<p>Industry, Science & Medical</p>
LED	<p>Light Emitting Diode</p>
LF	<p>Low Frequency</p>
LSB	<p>Least Significant Byte. Also referred to as the Low Byte or second byte in a 2-byte “word.”</p>

TERM	DEFINITION
Memory Card	A Read/Write or re-programmable transponder in credit card size. Data can be accessed via direct contact, through a microprocessor (smart card) or via a non-contact RF link.
MSB	Most Significant Byte. Also referred to as the High Byte or first byte in a 2-byte "word."
Multidrop	Multiple devices at various locations connected in parallel (or acting similar to parallel devices). RS-485 (2-wire or 4-wire) supports Multidrop RFID controller configurations.
MUX	Multiplexer
Noise	Unwanted ambient electrical signals found in the operating environment of RFID equipment.
OEM	Outside Engineering Manufacturer or Original Equipment Manufacturer.
Orientation	The alignment of a transponder with respect to the RFID controller's antenna.
Out of Field Reporting	A mode of operation in which the data from a transponder is reported only after the transponder has left the capture field of the controller.
Parity	A technique used to detect data transmission errors by adding an extra bit to each character. This bit is set to 1 or 0 to make the total number of bits ODD or EVEN, depending on the type of parity in use.
Passive Tags	An RFID transponder that does not contain any internal power source (such as a battery). It is powered by electromagnetic signals generated from an RFID antenna.
PCB	Printed Circuit Board
Penetration	This term is used to indicate the ability of a particular radio frequency to pass through non-metallic materials. Low frequency tagging systems are said to have good penetrative properties as their transponders can be read when behind or encased in other materials. Microwave tagging systems, while having greater ranges, are less capable of penetration of materials.
PLC	Programmable Logic Controller

TERM	DEFINITION
Polar Field	A graphical representation of the RF field strength of a transmitting antenna.
Protocol	A set of rules governing the flow of information in a communications system.
Range	The distance between the antenna and a tag or transponder in an RFID system at which signals can be properly received.
Read	The action of obtaining information contained in a tag.
Reader	The device containing the digital electronics that extract information from a transponder and passes the data on to a host computer. Synonymous with RFID controller.
Read Only	A tag that has certain information written into it (usually during manufacturing) and thereafter can only be read.
Read Rate	The maximum rate at which the complete data string can be transferred from a transponder to an RFID controller.
Read/Write	A type of tag that allows new data to be written into it, or that permits the current data to be changed.
Reader/Writer	An RFID device that can act as both reader and writer to a tag. Synonymous with RFID controller.
Response Packet	The string of data sent from the RFID controller to the Host after a command has been issued.
RF	Radio Frequency
RFID	Radio Frequency Identification
RF Tag	See Transponder
RS232	A common physical interface standard specified by the EIA for the interconnection of devices. The standard allows for a single device to be connected (point-to-point) at baud rates up to 9600 bps, and at distances up to 15 meters.

TERM	DEFINITION
RS422	A balanced connection interface standard similar to RS232, but using differential voltages across twisted pair wires. RS422 is more noise immune than RS232 and can be used to connect single or multiple devices to a master unit, at distances up to 3000 meters.
RS485	An enhanced version of RS422, which permits multiple devices (commonly up to 32) to be attached to a twisted pair wire bus at distances of over a kilometer.
Rx	Receive
SCI	Serial Communications Interface
Serial Interface	<p>A physical standard for the interconnection of devices. Common serial interfaces include:</p> <ul style="list-style-type: none"> • RS232 • RS422 • RS485
Synchronization	A mechanism that allows multiple RFID controllers to operate in close proximity by synchronization of their transmissions.
Tag	See Transponder
Transponder	An electronic TRANSMITTER / resPONDER which is attached to an object to be identified and, when appropriate RF signals are received, transmits information as radio signals to a RFID controller. Synonymous with Tag.
Tx	Transmit
Write	The transfer of data to a tag.
Write Rate	The rate at which data can be transferred to a tag, written into the tag's memory and verified as correct. It is measured in bits per second.

Index

<i>I</i>	
13.56 MHZ	See

<i>C</i>	
configuration tag.....	44

<i>D</i>	
dimensions	24

<i>I</i>	
<i>inductive coupling</i>	10
IP67	20
ISM	10

<i>M</i>	
mounting the HF-0405.....	28

<i>P</i>	
package contents.....	16

<i>R</i>	
RFID Case Studies	21
RFID Demonstration Utility.....	20
RFID Installation Checklist.....	25
<i>RFID Strategy</i>	21

<i>S</i>	
Software Updates	19

<i>U</i>	
user supplied components	17





www.ems-rfid.com



HF-0405 RFID CONTROLLER



OPERATOR'S GUIDE



ESCORT MEMORY SYSTEMS
A DATALOGIC GROUP COMPANY