



# ESCORT MEMORY SYSTEMS

A DATALOGIC GROUP COMPANY

## HS500E

OPERATOR'S MANUAL



RFID AT  
WORK™



EMS-RFID.COM



## ESCORT MEMORY SYSTEMS

# HS500E

*Industrial Ethernet Antenna*



### Operator's Manual

P/N: 17-1305 REV 02 (12/05)

Copyright © 2005 Escort Memory Systems, All rights reserved.

Escort Memory Systems reserves the right to make modifications or improvements to its products and/or documentation without prior notification. Escort Memory Systems shall not be liable for technical or editorial errors or omissions contained herein, nor for incidental or consequential damages resulting from the use of this material. Product names mentioned herein are for identification purposes only and may be trademarks and/or registered trademarks of their respective companies.

EMS®, Escort Memory Systems® and the Escort Memory Systems logo are registered trademarks of Escort Memory Systems, a Datalogic Group Company.

Published in USA

## ESCORT MEMORY SYSTEMS

**170 Technology Circle • Scotts Valley • CA • 95066 • USA**

(800) 626-3993 (toll free) • (831) 438-7000 (office) • (831) 438-5768 (fax)

**[www.ems-rfid.com](http://www.ems-rfid.com)**

# HS500E

---

*Read/Write Industrial Ethernet Antenna*



## OPERATOR'S MANUAL

---

*How to Install, Configure and Operate  
Escort Memory Systems'  
HS500E Industrial Ethernet Antenna*



# FCC COMPLIANCE NOTICE

---

## FCC Part 15

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses, generates, and can radiate radio frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Users are cautioned that changes or modifications to the unit not expressly approved by Escort Memory Systems may void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference that may cause undesired operation.

This product complies with CFR Title 21 Part 15.





---

# TABLE OF CONTENTS

---

<b>FCC COMPLIANCE NOTICE</b>	<b>4</b>
<b>TABLE OF CONTENTS</b>	<b>5</b>
<b>CHAPTER 1: GETTING STARTED</b>	<b>8</b>
<b>1.1 Introduction</b>	<b>8</b>
1.1.1 Company Background	8
1.1.2 RFID Overview	8
<b>1.2 About this Manual</b>	<b>9</b>
1.2.1 Who Should Read this Manual?	9
1.2.2 HEX Notation	9
<b>1.3 Dimensions &amp; Diagrams</b>	<b>10</b>
1.3.1 Dimensions – Top View	10
1.3.2 Dimensions – Side View	11
1.3.3 Dimensions – Rear View (Power & Ethernet)	12
1.3.4 LED Descriptions	13
1.3.5 Antenna Read Range - Front View	14
1.3.6 Antenna Read Range - Side View	15
<b>1.4 Installation &amp; Setup</b>	<b>16</b>
1.4.1 Installation Precautions	16
1.4.2 Installing the HS500E	17
<b>CHAPTER 2: IP CONFIGURATION</b>	<b>18</b>
<b>2.1 The HTML Server</b>	<b>18</b>
<b>2.2 IP Address Configuration</b>	<b>18</b>
2.2.1 Default IP Address	18
2.2.2 Changing IP Settings	18
<b>2.3 Pinging the HS500E</b>	<b>20</b>
<b>CHAPTER 3: RFID COMMANDS</b>	<b>21</b>
<b>3.1 Command Structure</b>	<b>21</b>
3.1.1 Command Packet Structure Table	22
3.1.2 Response Packet Structure Table	23
<b>3.2 RFID Commands</b>	<b>25</b>
3.2.1 RFID Commands Table	25
Command 02: Read Data	26
Command 03: Write Data	28
Command 05: Fill Tag	30
Command F1: Test LEDs / Get Info	31



Command F2: Start/Stop Repetitive Command	33
Command F3: Write IP Address	35
Command F4: Reset Battery Counter	37
 <b>CHAPTER 4: ERROR CODES</b>	 <b>38</b>
<b>4.1 Error Types</b>	<b>38</b>
4.1.1 Syntax Errors	38
4.1.2 RF Response Errors	38
 <b>CHAPTER 5: ETHERNET/IP PROTOCOL</b>	 <b>39</b>
<b>5.1 Steps to Configure the HS500E</b>	<b>40</b>
5.1.1 HTML Server and OnDemand Overview	40
<b>5.2 HS500E Node Configuration</b>	<b>40</b>
5.2.1 OnDemand Configuration Page	40
5.2.2 OnDemand Node 01 Configuration Page	42
5.2.3 OnDemand Configuration Page (Summary)	44
<b>5.3 Configuring PLC Controller Tags</b>	<b>45</b>
5.3.1 Controller Tags Summary	45
<b>5.4 Checking OnDemand Status</b>	<b>46</b>
<b>5.5 Using the HS500E with RSLogix 5000</b>	<b>47</b>
5.5.1 Ethernet/IP Handshaking	48
5.5.2 Ethernet/IP Handshaking Example	48
<b>5.6 HTML Server and OnDemand PLC Support</b>	<b>51</b>
 <b>CHAPTER 6: MODBUS TCP PROTOCOL</b>	 <b>52</b>
<b>6.1 Modbus TCP Overview</b>	<b>52</b>
6.1.1 Modbus TCP Command Structure	52
6.1.2 Modbus TCP Response Structure	54
<b>6.2 Modbus TCP Handshaking</b>	<b>55</b>
6.2.1 Host/HS500E Modbus TCP Handshaking	55
6.2.2 Modbus TCP Command, Response & Handshaking Example	56
 <b>CHAPTER 7: RAW TCP/IP PROTOCOL</b>	 <b>57</b>
<b>7.1 RAW TCP/IP Overview</b>	<b>57</b>
<b>7.2 RAW TCP/IP Command &amp; Response Examples</b>	<b>58</b>
7.2.1 RAW TCP/IP Command Example	58
7.2.2 RAW TCP/IP Response Example	59
 <b>APPENDIX A: IP ADDRESS RESET</b>	 <b>60</b>



<b>APPENDIX B: ASCII CHART</b>	<b>61</b>
<b>APPENDIX C: ETHERNET/IP - OBJECT MODEL</b>	<b>63</b>
<b>C.1 Ethernet/IP - Required Objects</b>	<b>64</b>
C.1.1 Identity Object (0x01- 1 Instance)	64
C.1.2 Message Router Object (0x02)	66
C.1.3 Assembly Object (0x04 – 3 Instances)	66
C.1.4 Connection Manager Object (0x06)	70
C.1.5 TCP Object (0xF5 - 1 Instance)	70
C.1.6 Ethernet Link Object (0xF6 - 1 Instance)	72
<b>C.2 Vendor Specific Objects</b>	<b>73</b>
C.21 HS500E Consume Data Object (0x64 - 32 Instances)	73
C.22 HS500E Produce Data Object (0x65 - 32 Instances)	76
C.23 OnDemand Object (0x67 - 10 Instances)	79
<b>EMS WARRANTY</b>	<b>82</b>





# CHAPTER 1: GETTING STARTED

## 1.1 INTRODUCTION

Welcome to the **HS500E Industrial Ethernet Antenna - Operator's Manual**. This manual will assist you in the installation, configuration and operation of Escort Memory Systems' HS500E Industrial Ethernet Antenna.

The HS500E Ethernet Antenna is a complete read/write Radio-Frequency Identification solution. It is designed to be reliable and rugged, in order to meet and exceed the requirements of the industrial automation industry. The HS500E Ethernet Antenna provides RFID data collection and control solutions to shop floor, item-level tracking and material handling applications.

### 1.1.1 Company Background

Escort Memory Systems has long been an industry leader in providing Radio Frequency Identification (RFID) devices, building a solid reputation by consistently delivering an extended selection of quality, durable industrial RFID systems.

### 1.1.2 RFID Overview

Aside from configuring the RFID network equipment, the first step in most RFID applications involves attaching a tag (which is also called a "*transponder*") to a product or its carrier. The RFID tag acts as an electronic identifier, portable job sheet, or real-time tracking database. Tags can be identified, read from and written to by issuing specific RFID commands from a Host computer or PLC (Programmable Logic Controller).

The HS500E can transmit data through any nonconductive, non-metallic material, while the tag is moving or standing still and while it is in or out of the direct line of sight.







## 1.2 ABOUT THIS MANUAL

This document provides guidelines and instructions on how to install, configure and operate the HS500E Industrial Ethernet Antenna. Descriptions of the RFID command set are also included, as are instructions detailing how to issue commands from a Host computer to the HS500E.

### 1.2.1 Who Should Read this Manual?

Those who will be installing, configuring and operating the HS500E should read this manual. This may include the following people:

- **Hardware Installers**
- **System Integrators**
- **Project Managers**
- **IT Personnel**
- **System and Database Administrators**
- **Software Application Engineers**
- **Service and Maintenance Engineers**

### 1.2.2 HEX Notation

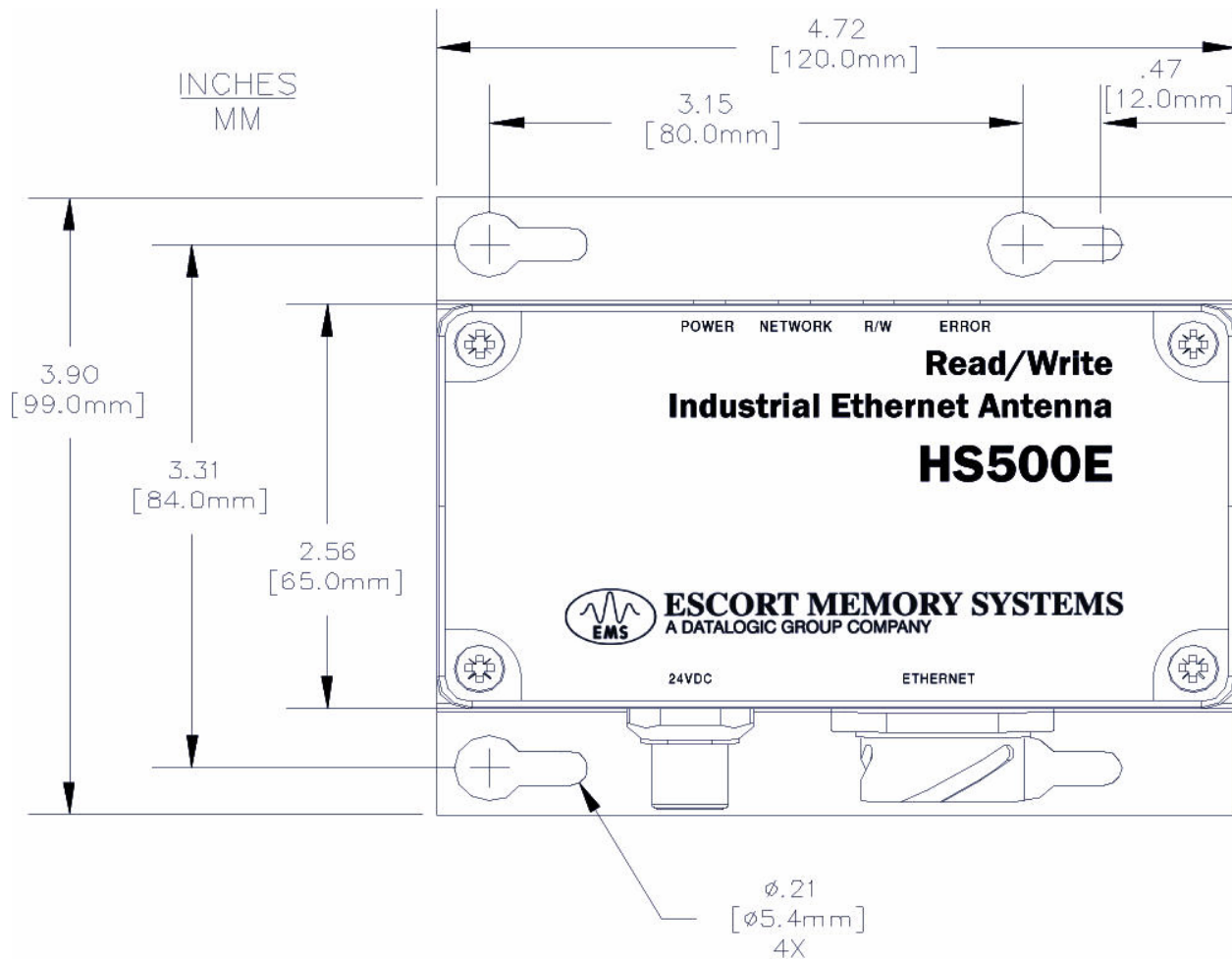
In this manual, numbers expressed in Hexadecimal notation are prefaced with "0x". For example, the number "10" in decimal is expressed as "0x0A" in hexadecimal. See Appendix A for a chart containing Hex values, ASCII characters and their corresponding decimal integers.





## 1.3 DIMENSIONS & DIAGRAMS

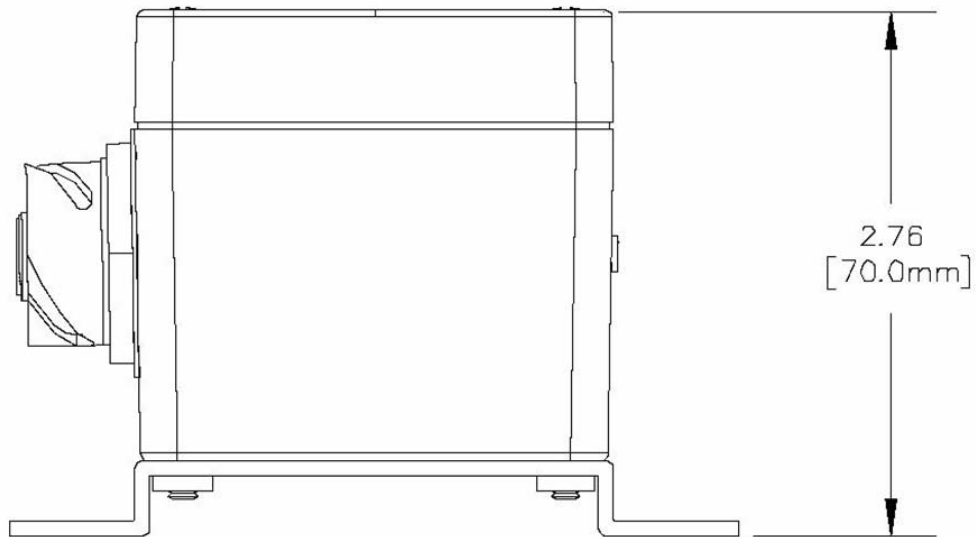
### 1.3.1 Dimensions – Top View



*Dimensions – Top View*

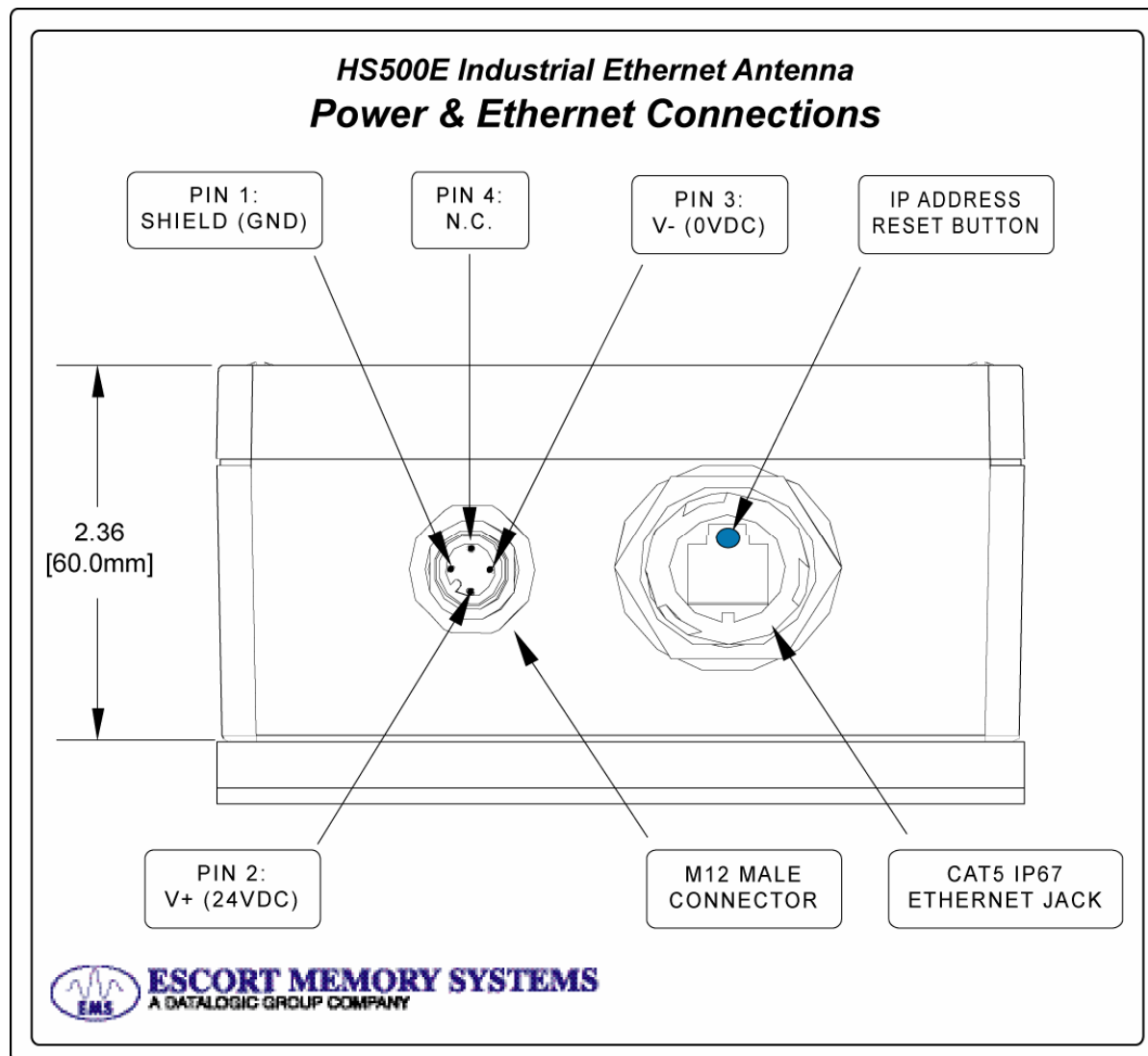


### 1.3.2 Dimensions – Side View



*Dimensions – Side View*

### 1.3.3 Dimensions – Rear View (Power & Ethernet)

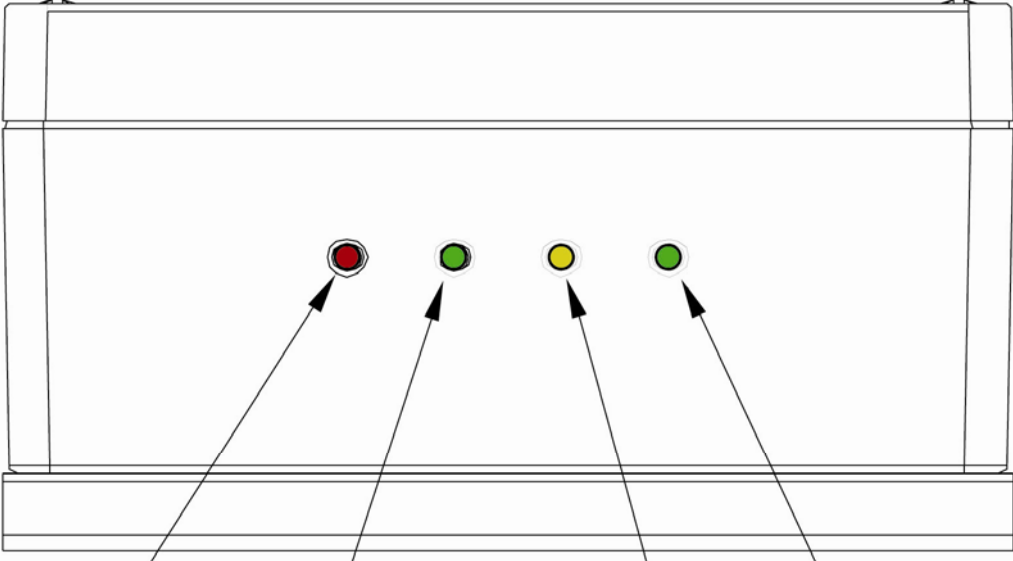


*Dimensions – Rear View  
(Power & Ethernet)*

### 1.3.4 LED Descriptions


**HS500E Industrial Ethernet Antenna**

**LED Descriptions**



<b>ERROR</b> RED	<b>R/W</b> GREEN	<b>NETWORK</b> YELLOW	<b>POWER</b> GREEN
---------------------	---------------------	--------------------------	-----------------------

- ERROR:** This red LED will illuminate (ON) - signaling that an error has occurred. LED will remain ON until unit receives another command.
- R/W:** This green LED will flicker ON and OFF during which unit is reading data from or writing data to a tag.
- NETWORK:** This yellow LED will flicker on/off while the unit is receiving data from or writing data to the Host or PLC.
- POWER:** This green LED will remain lit while power is applied to the unit.



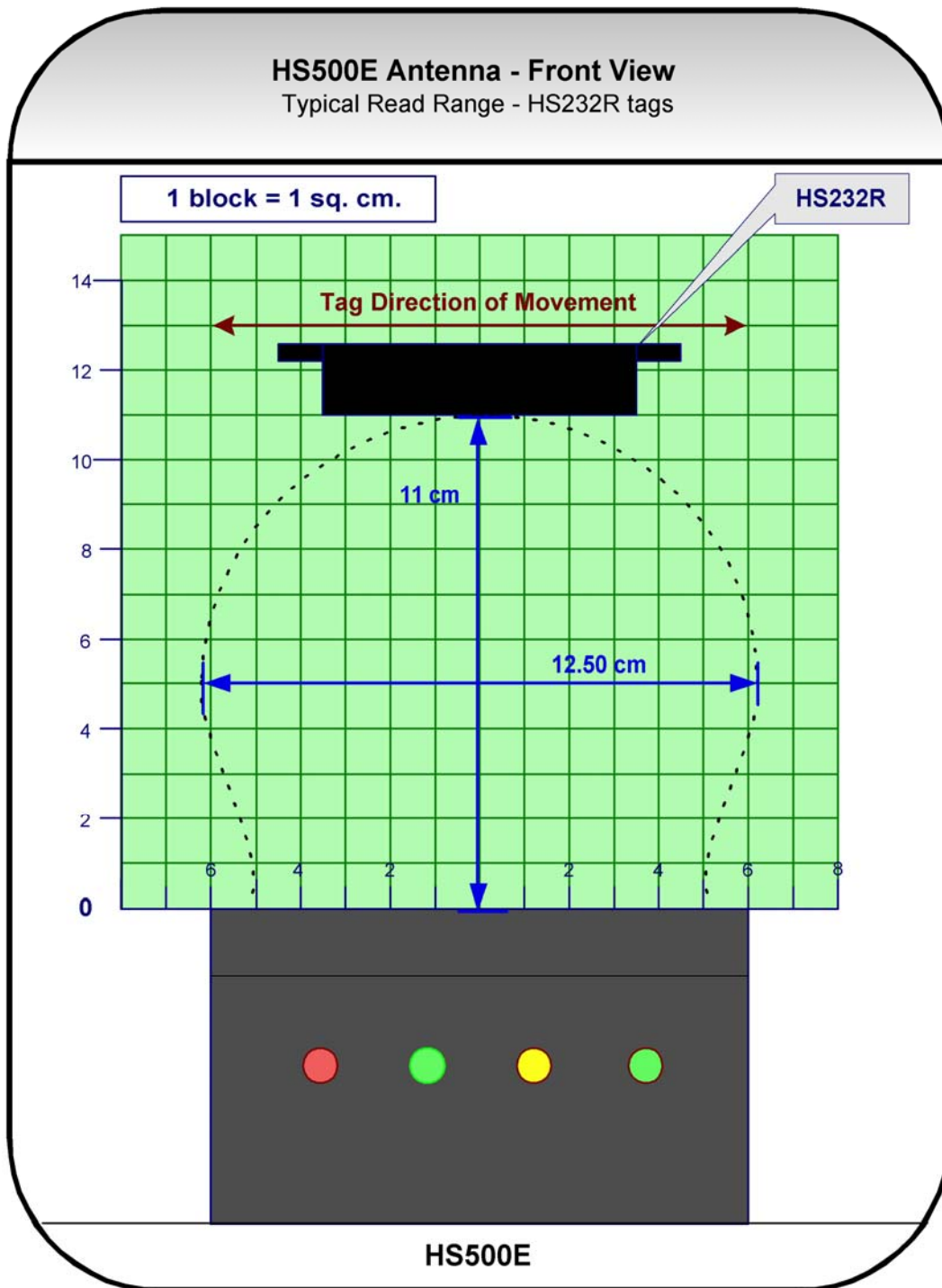
**ESCORT MEMORY SYSTEMS**

A DATALOGIC GROUP COMPANY

*LED Descriptions*



### 1.3.5 Antenna Read Range - Front View

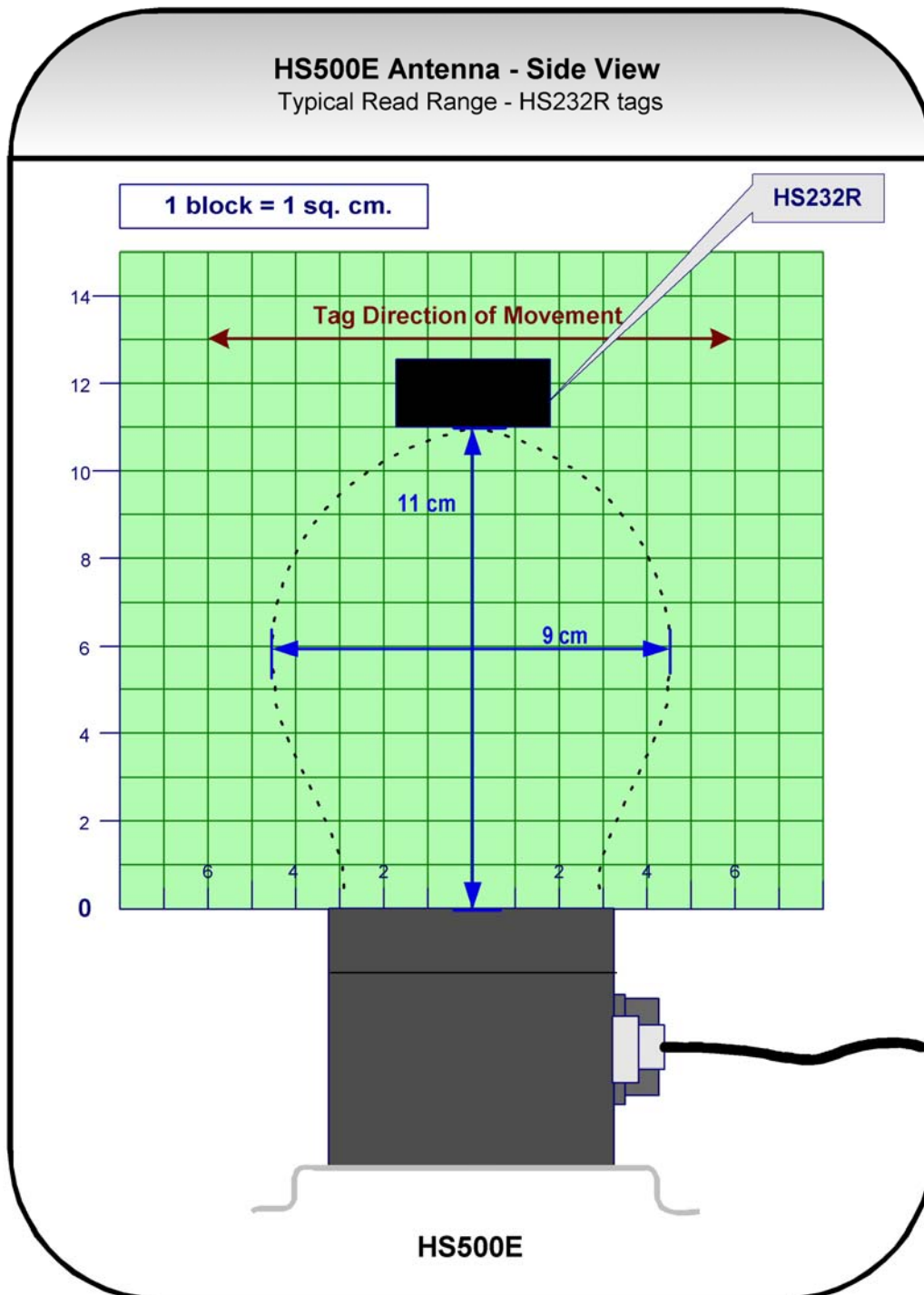


**NOTE:**

The range listed above was defined in free air. However, proximity to metal, water and RF interference can affect range performance and results. All RFID applications should be tested to ensure adequate RF performance can be achieved.



### 1.3.6 Antenna Read Range - Side View



**NOTE:**

The range listed above was defined in free air. However, proximity to metal, water and RF interference can affect range performance and results. All RFID applications should be tested to ensure adequate RF performance can be achieved.





## 1.4 INSTALLATION & SETUP

### 1.4.1 Installation Precautions

#### *Mounting Guidelines*

- Avoid mounting the HS500E or its RFID controllers near sources of EMI (electro-magnetic interference) or near devices that generate high ESD (electro-static discharge) levels.
- Do not route cables near unshielded cables or near wiring carrying high voltage or high current.
- Avoid routing cables near motors and solenoids.
- Cross cables only at perpendicular intersections (if at all).

#### *Important Configuration Note*

All HS500E Antennas leave the factory configured to the same default IP address – **192.168.0.100**. It is recommended that installers attach and configure only one HS500E Antenna at a time. Connecting multiple HS500E Antennas prior to assigning each a unique IP address could result in network errors and IP conflicts.

#### *Power Requirements*

The HS500E requires a power supply capable of providing 24 volts DC @ 0.5A (12W).



### 1.4.2 Installing the HS500E

1. Unpack and inspect the HS500E hardware and accessories. If an item appears to be damaged, notify your EMS distributor immediately.
2. Securely mount the HS500E to your chosen location using four (4) #10 [M5] screws and matching locking washers and nuts. The HS500E may be mounted in any orientation, but should be aligned in such a manner that the four LED indicators can be seen during operation.
3. Insert one end of a Category 5 Ethernet cable into the IP67 RJ45 connection housing. Install the RJ45 plug per the included instruction sheet. Attach the assembled mating connector to the HS500E and twist clock-wise one-half revolution.
4. Connect the other end of the Ethernet cable to the Host or PLC network. A crossover cable (P/N: CBL-1479) may be required if connecting the HS500E directly to a computer (rather than to a switch, hub or router).
5. Connect the female 4-pin M12 power supply cable to the male 4-pin M12 connector on the HS500E.
6. Turn the power supply ON. The Network and Error LEDs will flash 6 times (4 slow, 2 fast), after which the antenna will be ready to receive commands.
7. From the Host, connect to the HS500E and assign it a new IP address (see *Chapter 2 – IP Configuration*).
8. Note the new IP address on a sticker or label and attach it to the unit.
9. Repeat these steps for each HS500E Antenna to be installed.

Plan to perform a test phase and construct a small scale, independent network that includes only the essential devices required to test your RFID application. To avoid possible interference with other devices, do not, at first, connect the RFID testing environment to an existing office network.





# CHAPTER 2: IP CONFIGURATION

---

## 2.1 THE HTML SERVER

Built into the HS500E is an embedded **HTML Server** which provides a Website-like user interface with all of the tools necessary to configure the unit.

The first step in configuring the HS500E is to set its IP address. This particular chapter describes the IP configuration procedure via the HTML Server. The HTML Server has many other uses and features which are covered later in this manual.

## 2.2 IP ADDRESS CONFIGURATION

### 2.2.1 Default IP Address

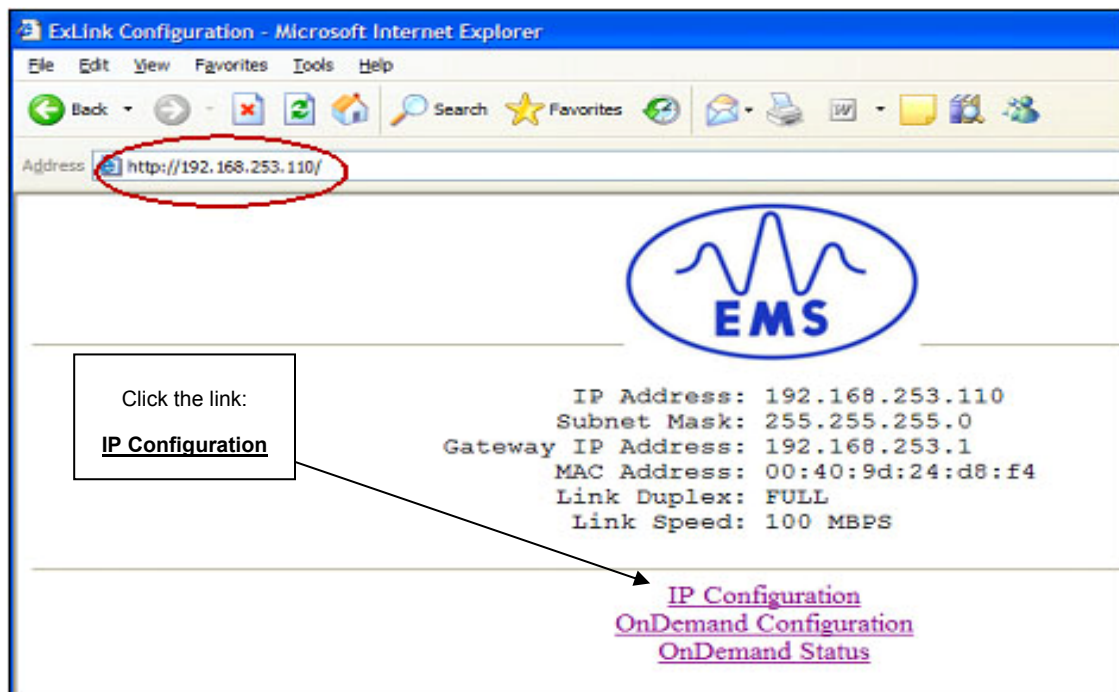
**The HS500E's factory default IP address is 192.168.0.100.**

To reset the unit's IP address to the factory default settings, please see **Appendix A**.

### 2.2.2 Changing IP Settings

- 1 **Open** a Web browser on the PC.
- 2 In the URL address field, **enter** the HS500E's IP address (**192.168.0.100 = factory default**).
- 3 **Press** ENTER.

The *HTML Server - Main Page* will be displayed.



*The HTML Server- Main Page*

- 4 At the *HTML Server - Main Page*, **click** the link labeled **IP Configuration**.

The *IP Configuration Page* will be displayed. You will arrive at a page similar to the one displayed below.

## IP Configuration

IP Address:	<input type="text" value="192.100.100.210"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Gateway Address:	<input type="text" value="0.0.0.0"/>

*(The unit resets automatically when settings are modified)*

[Main Page](#)

*The HTML Server - IP Configuration Page*

- 5 **Enter** new IP address values in the fields provided.



- 6 Click the “**Save Settings**” button to store the configuration changes to the HS500E’s non-volatile flash memory.
- 7 Manually **cycle power** to the HS500E. It takes 15 – 30 seconds for the HS500E to reboot, at which time your IP configuration changes will be implemented.
- 8 After the HS500E has completely restarted, **verify** the new IP configuration by opening a Web browser and entering the newly assigned IP address in the URL field.

## 2.3 PINGING THE HS500E

After the HS500E has restarted, go to the PC and run **PING.EXE** (from Microsoft Windows systems) or use another network diagnostic tool that can run a similar TCP/IP ping command. Using a Ping utility helps verify that the HS500E is accessible across the network.

- To Ping the HS500E from the PC, open a command prompt and at the C:\> prompt type:

```
Ping (IP Address)
```

(Where “*IP Address*” is the new IP address assigned to the HS500E).

If the HS500E is online and functioning, a successful response will be similar to:

```
Reply from (IP Address): bytes=32 time=3ms TTL=60
Reply from (IP Address): bytes=32 time=1ms TTL=60
Reply from (IP Address): bytes=32 time=1ms TTL=60
Reply from (IP Address): bytes=32 time=1ms TTL=60
```

If the PC does not receive a successful response from the HS500E, it may indicate an improperly configured IP address setting. Please verify that you followed the instructions above for setting the IP address of the HS500E.

Also, be sure to disable any firewall services running on the PC. Firewalls can potentially block communications between the PC, the PLC and/or the HS500E.



## CHAPTER 3: RFID COMMANDS

---

### 3.1 COMMAND STRUCTURE

RFID commands are Host-generated packets of data that contain instructions intended for the HS500E.

In general, RFID commands adhere to a **6-word** minimum packet structure, where each **word** within a packet is comprised of **2-bytes**; a Most Significant Byte (**MSB**) and a Least Significant Byte (**LSB**). The MSB and LSB are also sometimes referred to as the *High Byte* and the *Low Byte*, respectively.

**NOTE:**

The basic format and packet structure of the RFID commands presented in this manual are protocol independent and can be implemented the same for all Industrial Ethernet protocols (Ethernet/IP, Modbus/TCP, etc.).



### 3.1.1 Command Packet Structure Table

<u>Word #</u>	<u>MSB</u>	<u>LSB</u>	<u>Description</u>
01	00	06 (+ number of additional data words, if any)	<b>OVERALL LENGTH:</b> The first word in a command packet is the <b>Overall Length</b> . This 2-byte value indicates the total number of words in the command (including this - the <i>Overall Length</i> field). This value will always be at least six words (0x0006).
02	AB	03	<b>COMMAND ID:</b> The second word contains the <b>Command ID</b> . For example: Write Data Command = 0xAB03  <i>See the Section 3.2.1 - RFID Command Table for a complete list.</i>
03	00	01	<b>NODE ID:</b> The third word contains the <b>Node ID</b> of the antenna / controller for which the command is directed. This value should always be <b>0x0001</b> for the HS500E.
04	00	32	<b>TIMEOUT VALUE:</b> Word four in a command packet contains the 2-byte <b>Timeout Value</b> . This value sets the maximum length of time for which the HS500E will attempt to complete the given command. This " <i>time limit</i> " is measured in $1/10^{\text{th}}$ (.10) second increments, where <b>0x0032</b> = $50 \times .10 = 5$ seconds.
05	00	01	<b>START ADDRESS:</b> The fifth word, <b>Start Address</b> , indicates the location of tag memory where a read or write operation will begin (when applicable).
06	00	01	<b>READ/WRITE LENGTH:</b> The <b>Read/Write Length</b> is the sixth word (when applicable) and represents the number of bytes that are to be retrieved from or written to the RFID tag.





### 3.1.2 Response Packet Structure Table

<u>Word #</u>	<u>MSB</u>	<u>LSB</u>	<u>Description</u>	
01	00	06 (+ number of returned data words, if any)	<b>OVERALL LENGTH:</b> The first word in a response packet is the <b>Overall Length</b> . This 2-byte value indicates the total number of words in the response (including this - the <i>Overall Length</i> field). Length will always be at least six words (0x0006).	
2	(RF Error)	(Command Echo / Error Code)	<b>RF ERROR COUNTER:</b> The MSB of the second word holds the single-byte <b>RF Error Counter</b> . This value identifies the number of times RF transmission failed or could not be completed for this command.	<b>COMMAND ECHO / ERROR CODE:</b> The <b>Command Echo</b> is returned in the LSB and displays the Hex value of the executed command.  When an error occurs, the LSB will hold a single byte <b>Error Code</b> .
03	(IC)	(Node ID Echo) 0x01	<b>INSTANCE COUNTER:</b> The MSB of word 03 contains the <b>Instance Counter</b> . This single-byte value is incremented by one following each response (range = 0x00 to 0x7F). Cycling power to the unit resets this counter to 0x00.	<b>NODE ID ECHO:</b> The LSB of the third word, <b>Node ID Echo</b> , retrieves the Node ID of the antenna that executed the command (this value will always be 0x01 for the HS500E).
04	(RFT1)	(RFT2)	<b>RF TIME:</b> Word 04 of a response packet contains the <b>RF Time</b> . This two-byte value indicates the portion of the Timeout Value (set in the Command Packet) that remains after the completion of the command (see <i>Total Time</i> below).  <b>RF TIME = (TIMEOUT VALUE - TOTAL TIME)</b>	



<u>Word #</u>	<u>MSB</u>	<u>LSB</u>	<u>Description</u>	
05	(RF Retry)	(Reserved) 0x00	<b>RF RETRY COUNTER:</b> The fifth word contains the <b>RF Retry Counter</b> in the MSB. This counter indicates the number of packets that required re-transmission to successfully complete the given command.	<b>RESERVED:</b> LSB: 0x00
06	(TT1)	(TT2)	<b>TOTAL TIME:</b> The sixth word in a response contains a 2-byte <b>Total Time</b> value used to indicate the interval of time required to complete the specified command and generate this corresponding response.	
07	(RD Byte 1)	(RD Byte 2)	<b>RETURNED DATA (Bytes 1 – 2):</b> Any remaining words will contain <b>Returned Data</b> (when applicable). These additional fields are added to the response packet to hold data that was requested in the command. If an odd number of bytes are retrieved, the LSB of the final Returned Data word will contain 0x00.	
08	(RD Byte 3)	(RD Byte 4)	<b>RETURNED DATA (Bytes 3 – 4) :</b> <b>Returned Data</b> – bytes 3 and 4 (etc.).	



## 3.2 RFID COMMANDS

The HS500E uses a 2-byte *Command ID* number to specify the type of operation to perform.

**Commands 02, 03 and 05** must include the command prefix “**AB**” (0xAB), as in **AB03** (for Command 03). These three commands instruct the HS500E to perform standard RFID operations such as reading from and writing to an RFID tag.

**Commands F1, F3 and F4** must be appended with “**00**” (0x00), as in **F300** (for Command F3). Commands F1, F3 and F4 are used to retrieve information or modify configuration settings that are stored internally in the HS500E Antenna.

**Command F2xx** is designed to continuously repeat one of the first three commands (where **xx** represents the type of repetitive command). Command F2 is to be appended with **02, 03 or 05** which evokes Repetitive Read, Write or Fill commands. For example, **F202** indicates a *Repetitive Read Data* command.

### 3.2.1 RFID Commands Table

<u>Command ID</u>	<u>Command Name</u>	<u>Description</u>
(AB) 02	<a href="#">Read Data</a>	Used to read data from contiguous areas of an RFID tag's memory.
(AB) 03	<a href="#">Write Data</a>	Used to write data to contiguous areas of an RFID tag's memory.
(AB) 05	<a href="#">Fill Tag</a>	Used to fill a specified area of a tag with a single data byte value.
F1 (00)	<a href="#">Test LEDs / Read Info</a>	Used to run an LED diagnostic test and retrieve the installed software version number from the HS500E.
F2 (xx)	<a href="#">Start/Stop Repetitive Command</a>	Used to start (or stop) the repetitive execution of a command. (Where <b>xx</b> represents Commands 02, 03 or 05 for repeating a Read, Write or Fill command).
F3 (00)	<a href="#">Write IP Address</a>	Used to write new IP address configuration settings to the HS500E.
F4 (00)	<a href="#">Reset Battery Counter</a>	Used to reset the value of a tag's Battery Counter.



## COMMAND 02: READ DATA

### DESCRIPTION

Command 02 instructs the H500E to retrieve a specified number of bytes from a contiguous (sequential) area of an RFID tag's memory. The **Read Data** command consists of the Overall Length (OAL), the Command ID Number, Node ID value, Timeout Value, Start Address and Read Length.

The minimum Read Length is 1 byte. If the Read Length extends beyond the last tag address, an error will occur.

The Timeout Value is measured in .10 second increments and can have a minimum value of 1 (0x0001).

Note: Tag address 0x0000 contains the *Battery Counter Value*. The Battery Counter stores a one-byte value that indicates the number of operating hours that an active tag has been in use since it last had its internal batteries replaced. To retrieve this value, the Start Address should be set to 0x0000.

### EXAMPLE

In the example below, the HS500E will read 4-bytes from the tag beginning at address 0x0001. The Timeout value is set for 5 seconds (0x0032 = 50 decimal, 50 x .10 = 5 seconds) for the completion of this command.

Command 02: Read Data – Command Structure			
Field Name	MSB	LSB	Word Value
Overall Length (in words)	00	06	0006
[0xAB] + Command ID Number: 0x02	AB	02	AB02
MSB = Reserved (always 0x00) LSB = Node ID # (always 0x01 for the HS500E)	00	01	0001
Timeout Value in .10 sec increments	00	32	0032
Start Address	00	01	0001
Read Length	00	04	0004



Command 02: Read Data – Response Structure			
Field Name	MSB	LSB	Word Value
Overall Length (in words)	00	08	0008
MSB = RF Error Counter LSB = Command ID Echo	00	02	0002
MSB = Instance Counter LSB = Node ID Echo	01	01	0101
RF Time	RFT1	RFT2	XXXX
MSB = RF Retry Counter LSB = Reserved	01	00	0100
Total Time	TT	TT	TTTT
Returned Data (bytes 1, 2)	D1	D2	DATA
Returned Data (bytes 3,4)	D3	D4	DATA



## COMMAND 03: WRITE DATA

### DESCRIPTION

Command 03 instructs the HS500E to write segments of data to contiguous addresses of an RFID tag's memory. The Write Data command consists of an Overall Length, the Command ID, a Timeout Value, Start Address and Write Length, and the Data Byte Value(s) to be written to the tag.

- **Start Address:** 0x0001 = Starts writing to the first accessible byte of tag memory (byte 0x0000 is reserved for the *Battery Counter Value*).
- **Write Length:** 0x0001 = One byte is the shortest possible Write Length. If the Write Length is set to 0, or extends past the last byte address of the tag, the unit will generate an error.
- When an odd number of bytes are to be written, the LSB (least significant byte) of the final word must contain 0x00.

### EXAMPLE

In this example, a Write Data command will instruct the HS500E to write the specified four bytes to the tag beginning at the Start Address of 0x0001. The Timeout value is set for 5 seconds (0x0032 = 50 decimal,  $50 \times .10 = 5$  seconds) for the completion of this command.

Command 03: Write Data – Command Structure			
Field Name	MSB	LSB	Word Value
Overall Length (in words)	00	08	0008
[0xAB] + Command ID Number: 0x03	AB	03	AB03
MSB = Reserved (always 0x00) LSB = Node ID # (always 0x01)	00	01	0001
Timeout	00	32	0032
Start Address	00	01	0001
Write Length	00	04	0004
Data Byte Values (01, 02)	11	22	1122
Data Byte Values (03, 04)	33	44	3344



Command 03: Write Data – Response Structure			
Field Name	MSB	LSB	Word Value
Overall Length	00	06	0006
MSB = RF Error Counter LSB = Command ID Echo	00	03	0003
MSB = Instance Counter LSB = Node ID Echo	01	01	0101
RF Time	XX	XX	XXXX
MSB = RF Retry Counter LSB = Reserved	01	00	0100
Total Time	TT	TT	TTTT





## COMMAND 05: FILL TAG

### DESCRIPTION

Command 05 is used to instruct the HS500E to write a particular data byte value to all specified contiguous areas of tag memory beginning at the Start Address.

### EXAMPLE

In this example, the HS500E will write the ASCII character “D” (0x44) to 8-bytes of tag memory starting at address 0x0001. The Timeout value is set for 5 seconds (0x0032 = 50 decimal,  $50 \times .10 = 5$  seconds) for the completion of this command.

Command 05: Fill Tag – Command Structure			
Field Name	MSB	LSB	Word Value
Overall Length	00	06	0006
[0xAB] + Command ID Number: 0x05	AB	05	AB05
MSB = Data Byte Value used for the fill. LSB = Node ID # (always 0x01)	44	01	4401
Timeout Value: (5 seconds = .10 seconds x 50)	00	32	0032
Start Address	00	01	0001
Fill Length	00	08	0008

Command 05: Fill Tag – Response Structure			
Field Name	MSB	LSB	Word Value
Overall Length	00	06	0006
MSB = RF Error Counter LSB = Command ID Echo	00	05	0005
MSB = Instance Counter LSB = Node ID Echo	01	01	0101
RF Time	XX	XX	XXXX
MSB = RF Retry Counter LSB = Reserved	01	00	0100
Total Time	TT	TT	TTTT



## COMMAND F1: TEST LEDs / GET INFO

### DESCRIPTION

Command F1 tests the HS500E's LEDs and retrieves the unit's currently installed software version number. This command causes the HS500E's LEDs to flash a coded diagnostic pattern while also retrieving the version number of the installed software.

### EXAMPLE

In this example the LEDs on the HS500E will be tested and its software version number will be retrieved. Timeout Value, Start Address and Read/Write Length parameters are not applicable for this command (all values for these fields should be set to 0x00).

Command F1: Test LEDs / Get Info – Command Structure			
Field Name	MSB	LSB	Word Value
Overall Length	00	06	0006
Command ID Number: 0xF1 + [0x00]	F1	00	F100
MSB = 0x00 LSB = Node ID # (always 0x01)	00	01	0001
Timeout Value	00	00	0000
Start Address	00	00	0000
Read/Write Length	00	00	0000



Command F1: Test LEDs / Read Info – Response Structure			
Field Name	MSB	LSB	Word Value
Overall Length	00	06	0006
MSB =RF Error Counter LSB = Command ID Echo	00	F1	00F1
MSB = Instance Counter LSB = Node ID Echo	01	01	0101
Response Data (first word)	31	2E	312E
Response Data (second word)	30	41	3041
Response Data (third word)	2E	38	2E38

The software version number returned for this example is **1.0A.8**, which is the ASCII equivalent of the Hex string **31 2E 30 41 2E 38**. Note: the period or “point” (.) between characters *is* considered part of the software version number.



## COMMAND F2: START/STOP REPETITIVE COMMAND

### DESCRIPTION

Command F2 is used to instruct the HS500E to continuously repeat a specified RFID command. Note that only Commands 02, 03 and 05 are repeatable.

To begin repeating a command, set the Overall Length to a value of 0x0006 or greater. To stop this command, change the Overall Length to 0x0000 and re-issue the command (or cycle power to the unit).

### EXAMPLE

This example will instruct the HS500E to repeatedly read 4-bytes of data beginning at address 0x0001 of tag memory. The Timeout value is set for 5 seconds (0x0032 = 50 decimal, 50 x .10 = 5 seconds) for the completion of this command.

Command F2: Start/Stop Repetitive Command – Command Structure				
Word #	Field Name	MSB	LSB	Word Value
1	Overall Length	00	06 + number of additional words (for Write and Fill Commands only). To stop, set LSB to 0x00.	0006
2	MSB = Repeat Command Flag: 0xF2 LSB = Command ID to be repeated	F2	02 (03 or 05 for Write and Fill Repeat)	F202
3	MSB is used to indicate Fill Data Byte Value when second word is 0xF205. MSB should be 0x00 when second word is F202 or F203. LSB = Node ID Number (will always be 0x01 for the HS500E)	00	01	0001
4	Timeout Value	00	32	0032
5	Start Address	00	01	0001
6	Read/Write Length	00	04	0004
7	Data Byte Value(s) for Write (only applicable when word 2 is F203).	ZZ	ZZ	ZZZZ



Command F2: Repeat Command (Read Data) – Response Structure				
Word #	Field Name	MSB	LSB	Word Value
1	Overall Length (in words)	00	08	0008
2	MSB = RF Error Counter LSB = Command ID Echo	00	02	0002
3	MSB = Instance Counter LSB = Node ID Echo	01	01	0101
4	RF Time	XX	XX	XXXX
5	MSB = RF Retry Counter LSB = Reserved	YY	00	YY, 00
6	Total Time	TT	TT	TTTT
7	Return Data (bytes 1, 2)*	D1	D2	D1, D2
8	Return Data (bytes 3,4)*	D3	D4	D3, D4

\* Only applicable when word 2 in the command = F202 (Repeat Read Data)



## COMMAND F3: WRITE IP ADDRESS

### DESCRIPTION

Command F3 is used to modify and store the IP address of the HS500E.

NOTE: The unit's IP address can also be changed using the built-in HTML Server. See Chapter 2 for instructions.

Follow the steps below to configure the unit's IP address.

### SETTING THE IP ADDRESS OF THE HS500E

1. Run Command F3 as shown below, (the R/W LED on the HS500E will blink repeatedly for 15 - 20 seconds).
2. After blinking stops, cycle power to the unit (the R/W LED will again blink for 15 -20 seconds).
3. After the R/W LED has stopped blinking (the second time) configure your Host application to connect to the new IP address assigned to the HS500E in step 1.

### EXAMPLE

This example sets the IP address of the HS500E to **192.168.253.115**.

Command F3: Write IP Address – Command Structure			
Field Name	MSB	LSB	Word Value
Overall Length	00	06	0006
MSB = Command ID (0xF3) LSB = 0x00 for this command.	F3	00	F300
IP Address (first octet)	0x00 (always)	C0 (192 decimal)	00C0
IP Address (second octet)	0x00 (always)	A8 (168 decimal)	00A8
IP Address (third octet)	0x00 (always)	FD (253 decimal)	00FD
IP Address (fourth octet)	0x00 (always)	73 (115 decimal)	0073

**RESPONSE FROM HS500E**

There is no response for Command F3 because as soon as the IP address is changed on the HS500E, the existing TCP/IP connection with the Host will be terminated.

To reset the IP address of the HS500E to factory default settings see:  
*Appendix A: IP Address Reset.*

**HS500E Factory Default IP Address: 192.168.0.100**





## COMMAND F4: RESET BATTERY COUNTER

### DESCRIPTION

Command F4 resets the value of a tag's *Battery Counter* to zero (0x00). This command is intended to be used when replacing the batteries in an active RFID tag and will reset the value of the *Battery Counter* to zero (0x00).

Located at tag address 0x0000, the Battery Counter stores a one-byte value that indicates the number of operating hours that the tag has been in use since it has last had its internal batteries replaced. A tag should have its batteries replaced after it has accumulated 15 hours of use. When this value reaches 0x0F, battery life is in a condition of decay and should be replaced.

To retrieve the Battery Counter Value, execute Command 02 and note the value stored at address 0x0000 on the tag. Reading address ZERO on the tag should only be performed by one station in a typical assembly line.

### EXAMPLE

Command F4: Reset Battery Counter Value – Command Structure			
Field Name	MSB	LSB	Word Value
Overall Length	00	06	0006
MSB = Command ID (0xF4) LSB = 0x00 for this command.	F4	00	F400
MSB = 0x00 LSB = Node ID #: (0x01)	00	01	0001
Timeout Value*	00	00	0000
Start Address*	00	00	0000
Read/Write Length*	00	00	0000

\* Not applicable for this command, set values to zero (0x00). This command uses a hard coded Timeout Value of 2 seconds.

### RESPONSE FROM HS500E

There is no response for this command.

### RESET BATTERY COUNTER ERROR

The Reset Battery Counter command may appear to time-out or generate an error. After executing Command F4, the user should execute Command 02 and check the data at tag address 0x0000 to confirm that the value of the Battery Counter was indeed reset to 0x00.



## CHAPTER 4: ERROR CODES

---

The HS500E will generate an error response if it is unable to complete an operation. When an error occurs, the LSB of the second word in a response (the Command Echo word) will be replaced by a 1-byte error code that indicates the actual error that was experienced.

### 4.1 ERROR TYPES

There are basically two types of errors that can occur.

#### SYNTAX ERRORS

The majority of errors that occur do so because of improperly formatted commands. Syntax errors include everything from entering an invalid command ID to attempting to read from or write to an address not within the range of the tag's memory limits.

#### RF RESPONSE ERRORS

This type of error can occur if the distance from the tag to the antenna exceeds the RF range or when a command is not completed before the Timeout Value expires.

#### 4.1.1 Syntax Errors

##### OVERALL LENGTH ERRORS

**0x89:** User sends a command with an overall length value of less than 6 bytes. User miscalculates overall length when executing a Write command.

##### LENGTH LIMITS

**0x8D:** Limits or boundaries concerning a Read/Write/Fill Length field were not satisfied.

**0x8F:** Tag starting address and length conflict with one another. This can occur if, for example, the user decides to read data near the end of the tag and specifies a length that exceeds the remainder of the tag memory.

##### WRITE LENGTH LIMIT

**0x99:** User attempts to write to the tag but does not provide the exact number of bytes specified in the Write Length field.

#### 4.1.2 RF Response Errors

##### TIMEOUT FAIL CODE

**0x9F:** Timeout Value has been exceeded. User needs to set a longer Timeout Value.

## CHAPTER 5: ETHERNET/IP PROTOCOL

The HS500E is designed to support many common Industrial Ethernet protocols and can be implemented in a wide variety of existing Host / PLC Industrial Ethernet applications. One such popular protocol that can be used to transfer data over Ethernet to and from the unit is **Ethernet/IP** (EIP).

This chapter focuses on the process of setting up and configuring the HS500E to communicate (via Ethernet/IP) with a ControlLogix Programmable Logic Controller (PLC). Also in this chapter you will find a description of EMS' HTML Server and *OnDemand* utility with step-by-step instructions to help you configure the HS500E for your Ethernet/IP environment.

**NOTE:**

This manual assumes that users are already familiar with communications protocols, industrial Ethernet principles and programmable logic controller technologies.

For specific information regarding the protocol used by your particular RFID application, please refer to the appropriate documentation from your Host software program provider.

**What is Ethernet/IP?**

Built on the standard TCP/IP protocol suite, EtherNet/IP is a high-level application layer protocol for industrial automation applications that uses traditional Ethernet hardware and software to define an application layer protocol that structures the task of configuring, accessing and controlling industrial automation devices.

Ethernet/IP classifies Ethernet nodes as predefined device types with specific behaviors. The set of device types and the EIP application layer protocol is based on the Common Industrial Protocol (CIP) layer used in both DeviceNet and ControlNet. Building on these two widely used protocol suites, Ethernet/IP provides a seamlessly integrated system from the RFID Subnet network to the Host and enterprise networks.

The HS500E is designed to communicate as an EtherNet/IP client device which will receive and execute RFID commands issued by the Host or PLC (acting as EtherNet/IP Server).

**ATTENTION:** for information regarding the Object Model implemented in the HS500E, see Appendix C.

## 5.1 STEPS TO CONFIGURE THE HS500E

See Chapter 2 for instructions on configuring the IP address of the HS500E.

Sections 5.2 through 5.4 in this chapter will help you accomplish the following:

- Configure the HS500E via *OnDemand Node Configuration*
- Create “Controller Tags” in the PLC
- Verify PLC and HS500E connectivity

### 5.1.1 HTML Server and OnDemand Overview

Embedded in the HS500E are an HTML Server and a set of configuration tools called the “*OnDemand Utilities*.” The HTML Server is used to modify and save IP address settings for the HS500E; *OnDemand* is used to configure and link the HS500E to specific **Controller Tags** as defined in the ControlLogix PLC. Both are accessed through a standard Web browser.

OnDemand is Escort Memory Systems’ approach to adding *Change of State* messaging to Rockwell Automation’s (RA) ControlLogix PLC and adding legacy support for the RA PLC5E and RA SCL5/05 PLCs.

#### NOTE:

The ControlLogix PLC refers to a “**controller tag**” as a small block of internal memory that is used to temporarily store outgoing (command) and incoming (response) data. Within each tag, information is stored in two-byte segments, known as registers or “words.”

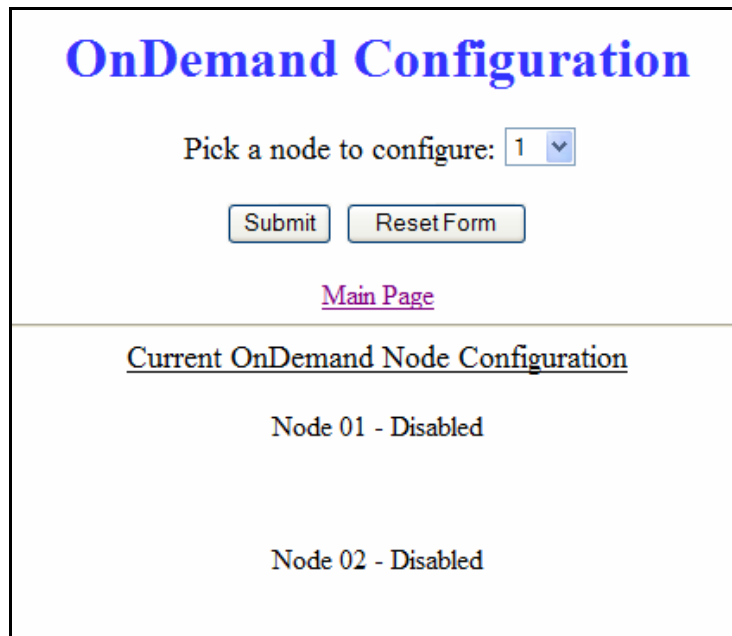
## 5.2 HS500E NODE CONFIGURATION

After you have configured the HS500E’s IP address, you must configure Node 01 on the HS500E.

- 1 Open a Web browser and enter the HS500E’s **new IP address** in the URL field. The *HTML Server – Main Page* will be displayed.
- 2 At the *HTML Server – Main Page* click the link labeled: **OnDemand Configuration**. The *OnDemand Configuration Page* will be displayed.

### 5.2.1 OnDemand Configuration Page

*OnDemand Configuration* is used to link the HS500E to controller tags defined in the ControlLogix PLC. The *OnDemand Configuration Page* allows the user to modify the settings of the HS500E’s Node.



**OnDemand Configuration**

Pick a node to configure: 1 ▼

[Main Page](#)

---

Current OnDemand Node Configuration

Node 01 - Disabled

Node 02 - Disabled

*The OnDemand Configuration Page*

- 3 At the HS500E's *OnDemand Configuration Page*, **select** Node 01 from the drop-down list (Node 01 is selected in the image above).
- 4 **Click** Submit. The *OnDemand Node 01 Configuration Page* will be displayed.

### 5.2.2 OnDemand Node 01 Configuration Page

OnDemand Node 01 Configuration	
Controller Type:	ControlLogix
Controller IP Address:	192.168.253.116
Controller Slot Number:	0 (ControlLogix)
Max Write Size:	100 words (0 to disable; 1-100 valid)
Write Tag Name (ControlLogix):	EMS_WRITE1 (upto 40 characters)
Write File Address (PLC,SLC,MicroLogic):	N0:0 (example: N7:0)
Write Heartbeat Timeout:	10 ticks (1 tick = 10ms; Range 5-6000 ticks)
Max Read Size:	100 words (0 to disable; 1-100 valid)
Read Tag Name (ControlLogix):	EMS_READ1 (upto 40 characters)
Read File Address (PLC,SLC,MicroLogic):	N0:0 (example: N14:0)
Read Poll Rate:	10 ticks (1 tick = 10ms; Range 5-6000 ticks)
<input type="button" value="Save Settings"/> <input type="button" value="Cancel Changes"/>	
<a href="#">Main Page</a>	

*The OnDemand Node 01 Configuration Page*

Use this page to modify the settings for Node 01.

#### Controller Settings

- 5 **Select** the **Controller Type** from the drop-down menu. The Controller Type (in this case) specifies the type of PLC that will be communicating with the HS500E.
- 6 **Enter** the **Controller's IP address**. Controller IP address is the IP address assigned to the PLC.
- 7 **Enter** the **Controller's Slot Number (0-255)**. Controller Slot Number indicates where in the PLC rack the controller module is installed; normally slot 0 for ControlLogix.

#### Write Settings

- 8 **Specify** the number of words (between 1 and 100, 0 = disabled) for the **Max Write Size**. The Max Write Size value represents the maximum number of 2-byte "words" that the HS500E will attempt to write to PLC memory during each command-response cycle. *Note: the actual data size required on the PLC is 3 words larger than the value specified in this field.*

9 Write Tag Name / Write File Address:

- a. **For ControlLogix:** Specify a **Write Tag Name** that is 40 characters or less. The Write Tag Name refers to the name of the *Controller Tag* in the PLC where the HS500E will write PLC-bound data for Node 01 (example: EMS\_WRITE1). Note: this is not to be confused with writing to an RFID transponder, which is often referred to as “writing to a tag.”

OR

- b. **For SLC505:** Enter a value in each of the two **Write File Address** fields. The first field contains the number of the (write) **Status File** on the PLC (for example: N7). The second field contains the **Write File Offset**. Together these values indicate the location in the PLC’s Status File where the HS500E will write Host-bound data.

10 Enter a number between 5 and 6000 to indicate the number of ticks for the **Write Heartbeat Timeout** (5 ticks = 50ms, 6000 ticks = 1 minute, 0 ticks = disabled). This value represents the frequency at which the HS500E will write data to the Write Tag (or the Write File Address) in the PLC when there is Host-bound data waiting.

### Read Settings

11 Specify the number of words (between 1 and 100, 0 = disabled) for the **Max Read Size**. The Max Read Size value represents the maximum number of 2-byte “words” that the HS500E will attempt to retrieve from PLC memory during a single command-response cycle. *Note: the actual data size required on the PLC is 3 words larger than the value specified in this field.*

12 Read Tag Name / Read File Address:

- a. **For ControlLogix:** Specify a **Read Tag Name** that is 40 characters or less. The Read Tag Name refers to the name of the tag in PLC memory from which the HS500E will retrieve data.

OR

- b. **For SLC505:** Enter a value in each of the two **Read File Address** fields. The first field contains the number of the (read) **Status File** on the PLC (for example: N7). The second field contains the **Read File Offset**. Together these values indicate the location in the PLC status file from which the HS500E will retrieve data.

13 Enter a value between 5 and 6000 to indicate the number of ticks for the **Read Poll Rate**. (5 ticks = 50ms, 6000 ticks = 1 minute, 0 ticks = disabled) This value represents the frequency at which the HS500E will poll the Read Tag (or the Read File Address) in PLC memory. Polling is the act of repeatedly querying a specific memory location for the presence of new data.

14 After you have entered the proper information on this page, click the **Save Settings** button. Your changes will be stored and you will be returned to the *OnDemand Configuration Page*.

### 5.2.3 OnDemand Configuration Page (Summary)

The screenshot displays a web interface titled "OnDemand Configuration". At the top, it prompts the user to "Pick a node to configure:" with a dropdown menu currently set to "1". Below this are two buttons: "Submit" and "Reset Form". A link labeled "Main Page" is positioned below the buttons. A horizontal line separates the top section from the "Current OnDemand Node Configuration" section. This section lists three nodes: "Node 01 - ControlLogix at 192.168.253.116, slot 0" with its specific write and read cycle settings, and "Node 02 - Disabled" and "Node 03 - Disabled". The configuration details for Node 01 are enclosed in a red rectangular box.

**OnDemand Configuration**

Pick a node to configure: 1 ▼

[Main Page](#)

---

Current OnDemand Node Configuration

Node 01 - ControlLogix at 192.168.253.116, slot 0  
Write 100 words to "EMS\_WRITE1" every 100 ms.  
Read 100 words from "EMS\_READ1" every 100 ms.

Node 02 - Disabled

Node 03 - Disabled

*OnDemand Configuration Page*

When you return to the *OnDemand Configuration Page*, you will notice a brief summary (similar to the image above) that displays the current details of the Node configuration settings for the HS500E.



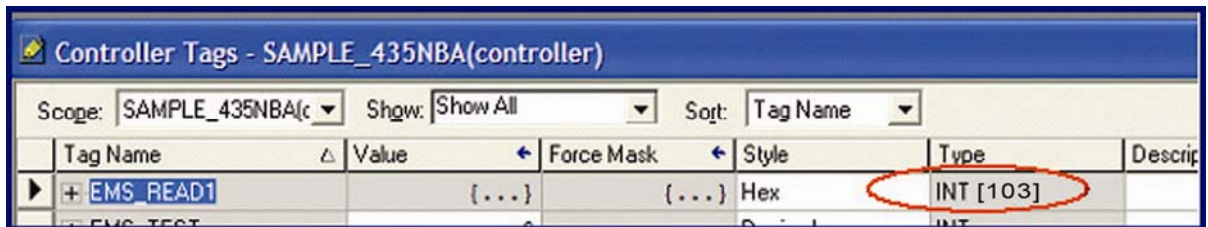
## 5.3 CONFIGURING PLC CONTROLLER TAGS

After you have configured Node 01 via *OnDemand Node Configuration*, open your PLC control software (RSLogix 5000 for ControlLogix) and define two **Controller Tags** (a **Write Tag** and a **Read Tag**).

Be sure to use the same **Write Tag Name** and **Read Tag Name** specified in the *OnDemand Node Configuration* (i.e., EMS\_WRITE1 and EMS\_READ1).

These tags must also have the capacity to store an integer array equal to your previously specified **Max Write/Read Size** + 3 words.

So for example, if the *Max Read Size* you specified earlier was 100 words, the corresponding Read Tag in the PLC must be able to store an array of 103 integers.



### 5.3.1 Controller Tags Summary

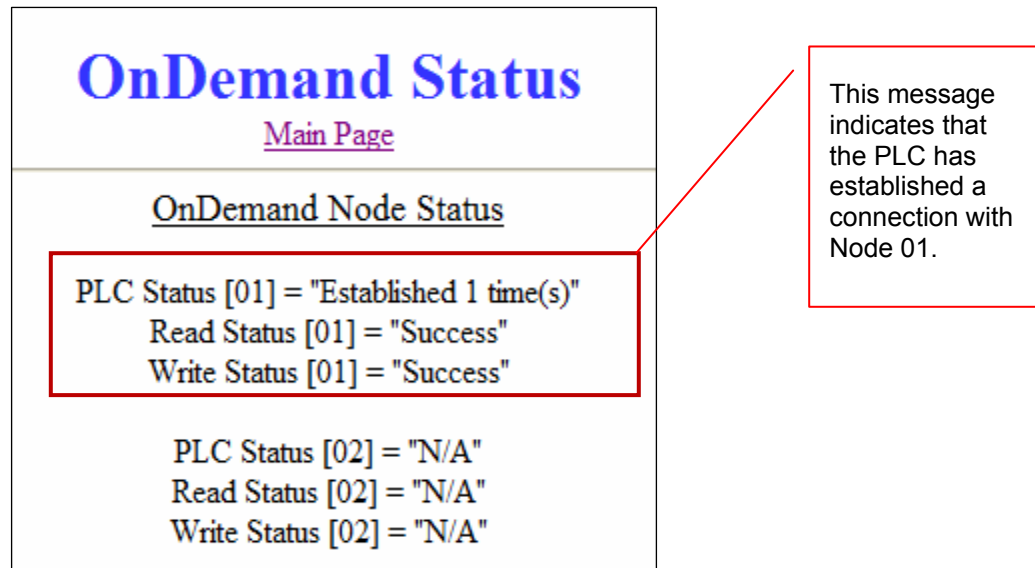
- **Write Tag** holds PLC-bound response data written by the HS500E after executing a command.
- **Read Tag** holds HS500E-bound RFID commands and other instructions written by the Host.

After creating and defining Write and Read Tags for the HS500E, return to the PC and the HS500E's *HTML Server – Main Page* to continue.

## 5.4 CHECKING ONDEMAND STATUS

Now that you have configured Node 01 for the HS500E and defined corresponding Write and Read Tags in the PLC, the last step is to check the communication status between the HS500E and the PLC.

- On the HS500E's *HTML Server - Main Page*, click the link labeled: "**OnDemand Status**." The *OnDemand Status Page* will be displayed.



*The OnDemand Status Page*

The *OnDemand Status Page* provides information regarding the connection status between the PLC and each configured Node (Node 01 in this case). This information can be used to verify that read and write connections between the Node and the PLC have been established successfully.

**ATTENTION:**

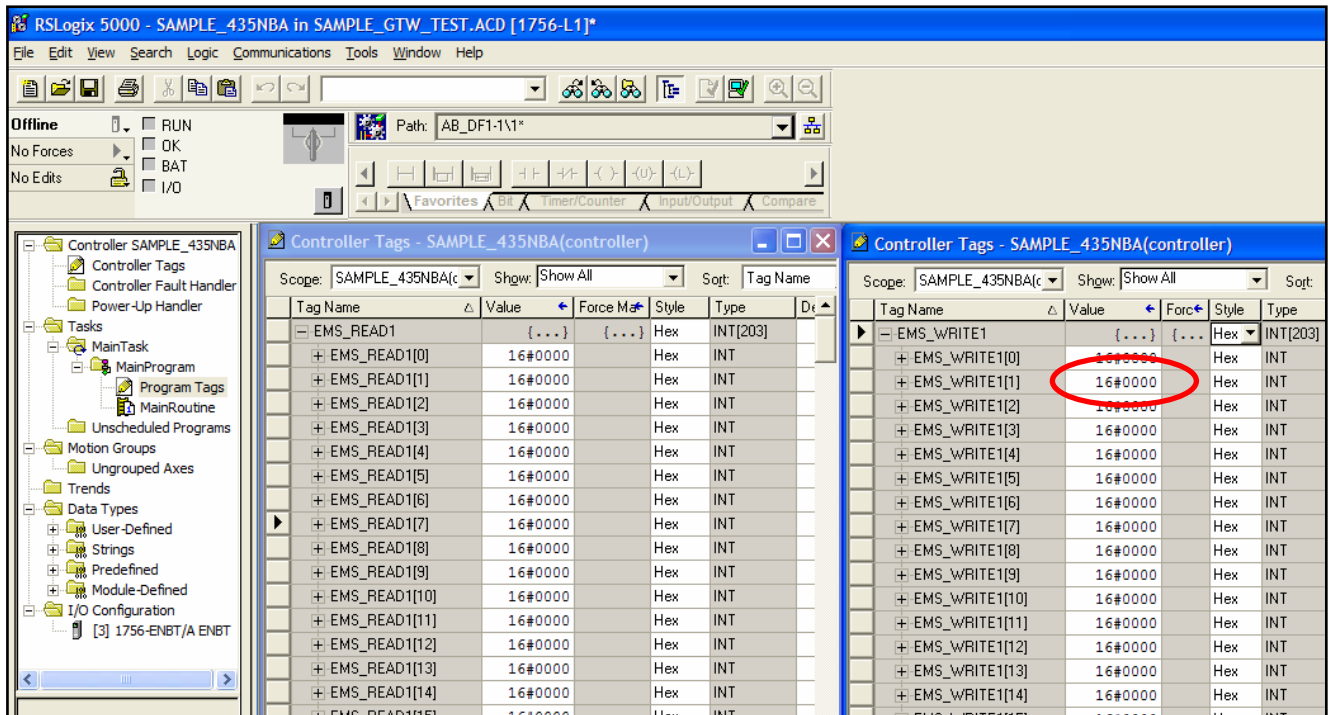
If the PLC and HS500E do not establish a successful connection, as depicted in the image above, Ethernet/IP services on the HS500E, PLC and/or the PLC's 1756-ENBT module might not be running. Cycle power to the HS500E and verify that Ethernet/IP services are indeed running on the PLC and the 1756-ENBT module.

## 5.5 USING THE HS500E WITH RSLOGIX 5000

At this point, communication between the PLC and the HS500E should be properly configured and a connection established. You can verify the exchange of information between devices using RSLogix 5000.

Note that under the Ethernet/IP protocol, the HS500E acts as the client and the PLC acts as the Ethernet/IP server.

Based on the **Write Heartbeat Timeout** and **Read Poll Rate** values specified in the *OnDemand Node Configuration* section, the HS500E will periodically read from and write to the specified portions of PLC memory directly with no messaging instructions or polling required on the part of the PLC.



A screen shot of RSLogix 5000

### 5.5.1 Ethernet/IP Handshaking

To ensure that messages to and from the HS500E are properly delivered and received, a handshaking mechanism has been implemented that uses a pair of dedicated words in the exchange. The first two words in each Controller Tag are dedicated to handshaking.

When new information is generated, the producing device (data producer) increments a counter, and the consuming device (data consumer) copies that same counter value to another memory location to signal that the information has been processed.

### 5.5.2 Ethernet/IP Handshaking Example

In the example below, EMS\_READ1 is the Read Tag for Node 1 and EMS\_WRITE1 is the Write Tag for Node 1.

NOTE: **[0]** indicates the first word, **[1]** indicates the second word in a Controller Tag.

- 1 The PLC writes a command to the Output area (of the Read Tag) and then increments the counter in EMS\_READ1 [1].
- 2 The counter in EMS\_READ1 [1] is copied by the HS500E to EMS\_WRITE1 [0] which acknowledges that it received the command.

Tag Name	Value	Force Mask	Style	Type
EMS_READ1	{...}	{...}	Hex	INT[2]
EMS_READ1[0]	16#0005		Hex	INT
EMS_READ1[1]	16#0004		Hex	INT
EMS_READ1[2]	16#0006		Hex	INT
EMS_READ1[3]	16#aa07		Hex	INT
EMS_READ1[4]	16#0001		Hex	INT
EMS_READ1[5]	16#07d0		Hex	INT
EMS_READ1[6]	16#0000		Hex	INT
EMS_READ1[7]	16#0000		Hex	INT
EMS_READ1[8]	16#0000		Hex	INT

Tag Name	Value	Force Mask	Style	Type
EMS_WRITE1	{...}	{...}	Hex	
EMS_WRITE1[0]	16#0004		Hex	
EMS_WRITE1[1]	16#0005		Hex	
EMS_WRITE1[2]	16#0000		Hex	
EMS_WRITE1[3]	16#0000		Hex	
EMS_WRITE1[4]	16#0000		Hex	
EMS_WRITE1[5]	16#0000		Hex	
EMS_WRITE1[6]	16#0000		Hex	
EMS_WRITE1[7]	16#0000		Hex	
EMS_WRITE1[8]	16#0000		Hex	
EMS_WRITE1[9]	16#0000		Hex	

- 3 After executing the command, the HS500E writes the response in the Write Tag and then increments the counter in EMS\_WRITE1 [1]. This signals that there is new information for the PLC (the HS500E generated response).

Tag Name	Value	Force Mask	Style	Type
EMS_READ1	{...}	{...}	Hex	INT[2]
EMS_READ1[0]	16#0005		Hex	INT
EMS_READ1[1]	16#0005		Hex	INT
EMS_READ1[2]	16#0006		Hex	INT
EMS_READ1[3]	16#aa07		Hex	INT
EMS_READ1[4]	16#0001		Hex	INT
EMS_READ1[5]	16#07d0		Hex	INT
EMS_READ1[6]	16#0000		Hex	INT
EMS_READ1[7]	16#0000		Hex	INT
EMS_READ1[8]	16#0000		Hex	INT
EMS_READ1[9]	16#0000		Hex	INT
EMS_READ1[10]	16#0000		Hex	INT
EMS_READ1[11]	16#0000		Hex	INT
EMS_READ1[12]	16#0000		Hex	INT
EMS_READ1[13]	16#0000		Hex	INT

Tag Name	Value	Force Mask	Style	Type
EMS_WRITE1	{...}	{...}	Hex	
EMS_WRITE1[0]	16#0005		Hex	
EMS_WRITE1[1]	16#0006		Hex	
EMS_WRITE1[2]	16#000a		Hex	
EMS_WRITE1[3]	16#aa07		Hex	
EMS_WRITE1[4]	16#0601		Hex	
EMS_WRITE1[5]	16#0204		Hex	
EMS_WRITE1[6]	16#0009		Hex	
EMS_WRITE1[7]	16#3408		Hex	
EMS_WRITE1[8]	16#e004		Hex	
EMS_WRITE1[9]	16#0100		Hex	
EMS_WRITE1[10]	16#000f		Hex	
EMS_WRITE1[11]	16#f0f0		Hex	
EMS_WRITE1[12]	16#0000		Hex	
EMS_WRITE1[13]	16#0000		Hex	

- 4 After the PLC has processed the response information, it copies the counter from EMS\_WRITE1 [1] to EMS\_READ1 [0] which signals (to the HS500E) that the PLC has read the response data.

Tag Name	Value	Force Mask	Style	Type
EMS_READ1	{...}	{...}	Hex	INT[2]
EMS_READ1[0]	16#0006		Hex	INT
EMS_READ1[1]	16#0005		Hex	INT
EMS_READ1[2]	16#0006		Hex	INT
EMS_READ1[3]	16#aa07		Hex	INT
EMS_READ1[4]	16#0001		Hex	INT
EMS_READ1[5]	16#07d0		Hex	INT
EMS_READ1[6]	16#0000		Hex	INT
EMS_READ1[7]	16#0000		Hex	INT
EMS_READ1[8]	16#0000		Hex	INT
EMS_READ1[9]	16#0000		Hex	INT
EMS_READ1[10]	16#0000		Hex	INT
EMS_READ1[11]	16#0000		Hex	INT
EMS_READ1[12]	16#0000		Hex	INT

Tag Name	Value	Force Mask	Style	Type
EMS_WRITE1	{...}	{...}	Hex	
EMS_WRITE1[0]	16#0005		Hex	
EMS_WRITE1[1]	16#0006		Hex	
EMS_WRITE1[2]	16#000a		Hex	
EMS_WRITE1[3]	16#0000		Hex	
EMS_WRITE1[4]	16#0000		Hex	
EMS_WRITE1[5]	16#0000		Hex	
EMS_WRITE1[6]	16#0000		Hex	
EMS_WRITE1[7]	16#0000		Hex	
EMS_WRITE1[8]	16#0000		Hex	
EMS_WRITE1[9]	16#0000		Hex	
EMS_WRITE1[10]	16#0000		Hex	
EMS_WRITE1[11]	16#0000		Hex	
EMS_WRITE1[12]	16#0000		Hex	

- 5 The HS500E will then clear the Write Tag by copying 0's to memory. After which it will be ready to receive another command.

**Write Tag (where responses are written by the HS500E)**

EMS\_Write1 [0] = (2) the counter is copied here by the HS500E to ACK

EMS\_Write1 [1] = (3) the HS500E increments this counter to signal a response is available

EMS\_Write1 [2] = Data Size

EMS\_Write1 [3-102] = Data

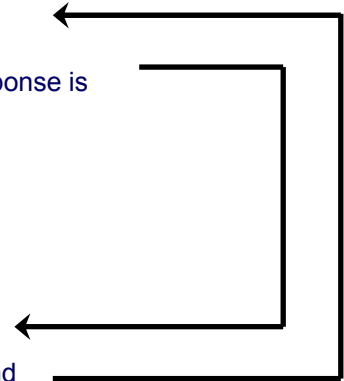
**Read Tag (where commands are retrieved by the HS500E)**

EMS\_Read1 [0] = (4) PLC copies the counter here to ACK the response

EMS\_Read1 [1] = (1) PLC increments this counter after writing a command

EMS\_Read1 [2] = Data Size

EMS\_Read1 [3-102] = Data



## 5.6 HTML SERVER AND ONDEMAND PLC SUPPORT

Below is a partial list of the programmable logic controllers that are supported by EMS' *HTML Server* and *OnDemand Utility*.

- ControlLogix – OnDemand supports all current versions
- RA's PLC5E releases:
  - Series C, Revision N.1
  - Series D, Revision E.1
  - Series E, Revision D.1
- PLC5 "Sidecar" Module Series B, Revision A with EIP support
- SLC5/05 releases:
  - Series A with firmware revision OS501, FRN5
  - All Series B and Series C PLC Controllers



# CHAPTER 6: MODBUS TCP PROTOCOL

One of the most popular and well-proven industrial automation protocols in use today is Modbus. Modbus TCP allows the Modbus protocol to be carried over standard Ethernet networks.

## 6.1 MODBUS TCP OVERVIEW

Under the Modbus TCP protocol, the HS500E acts as a Modbus Server and the Host or PLC is the Modbus Client. By utilizing **Produce** and **Consume** registers for mapping commands and responses, data produced by the HS500E is consumed by the Modbus Client and data produced by the Modbus Client is consumed by the HS500E.

**NOTE:**

The Modbus Client (Host or PLC) must connect to the Modbus Server (HS500E) on port **502**.

Maximum number of words transferred to/from an RFID tag per read/write cycle:  
**100 Words / 200 Bytes**

### 6.1.1 Modbus TCP Command Structure

**MAPPING NODE 01 (CONSUME REGISTERS)**

**Consume Registers** hold data destined for the HS500E. Modbus TCP commands must be placed in the holding registers of Device ID 1 (i.e. Node 01), starting at address 40001. Commands utilize at least six registers (double-byte values or words).

Modbus Address (4xxx / 3xxx)	Read / Write Privilege	Register Description
(4000) 1	R/W	2-byte HS500E Consume Data Overall Length (> 0 indicates that data is available; HS500E clears to 0 after data is processed)
2	R/W	MSB = Reader Type LSB = Command ID
3	R/W	MSB = 0x00 LSB = Node ID (0x01)



<b>4</b>	R/W	2-byte Timeout Value (0-65535) measured in milliseconds
<b>5</b>	R/W	2-byte Read/Write Start Address (0-65535)
<b>6</b>	R/W	2-byte Read/Write Data Length (0-65535)
<b>7 – 32774</b>	R/W	HS500E Consume Data (when applicable)
<b>32775 – 65536</b>	R/W	Reserved

*Modbus TCP Command Structure  
Node 01 Memory Map (Consume Registers)*

### 6.1.2 Modbus TCP Response Structure

#### MAPPING NODE 33 (PRODUCE REGISTERS)

*Produce Registers* hold data that is destined for the Host.

ModBus Address (4xxxx / 3xxxx)	Read / Write Privilege	Register Description
(40001) 1	R/W	HS500E Produce Data Overall Length (> 0 indicates that data is available; Modbus Client clears to 0 after data is processed)
2	RO	MSB = Reader Type; LSB = Command ID
3	RO	Node ID (33)
4	RO	Timeout Value (0-65535)
5	RO	Read/Write Start Address (0-65535)
6	RO	Read/Write Data Length (0-65535 bytes)
7 – 32774	RO	HS500E Produce Data (when applicable)
32775 – 65536	RO	Reserved

*Modbus TCP Response Structure  
Node 33 Memory Map (Produce Registers)*

## 6.2 MODBUS TCP HANDSHAKING

Modbus TCP handshaking is governed by the changing of the “**Overall Length**” value within a data packet. The Overall Length value is typically the first 2-bytes of a command or response and indicates the total number of data words in the packet (including one word for the Overall Length value).

Overall Length values are stored in the first holding register, *40001*, of **Device ID 1** (for commands) and **Device ID 33** (for responses). When the value at register 40001 (of Device ID 1) changes from **00**, the HS500E will recognize that a command is waiting to be executed. The HS500E will then execute the command and return a response at Device ID 33.

### 6.2.1 Host/HS500E Modbus TCP Handshaking

One implication of this process is that when the Host issues a command, it must first write the entire command to the holding registers for Device ID 1, leaving the Overall Length value to be written last.

For example, for the Host to issue the 6-word command “*Read Data*,” it must first write the last 5 words of the command to Device ID 1, beginning at register **40002**.

#### LAST 5 WORDS OF A READ DATA COMMAND

Word	MSB	LSB	Description
<b>02</b>	AA	02	Command ID: Read Data
<b>03</b>	00	01	Node ID
<b>04</b>	03	E8	Timeout Value of 1 second (measured in ms)
<b>05</b>	00	20	Read Start Address: 0x20
<b>06</b>	00	04	Read 4 Bytes

After writing the last 5 words of the command, the Host will write the Overall Length value to register 40001 of Device ID 1.

#### FIRST WORD OF A READ DATA COMMAND

Word	MSB	LSB	Description
<b>01</b>	00	06	Overall Length (in words)

The moment the Overall Length value at register 40001 of Device ID 1 changes to a “non-zero” value, the HS500E will recognize the waiting data and will execute the command.

### 6.2.2 Modbus TCP Command, Response & Handshaking Example

- 1 The Host issues an RFID command to the HS500E, writing the command string to the holding registers for Device ID 1. An Overall Length value of 0x06 is written last to holding register 40001.
- 2 The HS500E recognizes that the Overall Length value at holding register 40001 for Device ID 1 has changed, indicating that it has data waiting to be retrieved.
- 3 The HS500E retrieves the data and clears the Overall Length holding register of Device ID 1 - setting it back to its default value of zero (0x00).

Note: when the value stored at register 40001 of Device ID 1 returns to 0x00, the Host can assume that the command was at least received and execution was attempted. The Host will also assume that it is now OK to write another command to the holding registers of Device ID 1.

- 4 The HS500E, now having retrieved the pending data from the holding registers for Device ID 1, executes the command accordingly.
- 5 As the HS500E finishes executing the given command, it generates a Host-bound command response. Response data is written to the holding registers for Device ID 33, the Overall Length value is, again, written last to holding register 40001.

Note: Host-bound data is always written to Device ID 33 by the HS500E.

- 6 Because the holding register at 40001 (Overall Length value) of Device ID 33 now contains a non-zero length value, the Host recognizes that there is response data from the HS500E waiting to be retrieved.
- 7 The Host imports the pending data from the holding registers of Device ID 33 and then clears (sets back to 0x00) the Overall Length value at register 40001.

Note: the clearing of register 40001 of Device ID 33 indicates to the HS500E that the Host has indeed received the command response and that it is now OK to write another response to the holding registers of Device ID 33.

This completes the Modbus TCP handshaking cycle.



## CHAPTER 7: RAW TCP/IP PROTOCOL

---

### 7.1 RAW TCP/IP OVERVIEW

Another means of communicating with the HS500E is through the standard TCP/IP protocol. For this manual, the protocol is referred to as **RAW TCP/IP** to distinguish it from the other industrial protocols.

In the RAW TCP/IP environment, the HS500E acts as the server and the Host or PLC acts as client.

**NOTE:**

The RAW TCP/IP Client (Host or PLC) must connect to the RAW TCP/IP Server (HS500E) on port **50200**.

Maximum number of words transferred to/from an RFID tag per read/write cycle:  
**100 Words / 200 Bytes**

RAW TCP/IP sessions are established between the Host and the HS500E via TCP/IP client software and generally consist of three stages: *connection setup*, *data transactions* and *connection termination*.

All connections to the HS500E are initiated by client side software only. If, for example, an existing connection terminates unexpectedly, the HS500E will not attempt to contact the client software or re-establish a connection. The client is responsible for opening, maintaining, and closing all TCP/IP sessions.

After establishing a successful connection, communications between the client software and the HS500E can proceed. When communication is no longer necessary, it is the responsibility of the client side application to terminate the connection.



## 7.2 RAW TCP/IP COMMAND & RESPONSE EXAMPLES

In RAW TCP/IP, RFID commands issued by the Host resemble Modbus TCP commands; however RAW TCP/IP commands require an additional **two-byte** header (which includes **0xFF** in the MSB, and **0x01** - the Node ID of the HS500E - in the LSB). These two bytes are inserted in front of the standard Modbus TCP command string. RAW TCP/IP response packets also contain the same additional two-byte header; **0xFF** in the MSB and the **0x01** in the LSB. The HS500E handles all handshaking tasks.

### 7.2.1 RAW TCP/IP Command Example

In the following example, a 14-byte command has been issued to the HS500E (Node 01), instructing it to read 6 bytes from a tag within RF range starting at tag address 0x0001. A Timeout Value of two seconds has been set for the completion of the command.

Word	MSB	LSB	Description
01	FF	01	"Raw TCP/IP" 2-byte <b>Command Header</b> - 0xFF and Node 01
02	00	06	2-byte value indicating <b>Overall Length</b> measured in number of "words," not including the preceding 2-byte header
03	AA	05	MSB = AA LSB = <b>Command ID</b> : 02 - <i>Read Data Command</i>
04	00	01	MSB = 00 LSB = <b>Node ID</b> : 01 (Must be same as specified in header)
05	00	32	2-byte <b>Timeout Value</b> measured in .10 second increments (0x0032 = 50 x .10 or 5 seconds)
06	00	01	2-byte <b>Start Address</b> for the Read: 0x0001
07	00	06	2-byte <b>Read Length</b> : 6 bytes



### 7.2.2 RAW TCP/IP Response Example

The following is the response to the *Read Data* command issued in the previous example:

Word	MSB	LSB	Description
01	FF	01	“Raw TCP/IP” 2-byte <b>Response Header</b> : MSB = 0xFF LSB = Node ID Echo (0x01 for the HS500E)
02	00	09	<b>Overall Length</b> of response packet (not including the 2-byte header)
03	AA	02	MSB = AA LSB = <b>Command Echo</b> : <i>Read Data</i>
04	ICV	01	MSB = <b>Instance Counter Value</b> LSB = <b>Node ID Echo</b>
05	05	1b	<b>Time Stamp</b> (Month – Day)
06	01	0C	<b>Time Stamp</b> (Hour – Minute)
07	21	06	MSB = <b>Time Stamp</b> (Seconds) LSB = <b>Number of Additional Data Bytes Returned</b>
08	61	62	<b>Returned Data</b> Bytes 1 & 2
09	63	64	<b>Returned Data</b> Bytes 3 & 4
0A	65	66	<b>Returned Data</b> Bytes 5 & 6



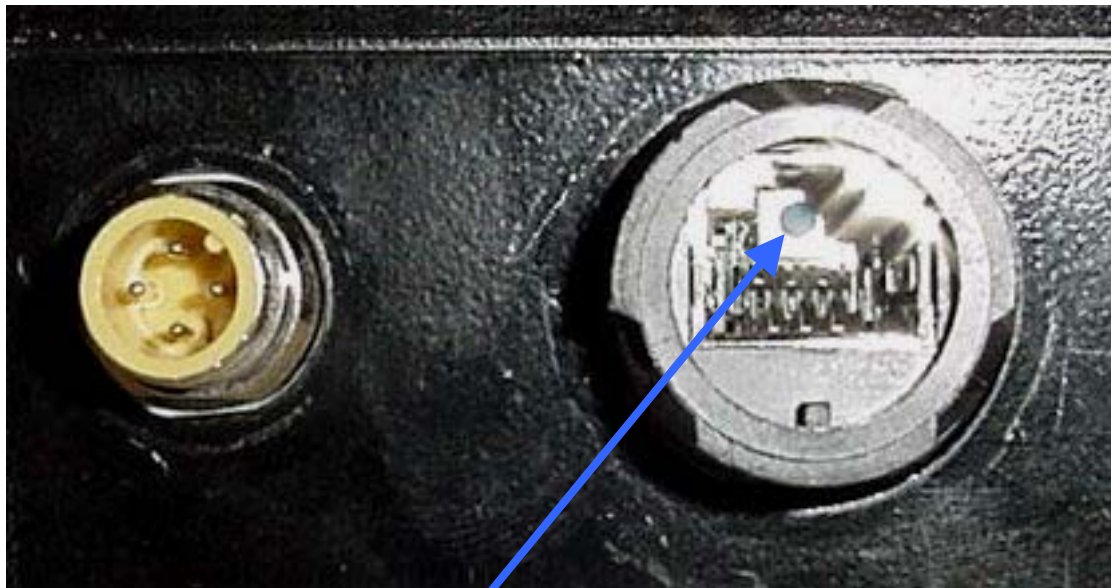
## APPENDIX A: IP ADDRESS RESET

To reset the IP address of the HS500E to factory default values, follow the steps below:

1. Disconnect the power supply and remove the Ethernet cable.
2. With a blunt toothpick (or similar non-metallic object), gently press and hold the small blue-colored button located within the RJ45 Ethernet connection socket. This is the HS500E's *IP Address Reset Button*.
3. While continuing to press the reset button, re-connect power to the unit.
4. Wait for the RED "Error" LED to flash twice, after which release the reset button and insert the Ethernet cable.

The LEDs will flash several more times while the unit automatically reboots.

***HS500E Factory Default IP Address: 192.168.0.100***




**IP Address Reset  
Button**





## APPENDIX B: ASCII CHART

 <b>ASCII Chart</b>		
Decimal	Hex	Character
000	00	NUL
001	01	SOH
002	02	STX
003	03	ETX
004	04	EOT
005	05	ENQ
006	06	ACK
007	07	BEL
008	08	BS
009	09	HT
010	0A	LF
011	0B	VT
012	0C	FF
013	0D	CR
014	0E	SO
015	0F	SI
016	10	DLE
017	11	DC1
018	12	DC2
019	13	DC3
020	14	DC4
021	15	NAK
022	16	SYN
023	17	ETB
024	18	CAN
025	19	EM
026	1A	SUB
027	1B	ESC
028	1C	FS
029	1D	GS
030	1E	RS
031	1F	US
032	20	(SPACE)
033	21	!
034	22	"
035	23	#
036	24	\$
037	25	%
038	26	&
039	27	'
040	28	(
041	29	)
042	2A	*
043	2B	+
044	2C	,
045	2D	-
046	2E	.
047	2F	/
048	30	0
049	31	1
050	32	2
051	33	3
052	34	4
053	35	5
054	36	6
055	37	7
056	38	8
057	39	9
058	3A	:
059	3B	;
060	3C	<
061	3D	=



Decimal	Hex	Character	Decimal	Hex	Character
062	3E	>	095	5F	_
063	3F	?	096	60	'
064	40	@	097	61	a
065	41	A	098	62	b
066	42	B	099	63	c
067	43	C	100	64	d
068	44	D	101	65	e
069	45	E	102	66	f
070	46	F	103	67	g
071	47	G	104	68	h
072	48	H	105	69	i
073	49	I	106	6A	j
074	4A	J	107	6B	k
075	4B	K	108	6C	l
076	4C	L	109	6D	m
077	4D	M	110	6E	n
078	4E	N	111	6F	o
079	4F	O	112	70	p
080	50	P	113	71	q
081	51	Q	114	72	r
082	52	R	115	73	s
083	53	S	116	74	t
084	54	T	117	75	u
085	55	U	118	76	v
086	56	V	119	77	w
087	57	W	120	78	x
088	58	X	121	79	y
089	59	Y	122	7A	z
090	5A	Z	123	7B	{
091	5B	[	124	7C	
092	5C	\	125	7D	}
093	5D	]	126	7E	~
094	5E	^	127	7F	DEL



## APPENDIX C: ETHERNET/IP - OBJECT MODEL

The **Object Model** is the logical organization of attributes (parameters) within classes (objects) and services supported by each device.

Objects are broken down into three categories: **Required Objects**, **Vendor Specific Objects** and **Application Objects**.

- **Required Objects** are classes that must be supported by all devices on EtherNet/IP. The HS500E has six Required Objects.
- **Vendor Specific Objects** are classes which add attributes and services that don't fit into the Required Objects or Application Objects categories. The HS500E has two Vendor Specific Objects.
- **Application Objects** are classes that must be supported by all devices using the same profile. An example of a profile is a Discrete I/O device or an AC Drive. This ensures that all devices with the same profile have a common look on the network.

### Data Type Definitions

EtherNet/IP was designed by the *Open Device Vendors Association (ODVA)* as an open protocol. The following table contains a description of the data types used by ODVA that are also found in this appendix.

<u>Data Type</u>	<u>Description</u>
USINT	Unsigned Short Integer (8-bit)
UINT	Unsigned Integer (16-bit)
UDINT	Unsigned Double Integer (32-bit)
STRING	Character String (1 byte per character)
BYTE	Bit String (8-bits)
WORD	Bit String (16-bits)
DWORD	Bit String (32-bits)



## C.1 ETHERNET/IP - REQUIRED OBJECTS

Under Ethernet/IP, the HS500E has six *Required Objects*:

### Required Objects:

- Identity Object (0x01)
- Message Router Object (0x02)
- Assembly Object (0x04)
- Connection Manager Object (0x06)
- TCP Object (0xF5)
- Ethernet Link Object (0xF6)

### C.1.1 Identity Object (0x01- 1 Instance)

#### Class Attributes

Attribute ID	Name	Data Type	Data Value	Access Rule
1	Revision	UINT	1	Get

#### Instance Attributes

Attribute ID	Name	Data Type	Data Value	Access Rule
1	Vendor Number	UINT	50 <sub>DEC</sub>	Get
2	Device Type	UINT	0C <sub>HEX</sub>	Get
3	Product Code Number	UINT	6102 <sub>DEC</sub>	Get
4	Product Major Revision Product Minor Revision	USINT USINT	01 25	Get
5	Status Word (see below for definition)	WORD	See Below	Get
6	Serial Number	UDINT	Unique 32 Bit Value	Get



7	Product Name <u>Structure of:</u> Product Name Size Product Name String	USINT USINT[26]	11 "HS500E"	Get
---	--	--------------------	----------------	-----

### Status Word

Bit	Bit = 0	Bit = 1
0	No I/O Connection	I/O Connection Allocated
1 – 15	Unused	Unused

### Common Services

Service Code	Implemented for		Service Name
	Class Level	Instance Level	
0E <sub>HEX</sub>	Yes	Yes	Get_Attribute_Single
05 <sub>HEX</sub>	No	Yes	Reset



### C.1.2 Message Router Object (0x02)

This object has no supported attributes.

### C.1.3 Assembly Object (0x04 – 3 Instances)

#### Class Attributes

Attribute ID	Name	Data Type	Data Value	Access Rule
1	Revision	UINT	1	Get
2	Max Instance	UINT	81	Get

#### Instance 0x64 Attributes (Input Instance)

Attribute ID	Name	Data Type	Default Data Value	Access Rule
3	Status Information <u>Structure of:</u> Bitmap of Consume Instances with Data Bitmap of Produce Instances with Data	 DINT DINT	 0 0	Get

#### UDP I/O Sequence Number Handshaking

Valid sequence numbers are 1-65535. The producing device increments the data sequence number by one on every new serial data packet. The device consuming the data must echo the sequence number in the handshake location once the data is processed to allow the producing Node to remove the data from the queue. This is needed for I/O communications since UDP isn't guaranteed to arrive in order.

If the Node ID number is passed as part of the I/O message, the message is stored to the appropriate location in the Modbus RTU table. Since communications are asynchronous, the Node ID number is also stored as part of the output data. It is the responsibility of the PLC programmer to make sure the proper request lines up with the proper response if the HS500E is used as a request/response device.

**Instance 0x65 Attributes (Input Instance 2)**

Attribute ID	Name	Data Type	Default Data Value	Access Rule
3	Serial Produce Data			Get
	<u>Structure of:</u>			
	Consume Data Seq. Number Handshake	UINT	0	
	Produce Data Sequence Number	UINT	0	
	Node 1 Serial Produce Data Size	UINT	0	
	Node 1 Serial Produce Data	WORD[100]	All 0's	

**Instance 0x66 Attributes (Input Instance 3)**

Attribute ID	Name	Data Type	Default Data Value	Access Rule
3	Serial Produce Data			Get
	<u>Structure of:</u>			
	Consume Data Seq. Number Handshake	UINT	0	
	Produce Data Sequence Number	UINT	0	
	Node ID (1)	UINT	1	
	Node Serial Produce Data Size	UINT	0	
	Node Serial Produce Data	WORD[100]	All 0's	



## Instance 0x70 Attributes (Output Instance 1)

Attribute ID	Name	Data Type	Default Data Value	Access Rule
3	Serial Consume Data			Get / Set
	<u>Structure of:</u>			
	Produce Data Seq. Number Handshake	UINT	0	
	Consume Data Sequence Number	UINT	0	
	Node 1 Serial Consume Data Size	UINT	0	
	Node 1 Serial Consume Data	WORD[100]	All 0's	



**Instance 0x71 Attributes (Output Instance 2)**

Attribute ID	Name	Data Type	Default Data Value	Access Rule
3	Serial Consume Data <u>Structure of:</u> Produce Data Seq. Number Handshake Consume Data Sequence Number Node ID (1-32) Node Serial Consume Data Size Node Serial Consume Data	UINT UINT UINT UINT WORD[100]	0 0 1 0 All 0's	Get / Set

**Instance 0x80 Attributes (Configuration Instance)**

Most I/O clients include a Configuration path when opening an I/O connection to a server. There is no Configuration data needed.

**Instance 0x81 Attributes (Heartbeat Instance – Input Only)**

This instance allows clients to monitor input data without providing output data.

**Common Services**

Service Code	Implemented for		Service Name
	Class Level	Instance Level	
0E <sub>HEX</sub>	Yes	Yes	Get_Attribute_Single
10 <sub>HEX</sub>	No	Yes	Set_Attribute_Single



### C.1.4 Connection Manager Object (0x06)

This object has no attributes.

### C.1.5 TCP Object (0xF5 - 1 Instance)

#### Class Attributes

Attribute ID	Name	Data Type	Data Value	Access Rule
1	Revision	UINT	1	Get

#### Instance Attributes

Attribute ID	Name	Data Type	Default Data Value	Access Rule
1	Status <sup>1</sup>	DWORD	1	Get
2	Configuration Capability <sup>2</sup>	DWORD	0	Get
3	Configuration Control <sup>3</sup>	DWORD	0	Get
4	Physical Link Object <sup>4</sup> <u>Structure of:</u> Path Size Path	UINT Array Of WORD	2 0x20F6 0x2401	Get

<sup>1</sup> See section 5-3.2.2.1 of "Volume 2: EtherNet/IP Adaptation of CIP" from ODVA for more details on this attribute.

<sup>2</sup> See section 5-3.2.2.2 of "Volume 2: EtherNet/IP Adaptation of CIP" from ODVA for more details on this attribute.

<sup>3</sup> See section 5-3.2.2.3 of "Volume 2: EtherNet/IP Adaptation of CIP" from ODVA for more details on this attribute.

<sup>4</sup> See section 5-3.2.2.4 of "Volume 2: EtherNet/IP Adaptation of CIP" from ODVA for more details on this attribute.



5	Interface Configuration <sup>5</sup> <u>Structure of:</u> IP Address Network Mask Gateway Address Name Server Name Server 2 Domain Name Size Domain Name	UDINT UDINT UDINT UDINT UDINT UINT STRING	0 0 0 0 0 0 0	Get
6	Host Name <sup>6</sup> <u>Structure of:</u> Host Name Size Host Name	UINT STRING	0 0	Get

**Common Services**

Service Code	Implemented for		Service Name
	Class Level	Instance Level	
0E <sub>HEX</sub>	Yes	Yes	Get_Attribute_Single

<sup>5</sup> See section 5-3.2.2.5 of “Volume 2: EtherNet/IP Adaptation of CIP” from ODVA for more details on this attribute.

<sup>6</sup> See section 5-3.2.2.6 of “Volume 2: EtherNet/IP Adaptation of CIP” from ODVA for more details on this attribute.



### C.1.6 Ethernet Link Object (0xF6 - 1 Instance)

#### Class Attributes

Attribute ID	Name	Data Type	Data Value	Access Rule
1	Revision	UINT	1	Get

#### Instance Attributes

Attribute ID	Name	Data Type	Default Data Value	Access Rule
1	Interface Speed <sup>7</sup>	UDINT	100	Get
2	Interface Flags <sup>8</sup>	DWORD	3	Get
3	Physical Address <sup>9</sup>	USINT Array[6]	0	Get

#### Common Services

Service Code	Implemented for		Service Name
	Class Level	Instance Level	
0E <sub>HEX</sub>	Yes	Yes	Get_Attribute_Single

<sup>7</sup> See section 5-4.2.2.1 of “Volume 2: EtherNet/IP Adaptation of CIP” from ODVA for more details on this attribute.

<sup>8</sup> See section 5-4.2.2.2 of “Volume 2: EtherNet/IP Adaptation of CIP” from ODVA for more details on this attribute.

<sup>9</sup> See section 5-4.2.2.3 of “Volume 2: EtherNet/IP Adaptation of CIP” from ODVA for more details on this attribute.



## C.2 VENDOR SPECIFIC OBJECTS

### C.21 HS500E Consume Data Object (0x64 - 32 Instances)

#### Class Attributes (Instance 0)

Attribute ID	Name	Data Type	Default Data Value	Access Rule
1	Revision	UINT	1	Get
2	Maximum Consume Data Buffer Size (in words)	UINT	32768	Get
3	Bitmap of Consume Instances with Data <i>Bit 0: Instance 1 ... Bit 31: Instance 32</i>	DINT	0	Get

#### Instance Attributes (Instances 1-32)

Attribute ID	Name	Data Type	Default Data Value	Access Rule
1	Consume Data Size (in words)	UINT	0	Get / Set
2	Consume Data [0-249]	UINT	0	Get / Set
3	Consume Data [250-499]	UINT	0	Get / Set
4	Consume Data [500-749]	UINT	0	Get / Set
5	Consume Data [750-999]	UINT	0	Get / Set
6	Consume Data [1,000-1,249]	UINT	0	Get / Set
...	...	...	...	...
10	Consume Data [2,000-2,249]	UINT	0	Get / Set



...	...	...	...	...
34	Consume Data [8,000-8,249]	UINT	0	Get / Set
...	...	...	...	...
38	Consume Data [9,000-9,249]	UINT	0	Get / Set
...	...	...	...	...
42	Consume Data [10,000-10,249]	UINT	0	Get / Set
...	...	...	...	...
82	Consume Data [20,000-20,249]	UINT	0	Get / Set
...	...	...	...	...
122	Consume Data [30,000-30,249]	UINT	0	Get / Set
...	...	...	...	...
126	Consume Data [31,000-31,249]	UINT	0	Get / Set
...	...	...	...	...
130	Consume Data [32,000-32,249]	UINT	0	Get / Set
131	Consume Data [32,250-32,249]	UINT	0	Get / Set
132	Consume Data [32,500-32,249]	UINT	0	Get / Set
133	Consume Data [32,750-32,767]	UINT	0	Get / Set

**Common Services**

Service Code	Implemented for		Service Name
	Class Level	Instance Level	
05 <sub>HEX</sub>	No	Yes	Reset <sup>10</sup>
0E <sub>HEX</sub>	Yes	Yes	Get Attribute Single
10 <sub>HEX</sub>	No	Yes	Set Attribute Single

---

<sup>10</sup> This Service Code is used to flush all attributes to zero.



## C.22 HS500E Produce Data Object (0x65 - 32 Instances)

### Class Attributes (Instance 0)

Attribute ID	Name	Data Type	Default Data Value	Access Rule
1	Revision	UINT	1	Get
2	Maximum Produce Data Buffer Size (in words)	UINT	32768	Get
3	Bitmap of Produce Instances with Data <i>Bit 0: Instance 1 ... Bit 31: Instance 32</i>	DINT	0	Get

### Instance Attributes (Instances 1-32)

Attribute ID	Name	Data Type	Default Data Value	Access Rule
1	Produce Data Size (in words)	UINT	0	Get / Set
2	Produce Data [0-249]	UINT	0	Get
3	Produce Data [250-499]	UINT	0	Get
4	Produce Data [500-749]	UINT	0	Get
5	Produce Data [750-999]	UINT	0	Get
6	Produce Data [1,000-1,249]	UINT	0	Get
...	...	...	...	...
10	Produce Data [2,000-2,249]	UINT	0	Get
...	...	...	...	...
34	Produce Data [8,000-8,249]	UINT	0	Get





...	...	...	...	...
38	Produce Data [9,000-9,249]	UINT	0	Get
...	...	...	...	...
42	Produce Data [10,000-10,249]	UINT	0	Get
...	...	...	...	...
82	Produce Data [20,000-20,249]	UINT	0	Get
...	...	...	...	...
122	Produce Data [30,000-30,249]	UINT	0	Get
...	...	...	...	...
126	Produce Data [31,000-31,249]	UINT	0	Get
...	...	...	...	...
130	Produce Data [32,000-32,249]	UINT	0	Get
131	Produce Data [32,250-32,249]	UINT	0	Get
132	Produce Data [32,500-32,249]	UINT	0	Get
133	Produce Data [32,750-32,767]	UINT	0	Get

**Common Services**

Service Code	Implemented for		Service Name
	Class Level	Instance Level	
05 <sub>HEX</sub>	No	Yes	Reset <sup>11</sup>
0E <sub>HEX</sub>	Yes	Yes	Get Attribute Single
10 <sub>HEX</sub>	No	Yes	Set Attribute Single

---

<sup>11</sup> This Service Code is used to flush all attributes to zero.



### C.23 OnDemand Object (0x67 - 10 Instances)

#### Class Attributes (Instance 0)

Attribute ID	Name	Data Type	Default Data Value	Access Rule
1	Revision	UINT	1	Get

#### Instance Attributes (Instances 1-32)

Attribute ID	Name	Data Type	Default Data Value	Access Rule
1	<u>Instance Type (0-3)</u> 0 - Disable 1 – ControlLogix 2 – SLC 5/05 3 – PLC5E	USINT	0	Get
2	<u>PLC IP Address</u>	UDINT	0	Get
3	<u>PLC Slot Location</u> (0-255)	USINT	0	Get
11	<u>Max Write Size in Words</u> 0 – Disabled 1 – 100 Words	UINT	0	Get
12	<u>Write Tag Name</u> (ControlLogix Only)	SHORT STRING	0	Get
13	<u>Write File Number</u> (SLC/PLC Only) NX:0 where X is the File Number	UINT	7	Get



14	<u>Write File Offset</u> (SLC/PLC Only) N7:Y where Y is the File Offset	UINT	0	Get
15	<u>Write Heartbeat Timeout:</u> 0 = disabled 5-60000 ticks = enable (10ms Resolution)	UINT	100	Get
21	<u>Max Read Size in Words</u> 0 – Disable 1 – 100 Words	UINT	0	Get
22	<u>Read Tag Name</u> (ControlLogix Only)	SHORT STRING	0	Get
23	<u>Read File Number</u> (SLC/PLC Only) NX:0 where X is the File Number	UINT	7	Get
24	<u>Read File Offset</u> (SLC/PLC Only) N7:Y where Y is the File Offset	UINT	0	Get
25	<u>Read Poll Rate</u> 5-60000 ticks = enable (10ms Resolution)	UINT	100	Get

**Common Services**

Service Code	Implemented for		Service Name
	Class Level	Instance Level	
0E <sub>HEX</sub>	Yes	Yes	Get Attribute Single



## EMS WARRANTY

ESCORT MEMORY SYSTEMS  
A DATALOGIC GROUP COMPANY



Escort Memory Systems warrants that all products of its own manufacturing conform to Escort Memory Systems' specifications and are free from defects in material and workmanship when used under normal operating conditions and within the service conditions for which they were furnished. The obligation of Escort Memory Systems hereunder shall expire one (1) year after delivery, unless otherwise specified, and is limited to repairing, or at its option, replacing without charge, any such product which in Escort Memory Systems' sole opinion proves to be defective within the scope of this Warranty. In the event Escort Memory Systems is not able to repair or replace defective products or components within a reasonable time after receipt thereof, Buyers shall be credited for their value at the original purchase price. Escort Memory Systems must be notified in writing of the defect or nonconformity within the warranty period and the affected product returned to Escort Memory Systems factory or to an authorized service center within thirty (30) days after discovery of such defect or nonconformity. Shipment shall not be made without prior authorization by Escort Memory Systems.

This is Escort Memory Systems' sole warranty with respect to the products delivered hereunder. No statement, representation, agreement or understanding oral or written, made by an agent, distributor, representative, or employee of Escort Memory Systems which is not contained in this warranty, will be binding upon Escort Memory Systems, unless made in writing and executed by an authorized Escort Memory Systems employee.

Escort Memory Systems makes no other warranty of any kind what so ever, expressed or implied, and all implied warranties of merchantability and fitness for a particular use which exceed the aforementioned obligation are hereby disclaimed by Escort Memory Systems and excluded from this agreement. Under no circumstances shall Escort Memory Systems be liable to Buyer, in contract or in tort, for any special, indirect, incidental, or consequential damages, expenses, losses or delay however caused. Equipment or parts which have been subject to abuse, misuse, accident, alteration, neglect, unauthorized repair or installation are not covered by warranty. Escort Memory Systems shall make the final determination as to the existence and cause of any alleged defect. No liability is assumed for expendable items such as lamps and fuses. No warranty is made with respect to equipment or products produced to Buyer's specification except as specifically stated in writing by Escort Memory Systems in the contract for such custom equipment. This warranty is the only warranty made by Escort Memory Systems with respect to the goods delivered hereunder, and may be modified or amended only by a written instrument signed by a duly authorized officer of Escort Memory Systems and accepted by the Buyer.

Extended warranties of up to four years are available for purchase for most Escort Memory Systems products. Contact Escort Memory Systems or your distributor for more information.

Copyright © 2005 Escort Memory Systems, all rights reserved.