ESCORT MEMORY SYSTEMS
A DATALOGIC GROUP COMPANY

HS500E
OPERATOR'S MANUAL

WE MAKE RFID WORK™

HS500E

READ/WRITE INDUSTRIAL ETHERNET ANTENNA

Escort Memory Systems' Active Radio Frequency Identification Device

OPERATOR'S MANUAL

How to Install, Configure and Operate

Escort Memory Systems'

HS500E Industrial Ethernet Antenna

HS500E Industrial Ethernet Antenna - Operator's Manual - P/N: 17-1305 REV 01.D (08-05)

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

CHAPTER 1: GETTING STARTED

This chapter contains an introduction to Escort Memory Systems and includes general information relating to the HS500E Industrial Ethernet Antenna and common uses for RFID technology.

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.

Escort Memory Systems' headquarters in Scotts Valley, CA.

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.

RFID Overview

The first step in most RFID systems involves attaching a tag to a product or its carrier. The RFID tag acts as an electronic identifier, portable job sheet, or real-time tracking database. Tags are identified, read and written to by issuing specific commands from a Host computer. Tags can be read and written to through any nonconductive, non-metallic material, while moving or standing still, in or out of the direct line of sight.

1.2 ABOUT THIS MANUAL

This document provides guidelines and instructions on how to install and operate the HS500E Industrial Ethernet Antenna. Also included are descriptions of the RFID command set with instructions detailing how to issue commands from the Host computer to the HS500E.

SIDE NOTE:

Occasionally throughout this manual, we refer to the **HS500E Industrial Ethernet Antenna** as the *HS500E*, the *HS500E Antenna,* the *Industrial Antenna* or just simply "*the* Antenna*.*"

Who Should Read this Manual?

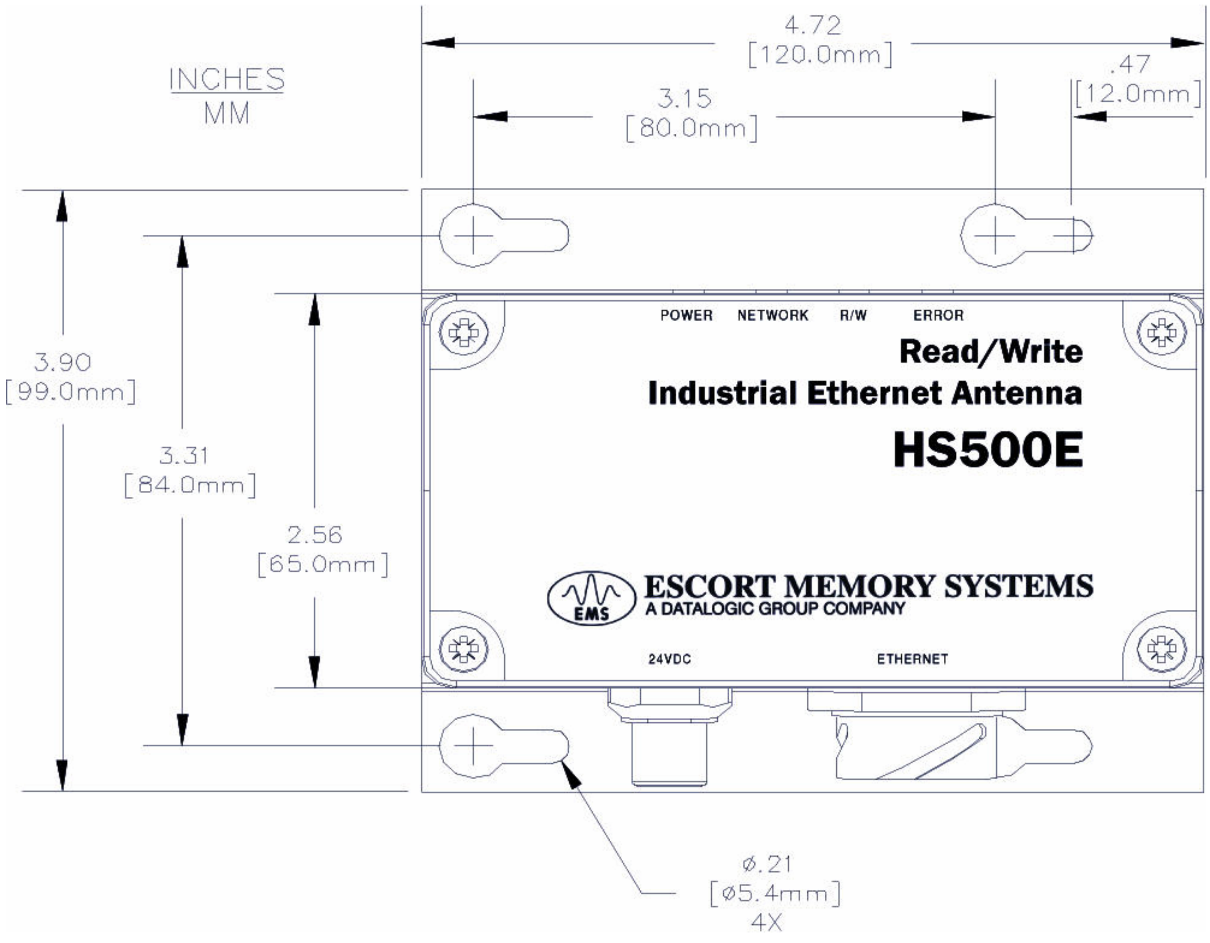
Those who will be installing, configuring and operating the HS500E should read this manual. This may include the following people:

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

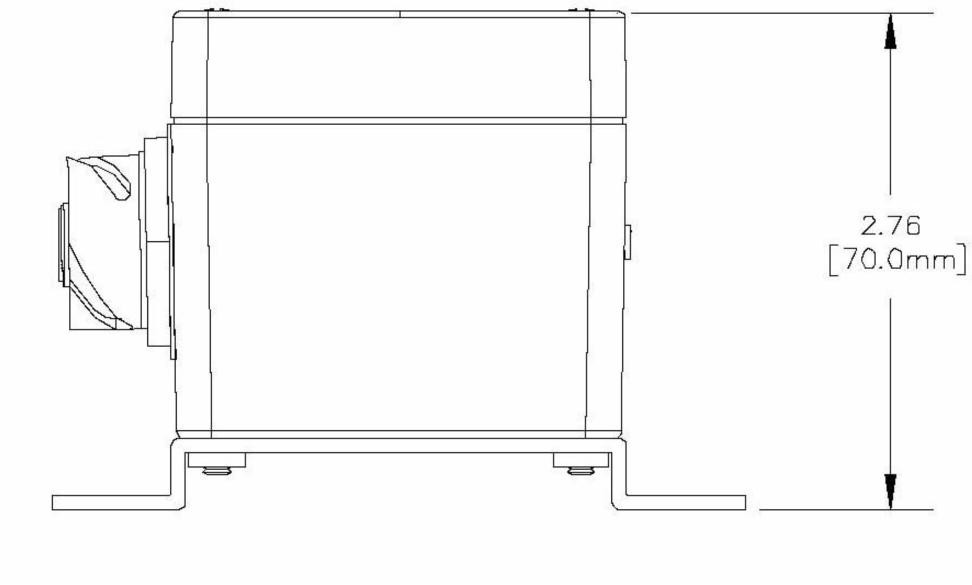
HEX Notation

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.

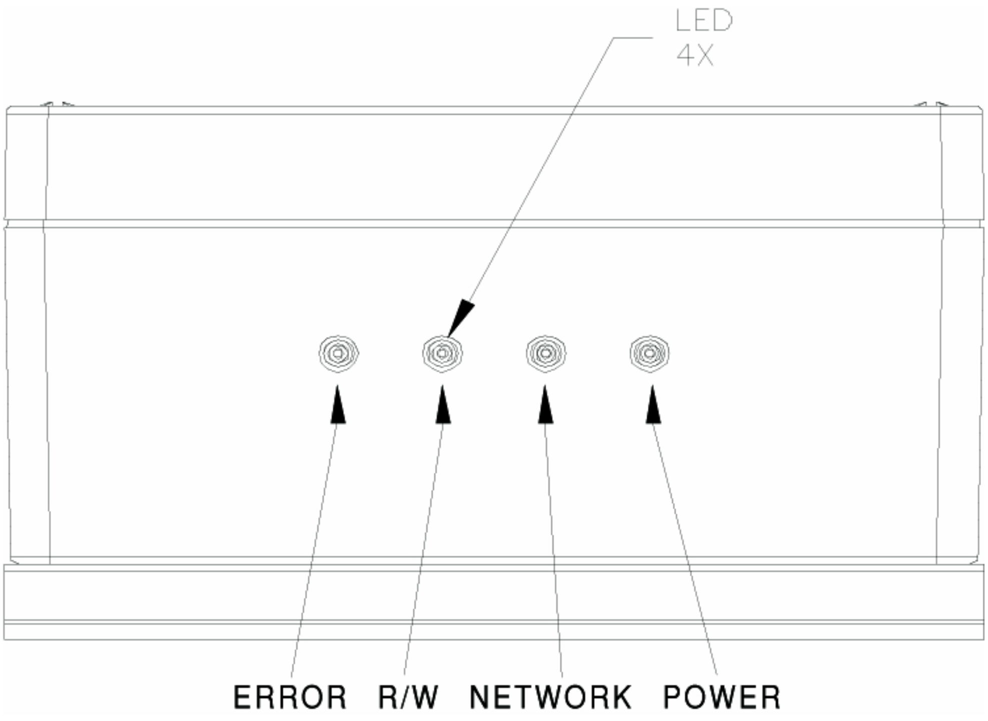
1.3 HS500E DIMENSIONS & DIAGRAMS



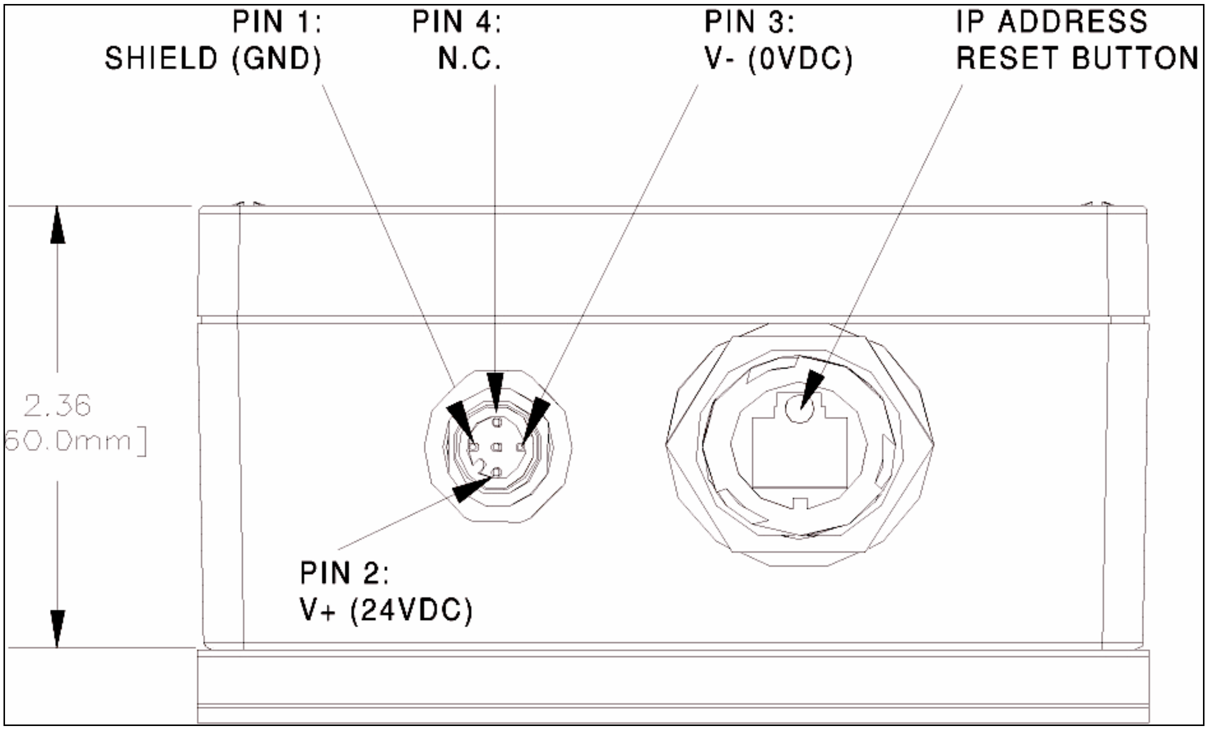
HS500E - Dimensions



HS500E Side/Profile View



HS500E LEDs



HS500E – Power & Ethernet Connections

CHAPTER 2: INTERFACING WITH THE HS500E

The HS500E supports four different interface connections over Ethernet.

- **MODBUS-TCP**
- **ETHERNET-IP**
- **TCP-IP**
- **OnDemand**

The process of issuing commands and receiving responses depends on the interface chosen and the Host computer that is connected to the HS500E.

This chapter contains a brief overview of how commands can be sent using the four different interfaces listed above.

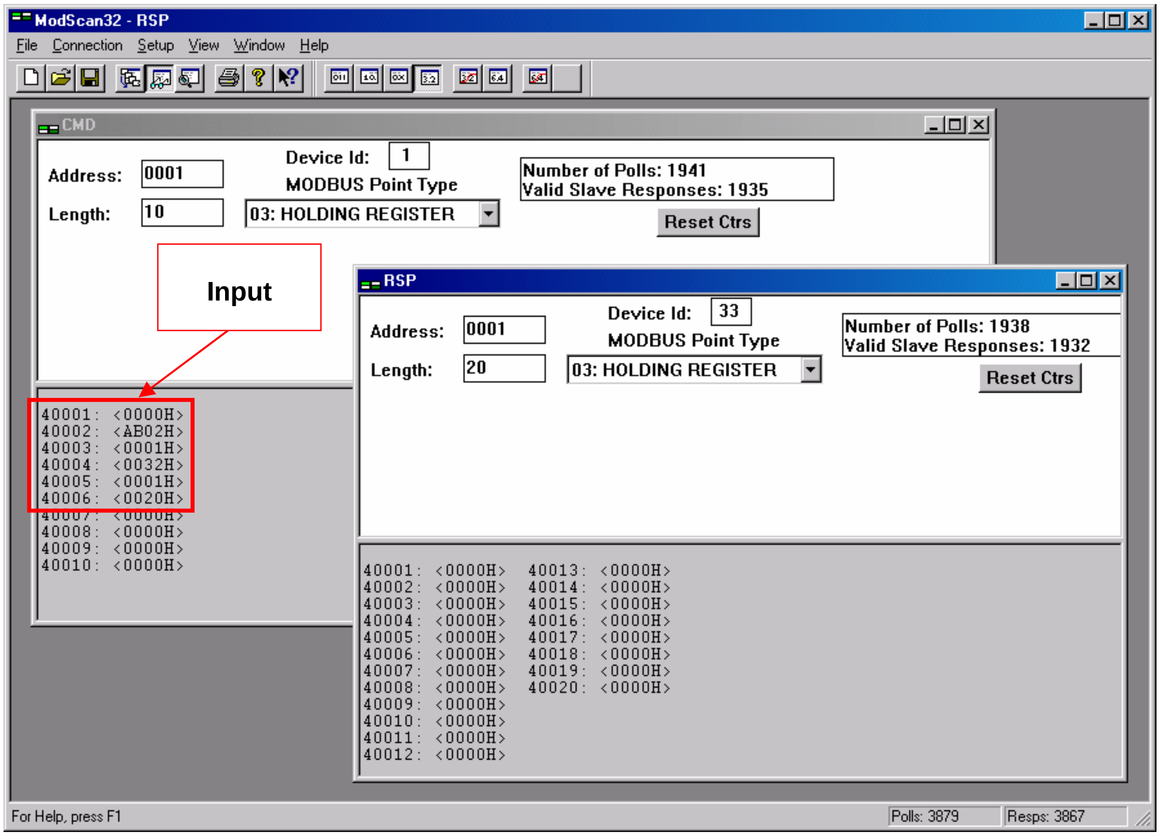
For additional information regarding the interface used by your particular RFID application, please refer to the documentation for your Host software program.

2.1 MODBUS-TCP INTERFACE

Note: Maximum number of registers transferred to/from an RFID tag per command issued = 125 Registers (250 Bytes).

Commands must be placed in the Holding Register Area of Node 1, starting at address 40001. Most commands utilize 6 registers (double-byte values or words). The Write Data command will require more words to transmit the data used for the Write.

The first register, 40001, indicates the number of words in the Command Packet (including the Overall Length). The command will trigger a response which will be returned at Node Address 33 (Device ID 33), in registers 40001 and up. Below is an example taken from Modscan32, a utility that implements ModBus on a PC.



CMD

Address: 0001
Device Id: 1
MODBUS Point Type
Length: 10
03: HOLDING REGISTER
Number of Polls: 1941
Valid Slave Responses: 1935

```
40001: <0000H>
40002: <AB02H>
40003: <0001H>
40004: <0032H>
40005: <0001H>
40006: <0020H>
40007: <0000H>
40008: <0000H>
40009: <0000H>
40010: <0000H>
```

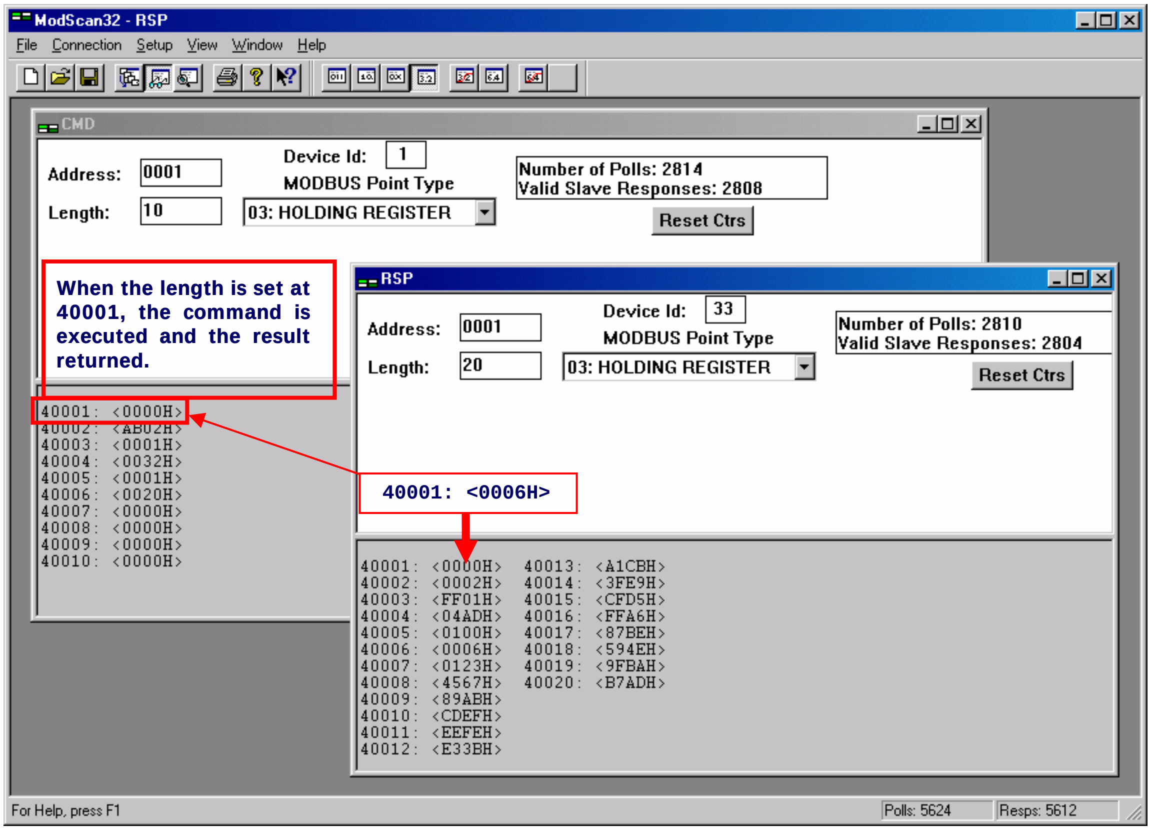
RSP

Address: 0001
Device Id: 33
MODBUS Point Type
Length: 20
03: HOLDING REGISTER
Number of Polls: 1938
Valid Slave Responses: 1932

```
40001: <0000H>  40013: <0000H>
40002: <0000H>  40014: <0000H>
40003: <0000H>  40015: <0000H>
40004: <0000H>  40016: <0000H>
40005: <0000H>  40017: <0000H>
40006: <0000H>  40018: <0000H>
40007: <0000H>  40019: <0000H>
40008: <0000H>  40020: <0000H>
40009: <0000H>
40010: <0000H>
40011: <0000H>
40012: <0000H>
```

Polls: 3879
Resps: 3867

The input area is highlighted in red. When the value of the 40001 register for Node Address 1 transitions from 0 to a non-zero length, the command will be issued by the Host and executed by the HS500E. The resulting response is reported in the output area at Node Address 33 (Device ID 33).



CMD

Address: 0001

Length: 10

Device Id: 1

MODBUS Point Type: 03: HOLDING REGISTER

Number of Polls: 2814
Valid Slave Responses: 2808

When the length is set at 40001, the command is executed and the result returned.

```
40001: <0000H>
40002: <AB02H>
40003: <0001H>
40004: <0032H>
40005: <0001H>
40006: <0020H>
40007: <0000H>
40008: <0000H>
40009: <0000H>
40010: <0000H>
```

RSP

Address: 0001

Length: 20

Device Id: 33

MODBUS Point Type: 03: HOLDING REGISTER

Number of Polls: 2810
Valid Slave Responses: 2804

40001: <0006H>

```
40001: <0000H>   40013: <A1CBH>
40002: <0002H>   40014: <3FE9H>
40003: <FF01H>   40015: <CFD5H>
40004: <04ADH>   40016: <FFA6H>
40005: <0100H>   40017: <87BEH>
40006: <0006H>   40018: <594EH>
40007: <0123H>   40019: <9FBAH>
40008: <4567H>   40020: <B7ADH>
40009: <89ABH>
40010: <CDEFH>
40011: <EEFEH>
40012: <E33BH>
```

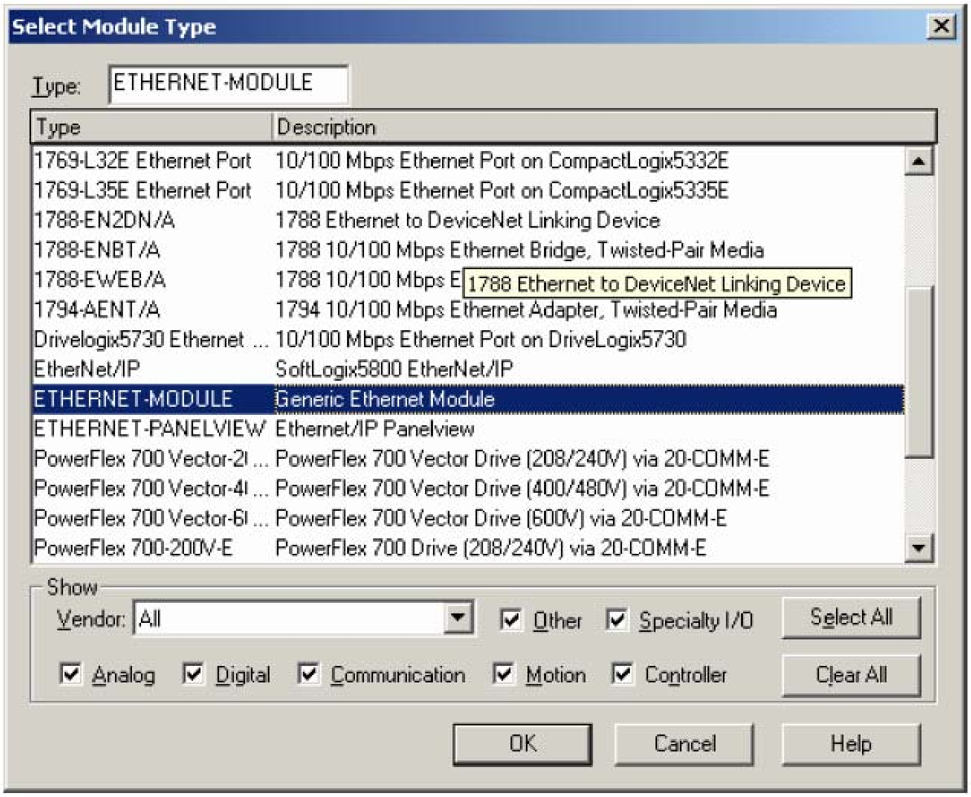
For Help, press F1 | Polls: 5624 | Resps: 5612

When the command is completed, the HS500E will reset the length at 40001 of Node Address 1 back to 0. This way a simple handshaking mechanism can be implemented.

2.2 ETHERNET/IP INTERFACE

The mechanism to send commands over Ethernet/IP is similar to that of MODBUS-TCP. Commands must still be copied to the appropriate registers. However, the mechanism for handshaking is different. For example, in a ControlLogix environment, commands must be written to the ControlLogix tags that are generated when the HS500E is added to the I/O Configuration.

The first step is to add the HS500E to the ControlLogix PLC. To add the HS500E to the PLC using RSLogix5000, right click on the Ethernet Bridge Device and select "New Module…" Choose **Generic Ethernet Module.**



Select Module Type

Type: ETHERNET-MODULE

Type	Description
1769-L32E Ethernet Port	10/100 Mbps Ethernet Port on CompactLogix5332E
1769-L35E Ethernet Port	10/100 Mbps Ethernet Port on CompactLogix5335E
1788-EN2DN/A	1788 Ethernet to DeviceNet Linking Device
1788-ENBT/A	1788 10/100 Mbps Ethernet Bridge, Twisted-Pair Media
1788-EWEB/A	1788 10/100 Mbps E 1788 Ethernet to DeviceNet Linking Device
1794-AENT/A	1794 10/100 Mbps Ethernet Adapter, Twisted-Pair Media
Drivelogix5730 Ethernet ...	10/100 Mbps Ethernet Port on DriveLogix5730
EtherNet/IP	SoftLogix5800 EtherNet/IP
ETHERNET-MODULE	Generic Ethernet Module
ETHERNET-PANELVIEW	Ethernet/IP Panelview
PowerFlex 700 Vector-2(...	PowerFlex 700 Vector Drive (208/240V) via 20-COMM-E
PowerFlex 700 Vector-4(...	PowerFlex 700 Vector Drive (400/480V) via 20-COMM-E
PowerFlex 700 Vector-6(...	PowerFlex 700 Vector Drive (600V) via 20-COMM-E
PowerFlex 700-200V-E	PowerFlex 700 Drive (208/240V) via 20-COMM-E

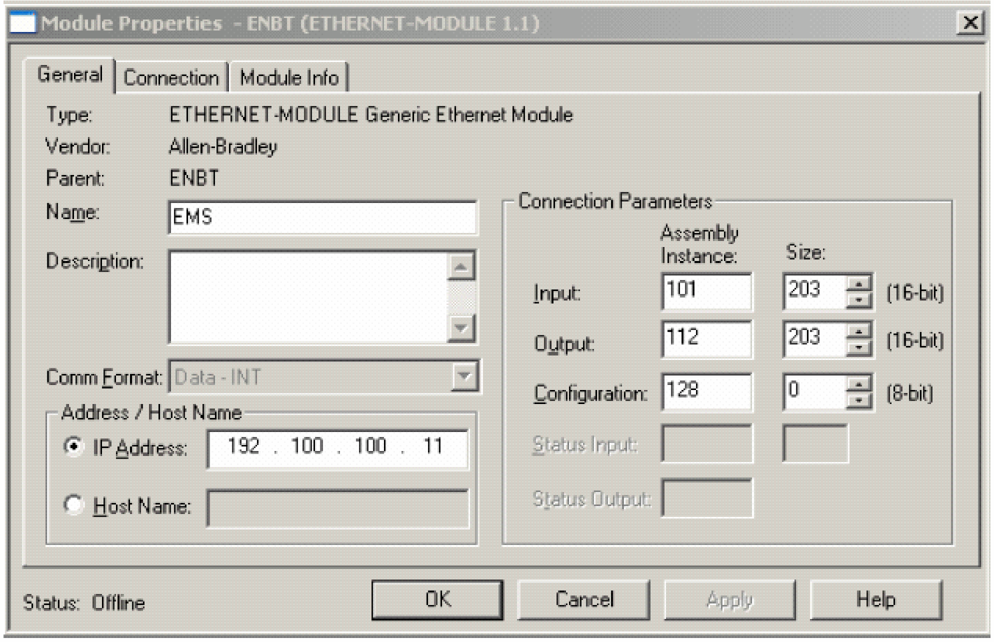
Show

Vendor: All

☑ Other ☑ Specialty I/O

☑ Analog ☑ Digital ☑ Communication ☑ Motion ☑ Controller

Assign a name to the new device. In the example below, the device has been named **EMS.** Configure the **IP Address** to match the IP Address of the HS500E. Match the **Connection Parameters** to the image below.



Type: ETHERNET-MODULE Generic Ethernet Module
Vendor: Allen-Bradley
Parent: ENBT
Name: EMS
Description:
Comm Format: Data - INT

Address / Host Name

● IP Address: 192 . 100 . 100 . 11
○ Host Name:

Connection Parameters

	Assembly Instance:	Size:	
Input:	101	203	(16-bit)
Output:	112	203	(16-bit)
Configuration:	128	0	(8-bit)
Status Input:			
Status Output:			

Status: Offline

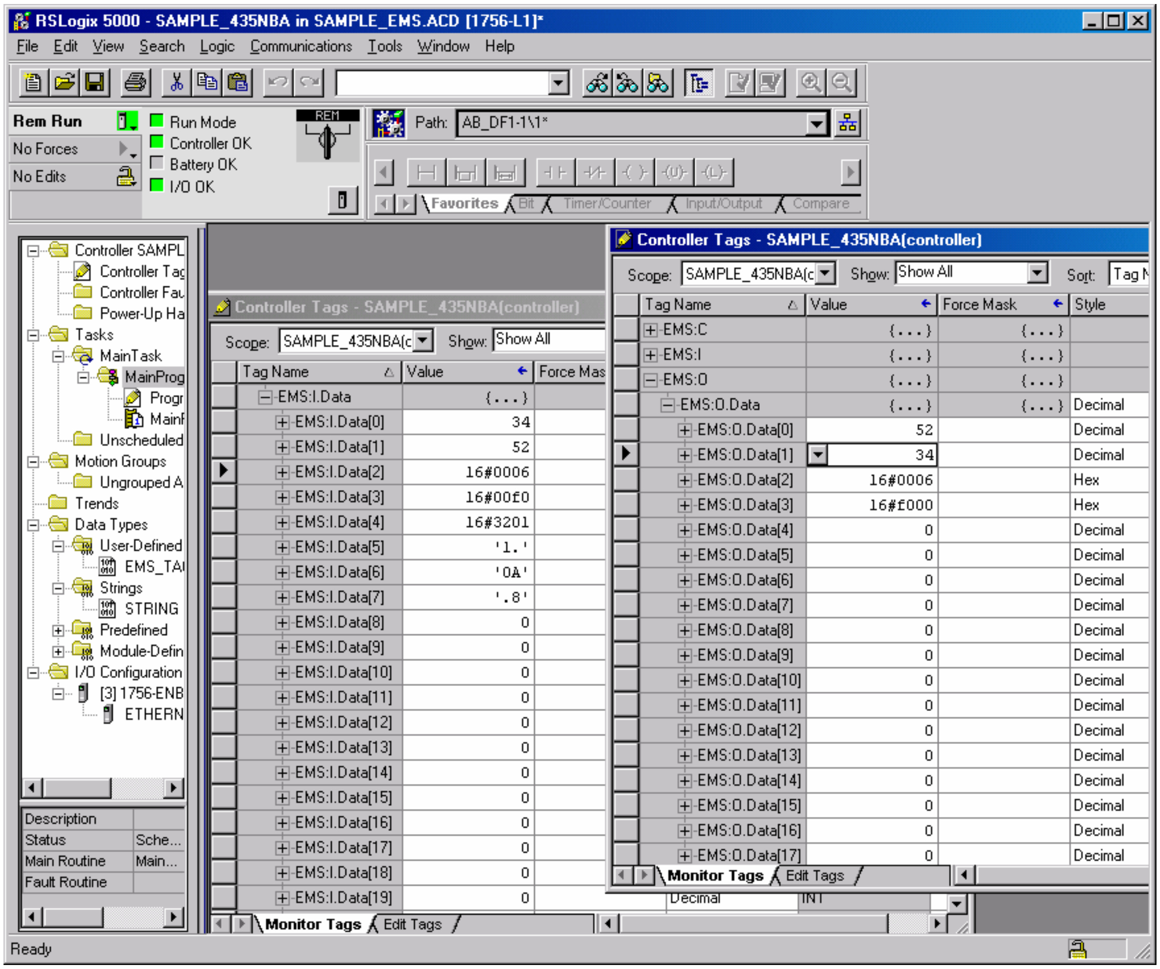
After clicking the **OK** button, there will be predefined tags containing the specified I/O Information.

Predefined Tags

```
INPUT
EMS:I.Data [0] = Consume Data Sequence Number Handshake
EMS:I.Data [1] = Produce Data Sequence Number
EMS:I.Data [2] = Node 1 Serial Produce Data Size
EMS:I.Data [3-202] = Node 1 Serial Produce Data

OUTPUT
EMS:O.Data [0] = Produce Data Sequence Number Handshake
EMS:O.Data [1] = Consume Data Sequence Number
EMS:O.Data [2] = Node 1 Serial Consume Data Size
EMS:O.Data [3-202] = Node 1 Serial Consume Data
```

The image below displays the input and output tags during the execution of a command:



Controller Tags - SAMPLE_435NBA(controller)

Scope: SAMPLE_435NBA(c Show: Show All

Tag Name	Value	Force Mas
EMS:I.Data	{...}	
EMS:I.Data[0]	34	
EMS:I.Data[1]	52	
EMS:I.Data[2]	16#0006	
EMS:I.Data[3]	16#00f0	
EMS:I.Data[4]	16#3201	
EMS:I.Data[5]	'1.'	
EMS:I.Data[6]	'0A'	
EMS:I.Data[7]	'.8'	
EMS:I.Data[8]	0	
EMS:I.Data[9]	0	
EMS:I.Data[10]	0	
EMS:I.Data[11]	0	
EMS:I.Data[12]	0	
EMS:I.Data[13]	0	
EMS:I.Data[14]	0	
EMS:I.Data[15]	0	
EMS:I.Data[16]	0	
EMS:I.Data[17]	0	
EMS:I.Data[18]	0	
EMS:I.Data[19]	0	

Monitor Tags / Edit Tags

Controller Tags - SAMPLE_435NBA(controller)

Scope: SAMPLE_435NBA(c Show: Show All Sort: Tag N

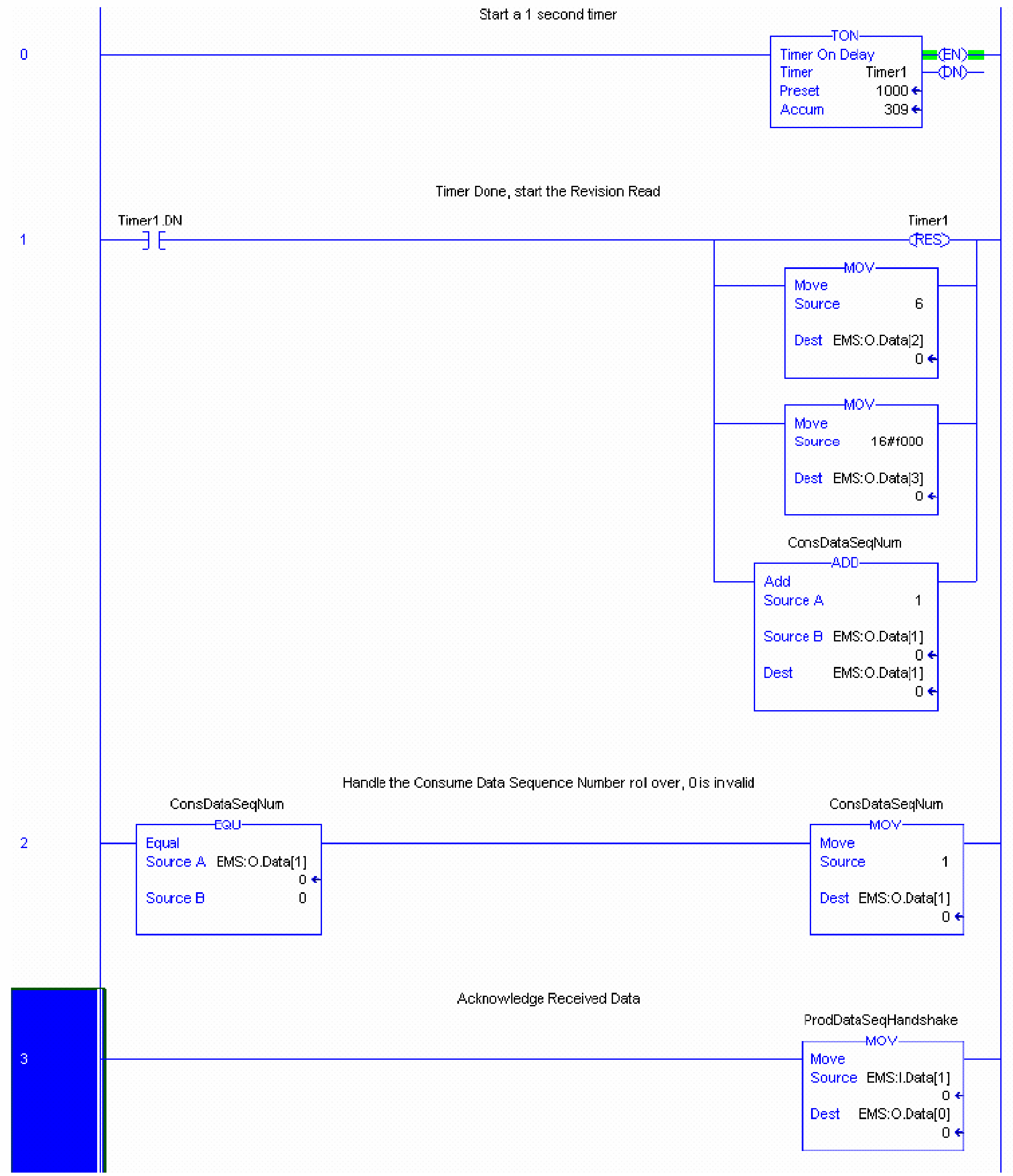
Tag Name	Value	Force Mask	Style
EMS:C	{...}	{...}	
EMS:I	{...}	{...}	
EMS:O	{...}	{...}	
EMS:O.Data	{...}	{...}	Decimal
EMS:O.Data[0]	52		Decimal
EMS:O.Data[1]	34		Decimal
EMS:O.Data[2]	16#0006		Hex
EMS:O.Data[3]	16#f000		Hex
EMS:O.Data[4]	0		Decimal
EMS:O.Data[5]	0		Decimal
EMS:O.Data[6]	0		Decimal
EMS:O.Data[7]	0		Decimal
EMS:O.Data[8]	0		Decimal
EMS:O.Data[9]	0		Decimal
EMS:O.Data[10]	0		Decimal
EMS:O.Data[11]	0		Decimal
EMS:O.Data[12]	0		Decimal
EMS:O.Data[13]	0		Decimal
EMS:O.Data[14]	0		Decimal
EMS:O.Data[15]	0		Decimal
EMS:O.Data[16]	0		Decimal
EMS:O.Data[17]	0		Decimal

Monitor Tags / Edit Tags

Commands are placed into the O.Data structure, beginning at word 2, while their corresponding responses can be located in the I.Data structure again beginning at word 2. The data located at words 0 and 1 are used for handshaking.

The device that produces the information must increment the sequence number by one for every data packet that is exchanged. The device that consumes the information must echo the sequence number in the handshake location after the data is processed. Valid sequence numbers are 1 to 65535, 0 is not allowed.

Below is a sample ladder logic program that sets up a timer to send a new request every 1000ms. Every time a new message is sent, the command (0xF000) and length (0x0006) are written to the I/O Data structure and the Consume Data Sequence Number is incremented by 1. Note that if the Consume Data Sequence Number reverts back to 0, the sequence number must be set to 1 (see rung 2 in the image below). With each scan the PLC copies the Produce Data Sequence Number to the Produce Data Sequence Number Handshake. This process is used to acknowledge the receipt of the data from the HS500E.



```
0   Start a 1 second timer
    TON  Timer On Delay
         Timer    Timer1
         Preset   1000
         Accum    309
    (EN) (DN)

1   Timer Done, start the Revision Read
    Timer1.DN                                    Timer1 (RES)
    MOV  Move
         Source   6
         Dest     EMS:O.Data[2]  0
    MOV  Move
         Source   16#f000
         Dest     EMS:O.Data[3]  0
    ConsDataSeqNum
    ADD  Add
         Source A 1
         Source B EMS:O.Data[1]  0
         Dest     EMS:O.Data[1]  0

2   Handle the Consume Data Sequence Number rol over, 0 is invalid
    ConsDataSeqNum                               ConsDataSeqNum
    EQU  Equal                                   MOV  Move
         Source A EMS:O.Data[1]  0                    Source   1
         Source B 0                                   Dest     EMS:O.Data[1]  0

3   Acknowledge Received Data
    ProdDataSeqHandshake
    MOV  Move
         Source   EMS:I.Data[1]  0
         Dest     EMS:O.Data[0]  0
```

2.3 TCP/IP Interface

It is also possible to communicate with the HS500E through a standard TCP-IP session. A session between the client software and the reader consists of a *connection setup, data transactions* and the *connection termination*. The HS500E acts as the server and the user must supply the client software.

All connections to the HS500E are initiated by client software only. If, for example, an existing connection terminates unexpectedly, the HS500E will not attempt to contact the client software to reestablish the connection. The client software is responsible for opening, maintaining, and closing any TCP-IP session.

The client software must first establish a TCP socket connection to the Ethernet Antenna on **port 50200**. After connecting successfully, communication between the client software and the Ethernet Antenna can proceed. When communication with the Ethernet Antenna is no longer necessary, it is the responsibility of the client application to terminate the connection.

RFID Commands follow the format below:

<Data_Size><Data><Reserved_Fields><Checksum>

WHERE:

<**Data_Size**> = data length in number of words.

<**Data**> = words that comprise the command.

<**Reserved_Fields**> = will always be 0x00, 0x00

<**Checksum**> = 16-bit 2's compliment of the sum of all bytes

Example:

The string below is an example of a **Read Data** command sent to the HS500E:

0x00 0x06 0xAB 0x02 0x00 0x01 0x00 0x32 0x00 0x01 0x00 0x20 0x00 0x00 0xFE 0xF9

Note: the first 12 bytes are listed in the table below; the remaining 4 bytes are reserved fields and checksum.

Command 02 - Read Data

Field Name	MSB	LSB	Word Value
Overall Length	00	06	0006
Command ID Number	AB	02	AB02
Node ID Number	00	01	0001
Timeout	00	32	0032
Start Address	00	01	0001
Read Length	00	20	0020

RFID Command Responses follow the format below:

<Data_Size><Data><Reserved_Field><Checksum>

WHERE:

<**Data_Size**> = data length in words.

<**Data**> = words of the command response.

<**Reserved_Field**> = N/A

<**Checksum**> = 16-bit 2's compliment of the sum of all bytes.

2’s Compliment Example

Byte	Value	Sum
0	0x02	0x0002
1	0x00	0x0002
2	0x12	0x0014
3	0x34	0x0048
4	0x54	0x009E
5	0x78	0x0116

Description	Binary	Hexadecimal
SUM	0000 0001 0001 0110	0x0116
1’s Compliment	1111 1110 1110 1001	0xFEE9
2’s Compliment	1111 1110 1110 1010	0xFEEA

2.4 ONDEMAND CONFIGURATION

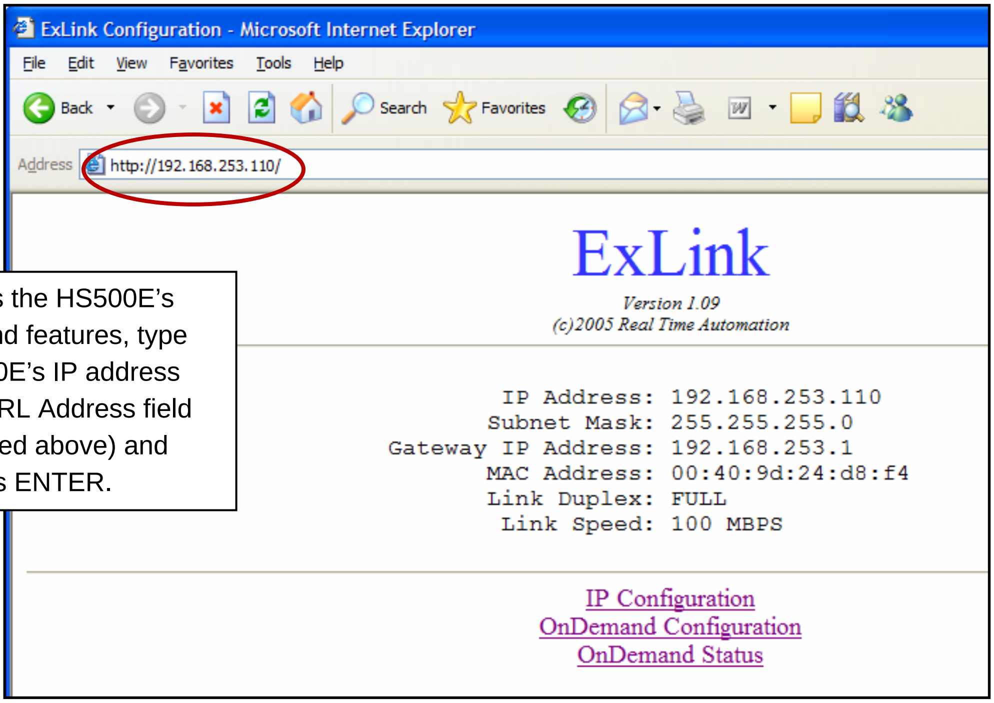
After you have confirmed that the PC, HS500E and PLC can communicate, it is time to use the HS500E's built-in Web Server to configure the HS500E's "***OnDemand***" communications features. OnDemand links the Industrial Antenna to specific "***Tags***" as defined in the ControlLogix PLC.

NOTE: the ControlLogix PLC refers to a "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."

OnDemand communications features are accessed through the HS500E's built-in Web Server.

1. Start by opening a Web browser on the PC.
2. In the URL address field, enter the Industrial Gateway's IP address: 192.168.0.100
3. Press ENTER.

The OnDemand Website will be displayed.



http://192.168.253.110/

ExLink

Version 1.09
(c)2005 Real Time Automation

```
          IP Address: 192.168.253.110
         Subnet Mask: 255.255.255.0
  Gateway IP Address: 192.168.253.1
         MAC Address: 00:40:9d:24:d8:f4
         Link Duplex: FULL
          Link Speed: 100 MBPS
```

IP Configuration
OnDemand Configuration
OnDemand Status

To access the HS500E's OnDemand features, type the HS500E's IP address into the URL Address field (as depicted above) and then press ENTER.

A screen shot of the HS500E's OnDemand Website – Main Page

The **Main Page** of the OnDemand Website lists the IP address (and several other network parameters) as currently stored on the HS500E.

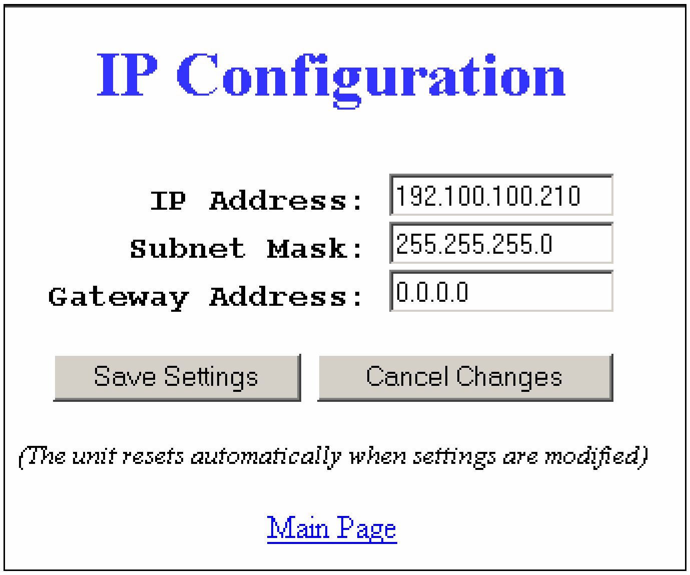
There are three important links on this page. They are labeled:

- **IP Configuration**
- **OnDemand Configuration**
- **OnDemand Status**

2.4.1 IP Configuration

The ***IP Configuration*** page provides an option to modify and configure the HS500E's IP address, Subnet Mask and (Network) Gateway Address.

To modify the IP settings of the HS500E, go to the HS500E's OnDemand Website Main Page and click the **IP Configuration** link to arrive at the page displayed below.



IP Configuration

IP Address: 192.100.100.210

Subnet Mask: 255.255.255.0

Gateway Address: 0.0.0.0

(The unit resets automatically when settings are modified)

The OnDemand Website - IP Configuration Page

Enter the new IP configuration values in the fields provided.

Click the "**Save Settings"** button to store the configuration changes to the HS500E's flash memory.

Power will be automatically recycled to the unit at which time the HS500E will reset and implement your IP configuration changes.

After the HS500E has completely restarted, you can view the new IP configuration by opening a Web browser and entering the HS500E's new IP address in the URL field.

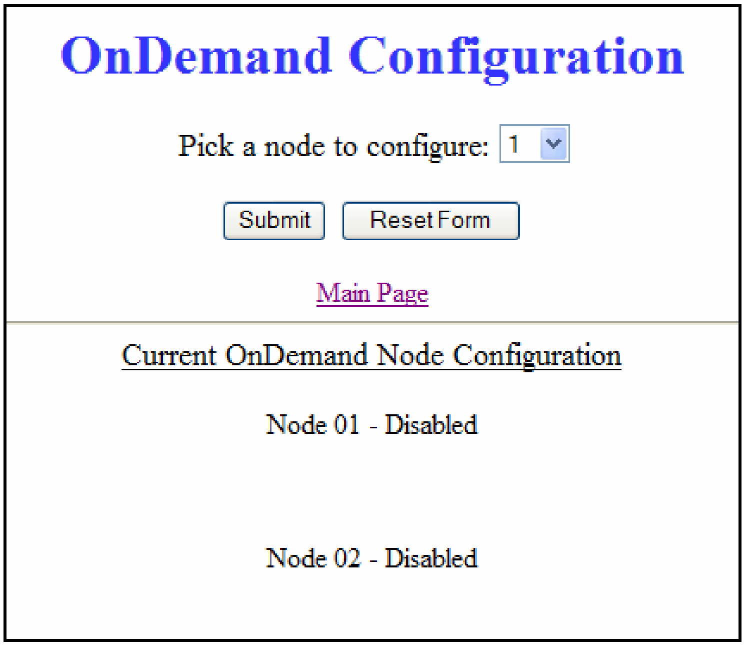
To return to the OnDemand Website – Main Page, click the link labeled **Main Page.**

2.4.2 OnDemand Configuration

At the **OnDemand Website – Main Page**, Click the link labeled "**OnDemand Configuration**."

The OnDemand Configuration page will be displayed.

As noted, OnDemand is used to link the HS500E to specific tags defined in the ControlLogix PLC. The OnDemand Configuration page allows you to modify the settings of the HS500E's Subnet Node.



OnDemand Configuration

Pick a node to configure: 1

Current OnDemand Node Configuration

Node 01 - Disabled

Node 02 - Disabled

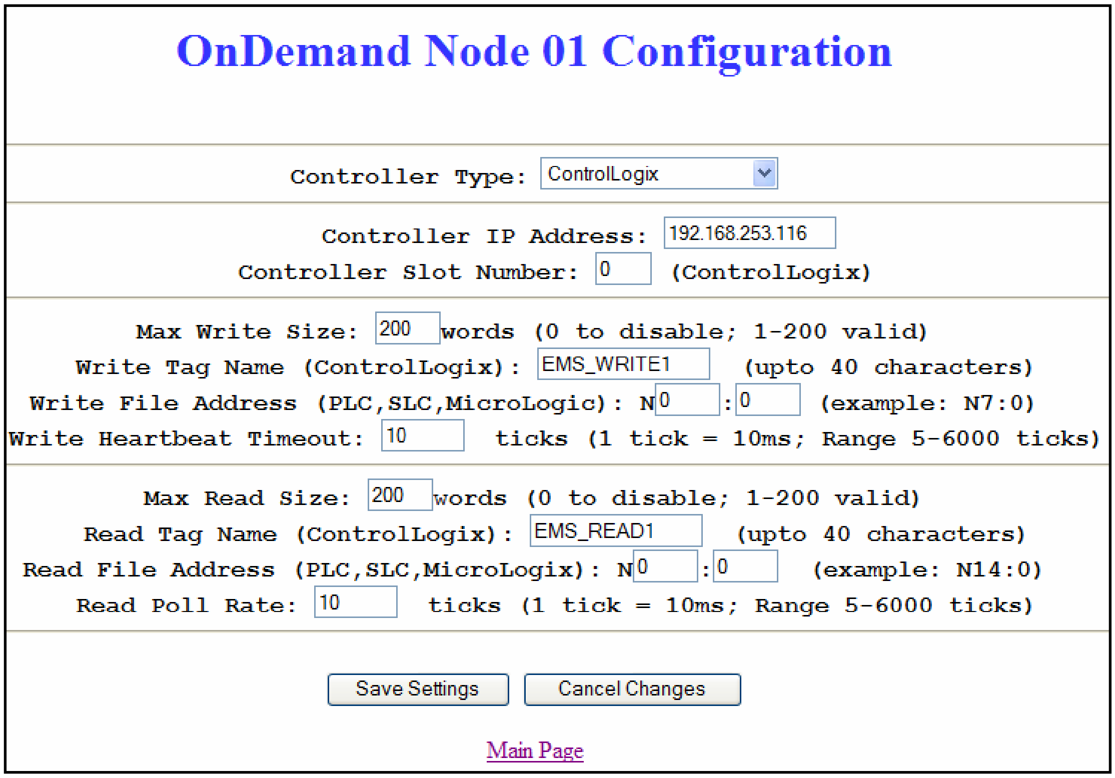
The OnDemand Website – OnDemand Configuration Page

Follow the steps below to modify the Node configuration settings for the HS500E:

At the OnDemand Configuration page, select **Node 01** from the drop-down list. (Note that Node 01 is selected in the image above).

Click **Submit**.

The OnDemand Node 01 Configuration Page will be displayed.



OnDemand Node 01 Configuration

Controller Type: ControlLogix

Controller IP Address: 192.168.253.116

Controller Slot Number: 0 (ControlLogix)

Max Write Size: 200 words (0 to disable; 1-200 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: 200 words (0 to disable; 1-200 valid)

Read Tag Name (ControlLogix): EMS_READ1 (upto 40 characters)

Read File Address (PLC,SLC,MicroLogix): N0 :0 (example: N14:0)

Read Poll Rate: 10 ticks (1 tick = 10ms; Range 5-6000 ticks)

The OnDemand Node 01 Configuration Page

PLC Controller Settings

1. Select a ***Controller Type*** from the drop-down menu.

(Controller Type specifies the type of PLC that will be communicating with the HS500E).

2. Enter the ***Controller's IP address***.

(Controller IP address is the IP address assigned to the PLC).

3. Enter the ***Controller's Slot Number***.

(Controller Slot Number indicates where in the PLC rack the CPU processor module is installed; normally slot 0 for ControlLogix.

Write Settings

4. Specify the number of words (between 1 and 200) for the ***Max Write Size***.

(The Max Write Size indicates the maximum number of 2-byte data “words” that the HS500E will write to PLC memory each command-response cycle).

5. Specify a ***Write Tag Name*** that is 40 characters or less.

(The Write Tag Name refers to the name of the tag in the PLC where the HS500E will write data).

6. Enter values for the ***Write File Address***.

(The Write File Address indicates the specific memory location within the tag where the HS500E will write data).

7. Enter a number between 5 and 6000 to indicate the number of ticks for the ***Write Heartbeat Timeout***. One tick equals 10ms.

Read Settings

8. Specify the number of words (between 1 and 200) for the ***Max Read Size***.

(The Max Read Size is the maximum number of words the Industrial Antenna will attempt to retrieve from PLC memory during a single command-response cycle).

9. Specify a ***Read Tag Name*** that is 40 characters or less.

(The Read Tag Name is the name assigned to the tag in the PLC where the HS500E will retrieve data from).

10. Enter values for the ***Read File Address***.

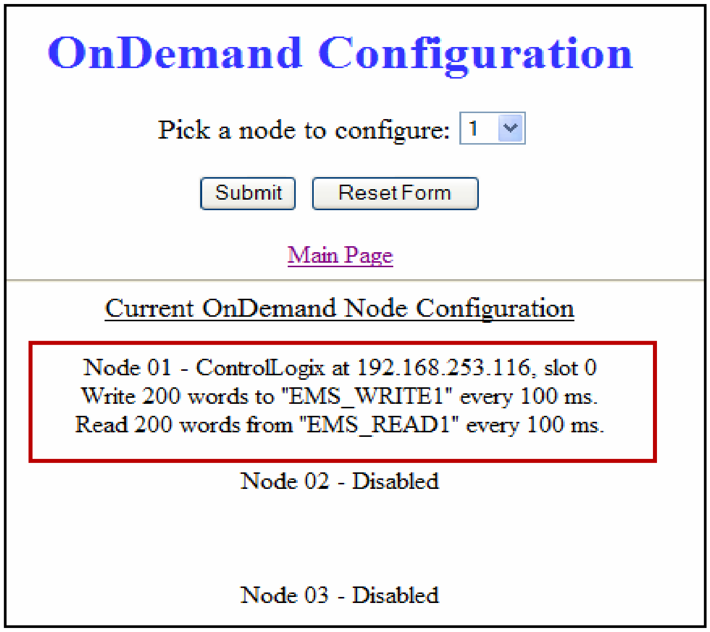
(The Read File Address is the specific memory location within the tag from which the HS500E will retrieve command directed data).

11. Enter a value between 5 and 6000 to indicate the number of ticks for the ***Read Poll Rate***. One tick equals 10ms.

(Read Poll Rate indicates the frequency at which the HS500E will poll tags in PLC memory. Polling is the act of repeatedly querying specific memory locations for the presence of new data).

12. After you have entered the proper information on this page, click the “SAVE SETTINGS” button.

Your changes will be stored and the OnDemand Configuration summary page will be displayed.



OnDemand Configuration

Pick a node to configure: 1

Current OnDemand Node Configuration

Node 01 - ControlLogix at 192.168.253.116, slot 0
Write 200 words to "EMS_WRITE1" every 100 ms.
Read 200 words from "EMS_READ1" every 100 ms.

Node 02 - Disabled

Node 03 - Disabled

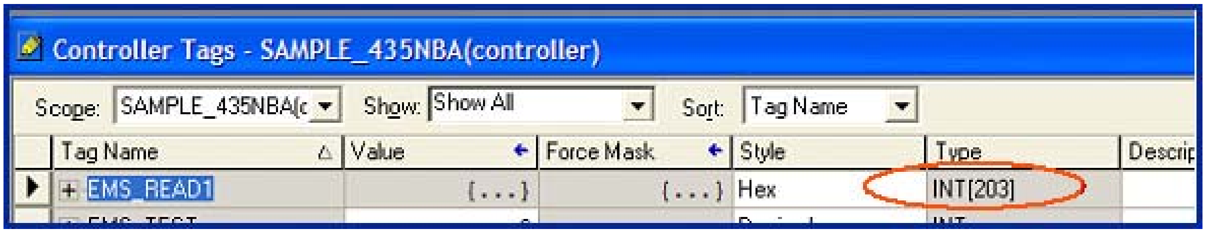
The OnDemand Website - OnDemand Configuration Summary

This page displays a brief configuration summary for the HS500E.

2.4.3 Configuring the PLC

Meanwhile, in your PLC program, define two tags using the same read tag name and write tag name specified earlier (i.e. EMS_READ1 and EMS_WRITE1).

In most PLC programs, the defined tag must have the capacity to store an integer array equal to the *Max Size* + 3 words. For example, if you previously specified 200 words for the Max Read, the capacity of the corresponding Read Tag in the PLC must be able to store an array of 203 integers.



Controller Tags - SAMPLE_435NBA(controller)

Scope: SAMPLE_435NBA(c Show: Show All Sort: Tag Name

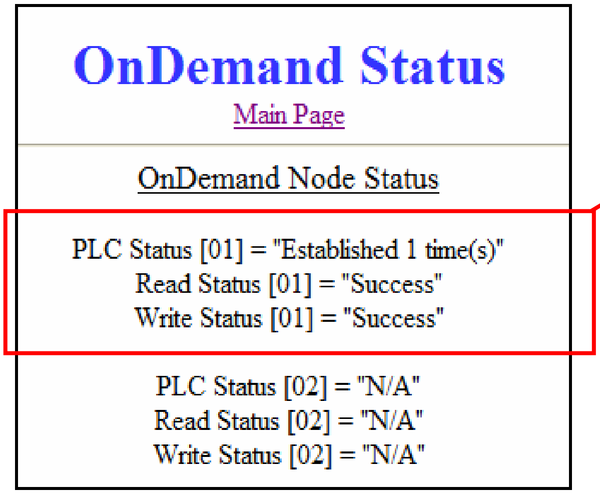
Tag Name	Value	Force Mask	Style	Type	Descrip
+ EMS_READ1	{...}	{...}	Hex	INT[203]	

2.5 CHECKING COMMUNICATION STATUS

2.5.1 Checking the OnDemand Status Page

After configuring the HS500E's Node (via OnDemand) and defining the two "tags" in the PLC, your next step is to check the communication status between the HS500E and the PLC.

- Back at the *OnDemand Website - Main Page*, click the link labeled: "OnDemand Status." The OnDemand Status page will be displayed.



OnDemand Status

Main Page

OnDemand Node Status

PLC Status [01] = "Established 1 time(s)"
Read Status [01] = "Success"
Write Status [01] = "Success"

PLC Status [02] = "N/A"
Read Status [02] = "N/A"
Write Status [02] = "N/A"

This message indicates that the PLC has established a connection with Node 01 on the HS500E.

The OnDemand Website – OnDemand Status Page

The OnDemand Status page provides limited diagnostic information regarding the connection status between the PLC and the HS500E. Using this page, however, you can verify that a connection between the PLC and HS500E has been established successfully.

CAUTION:

If the PLC and HS500E do not establish a successful connection (as depicted in the image above) restart the Ethernet/IP server on the PLC. If that does not resolve the issue, try cycling power to the HS500E and verify that the PLC and the 1756-ENBT module are functioning and that Ethernet/IP services are running properly.

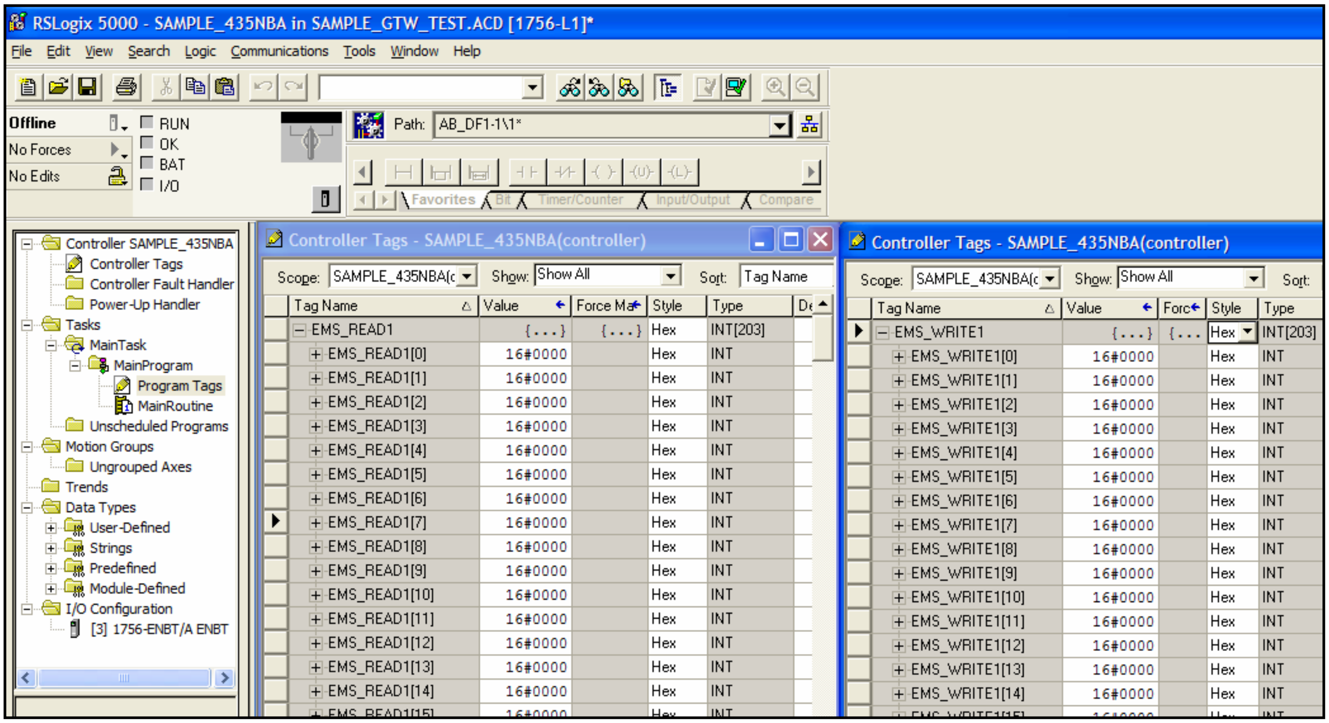
2.6 VERIFYING THE EXCHANGE OF DATA VIA RSLOGIX 5000

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 the two devices using RSLogix 5000.

Start the RSLogix program and (if you have not done so already) define two tags (EMS_READ1 and EMS_WRITE1) using the same settings you specified earlier in the OnDemand Configuration section of this guide.

- **EMS_READ1** is the name of the tag in which the PLC will place commands intended for HS500E (which is assigned to Node 01).
- **EMS_WRITE1** is the name of the tag in which the HS500E will place PLC-bound response data generated after the execution of a command.

NOTE: in RSLogix, “**tag**” refers to 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.”



Controller Tags - SAMPLE_435NBA(controller)

Scope: SAMPLE_435NBA(c Show: Show All Sort: Tag Name

Tag Name	Value	Force Ma	Style	Type	De
EMS_READ1	{...}	{...}	Hex	INT[203]	
EMS_READ1[0]	16#0000		Hex	INT	
EMS_READ1[1]	16#0000		Hex	INT	
EMS_READ1[2]	16#0000		Hex	INT	
EMS_READ1[3]	16#0000		Hex	INT	
EMS_READ1[4]	16#0000		Hex	INT	
EMS_READ1[5]	16#0000		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	
EMS_READ1[14]	16#0000		Hex	INT	
EMS_READ1[15]	16#0000		Hex	INT	

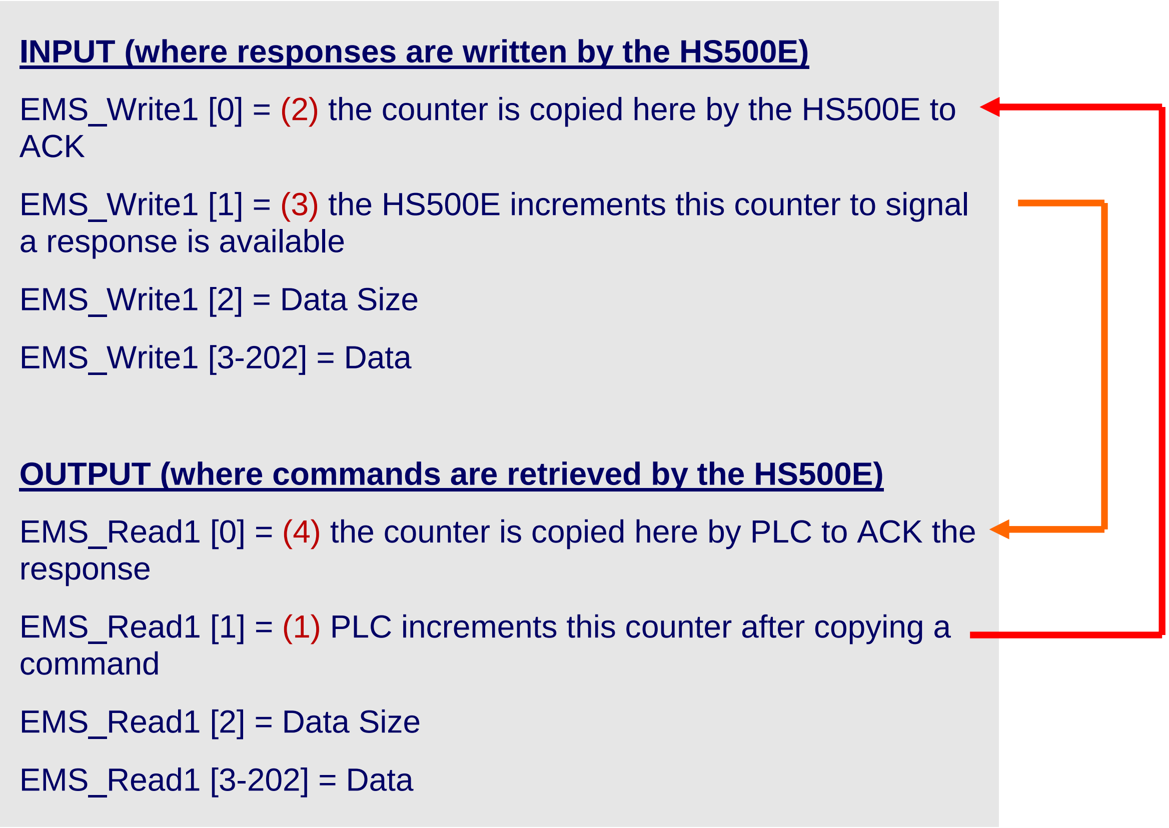
Controller Tags - SAMPLE_435NBA(controller)

Scope: SAMPLE_435NBA(c Show: Show All Sort:

Tag Name	Value	Forc	Style	Type
EMS_WRITE1	{...}	{...	Hex	INT[203]
EMS_WRITE1[0]	16#0000		Hex	INT
EMS_WRITE1[1]	16#0000		Hex	INT
EMS_WRITE1[2]	16#0000		Hex	INT
EMS_WRITE1[3]	16#0000		Hex	INT
EMS_WRITE1[4]	16#0000		Hex	INT
EMS_WRITE1[5]	16#0000		Hex	INT
EMS_WRITE1[6]	16#0000		Hex	INT
EMS_WRITE1[7]	16#0000		Hex	INT
EMS_WRITE1[8]	16#0000		Hex	INT
EMS_WRITE1[9]	16#0000		Hex	INT
EMS_WRITE1[10]	16#0000		Hex	INT
EMS_WRITE1[11]	16#0000		Hex	INT
EMS_WRITE1[12]	16#0000		Hex	INT
EMS_WRITE1[13]	16#0000		Hex	INT
EMS_WRITE1[14]	16#0000		Hex	INT
EMS_WRITE1[15]	16#0000		Hex	INT

A screen shot of RSLogix 5000

Most likely, you will not be required to add a new module under the 1756-ENBT entry in RSLogix. Through the use of OnDemand communication, the Industrial Gateway acts as an Ethernet/IP client and the PLC acts as the Ethernet/IP server. The Gateway periodically reads from and writes to portions of the PLC memory directly with no messaging instructions or polling required on the part of the PLC.



INPUT (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 [3-202] = Data

OUTPUT (where commands are retrieved by the HS500E)

EMS_Read1 [0] = (4) the counter is copied here by PLC to ACK the response

EMS_Read1 [1] = (1) PLC increments this counter after copying a command

EMS_Read1 [2] = Data Size

EMS_Read1 [3-202] = Data

2.6.1 Handshaking

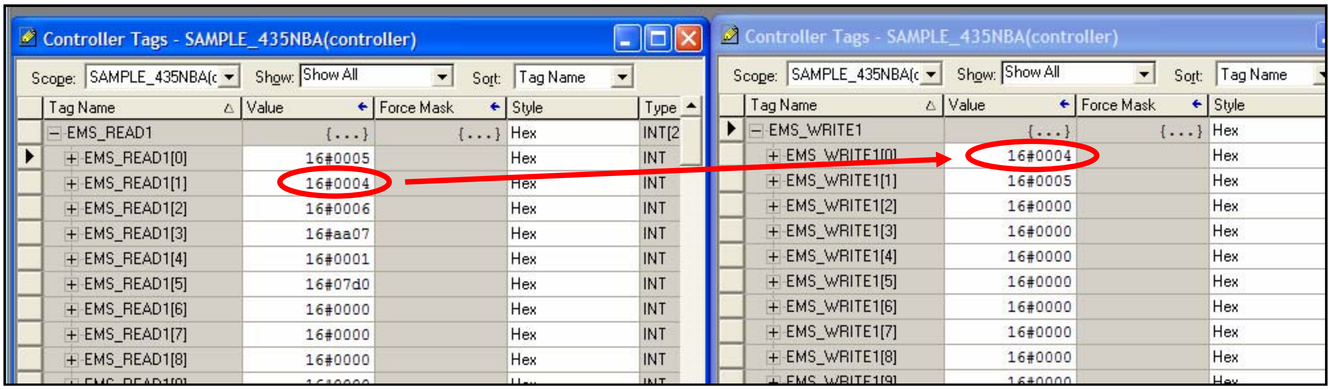
To ensure that messages to and from an HF-Series Controller are properly delivered and received, a handshaking mechanism has been implemented that uses a pair of dedicated words in the exchange. The first 2 words in each tag are dedicated to handshaking.

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.

2.6.2 Handshaking Example

The example below gives a simplified explanation of the handshaking scheme.

1. The PLC copies the command to the Output area 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 of the command.



Controller Tags - SAMPLE_435NBA(controller)

Scope: SAMPLE_435NBA(c Show: Show All Sort: Tag Name

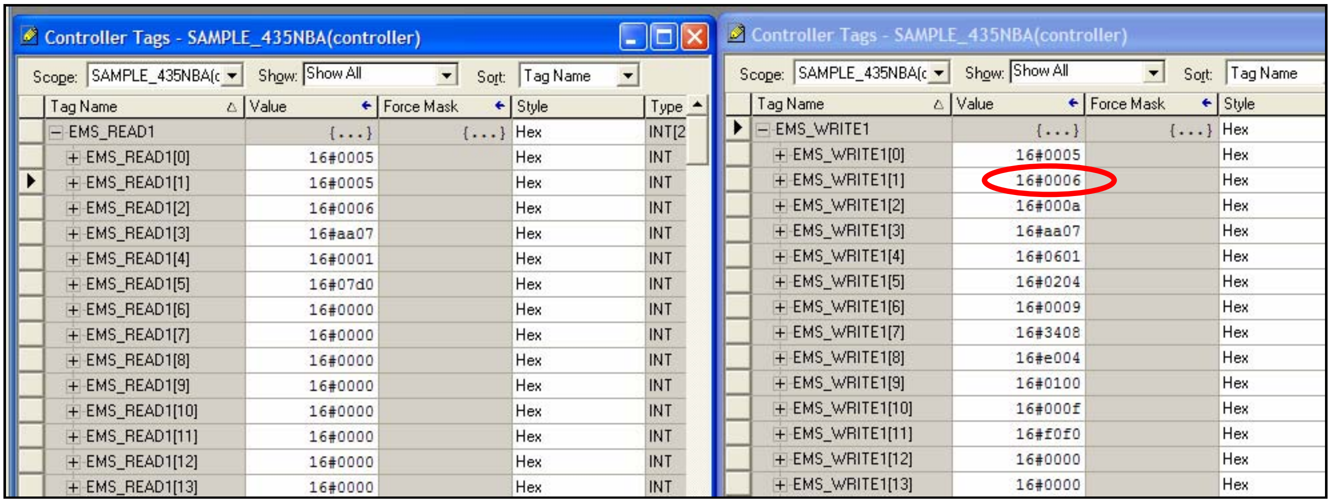
Tag Name	Value	Force Mask	Style	Type
EMS_READ1	{...}	{...}	Hex	INT[2
EMS_READ1[0]	16#0005		Hex	INT
EMS_READ1[1]	16#0004		Hex	INT
EMS_READ1[2]	16#0006		Hex	INT
EMS_READ1[3]	16#aa07		Hex	INT
EMS_READ1[4]	16#0001		Hex	INT
EMS_READ1[5]	16#07d0		Hex	INT
EMS_READ1[6]	16#0000		Hex	INT
EMS_READ1[7]	16#0000	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

Controller Tags - SAMPLE_435NBA(controller)

Scope: SAMPLE_435NBA(c Show: Show All Sort: Tag Name

Tag Name	Value	Force Mask	Style
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

3. The HS500E places the response in the write area and then increments the counter in EMS_WRITE1 [1] which signals that there is new information for the PLC (the RFID controller's command response).



Controller Tags - SAMPLE_435NBA(controller)

Scope: SAMPLE_435NBA(c Show: Show All Sort: Tag Name

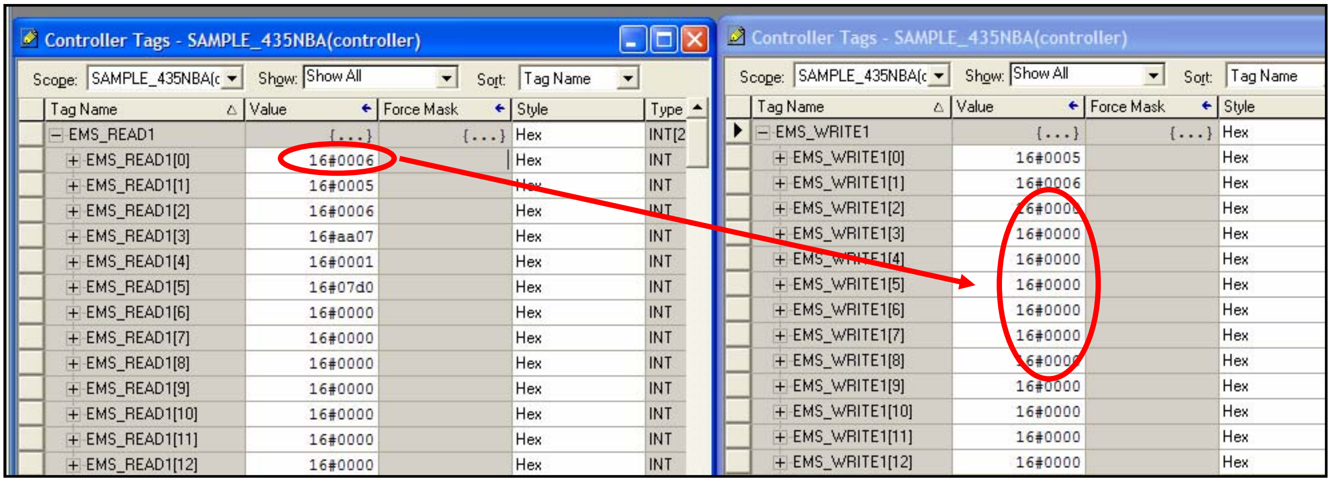
Tag Name	Value	Force Mask	Style	Type
EMS_READ1	{...}	{...}	Hex	INT[2
EMS_READ1[0]	16#0005		Hex	INT
EMS_READ1[1]	16#0005		Hex	INT
EMS_READ1[2]	16#0006		Hex	INT
EMS_READ1[3]	16#aa07		Hex	INT
EMS_READ1[4]	16#0001		Hex	INT
EMS_READ1[5]	16#07d0		Hex	INT
EMS_READ1[6]	16#0000		Hex	INT
EMS_READ1[7]	16#0000	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

Controller Tags - SAMPLE_435NBA(controller)

Scope: SAMPLE_435NBA(c Show: Show All Sort: Tag Name

Tag Name	Value	Force Mask	Style
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 found in EMS_WRITE1 [1] to the read area in EMS_READ1 [0] which signals (to the HS500E) that the PLC has read the response data.



Controller Tags - SAMPLE_435NBA(controller)

Scope: SAMPLE_435NBA(c Show: Show All Sort: Tag Name

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

Controller Tags - SAMPLE_435NBA(controller)

Scope: SAMPLE_435NBA(c Show: Show All Sort: Tag Name

Tag Name	Value	Force Mask	Style
⊟ EMS_WRITE1	{...}	{...}	Hex
⊞ EMS_WRITE1[0]	16#0005		Hex
⊞ EMS_WRITE1[1]	16#0006		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
⊞ EMS_WRITE1[10]	16#0000		Hex
⊞ EMS_WRITE1[11]	16#0000		Hex
⊞ EMS_WRITE1[12]	16#0000		Hex

5. The HS500E will clear its Write Areas by copying O’s to memory, after which it will be ready to receive another command.

CHAPTER 3: RFID COMMANDS

3.1 COMMAND STRUCTURE

In general, RFID commands sent to the HS500E adhere to a ***6-word*** (12-byte) packet structure, where each *word* within the packet is comprised of 2-bytes, a Most Significant Byte (MSB) and a Least Significant Byte (LSB).

RFID Command Packet Structure

Word #	Description
01	Overall Length (the number of words in the Command Packet, including the Overall Length field).
02	Command ID Number (example: 0xAB03 - Write Data Command). *See RFID Command Table below.*
03	Node ID # (will always be 0x0001 for the HS500E)
04	Timeout Value (indicated in .10 second increments).
05	Start Address (the region of tag memory where the Read/Write operation will begin).
06	Read/Write Length (the number of bytes that are to be Read/Written beginning at the Start Address).

Note: Commands 02, 03 and 05 are prefixed with AB, as in **AB03** (for Command 03). Commands F0, F1, F3 and F4 are appended with 00, as in **F300** (for Command F3). Command F2 is appended with 02, 03 or 05, which designates the type of repetitive command. For example, **F202** indicates a *Repetitive Read Data* command.

3.2 RFID COMMANDS

The first three commands in the table below, Commands (AB) 02, 03 and 05, instruct the HS500E to perform standard RFID operations such as data reads, writes and fills.

Commands F0 (00), F1, F3 and F4 are used to retrieve or modify information stored internally within the HS500E Ethernet Antenna.

Command F2 is designed to continuously repeat one of the first three commands (Continuous Read, Continuous Write, or Continuous Fill).

RFID Commands Table

Command ID	Command Name	Description
0xAB02	Read Data	Reads data from contiguous areas of an RFID tag's memory.
0xAB03	Write Data	Writes data to contiguous areas of an RFID tag's memory.
0xAB05	Fill Tag	Fills a specified area of a tag with a single data byte value.
0xF000	Read HS500E Info	Retrieves the software version number from the Ethernet Antenna.
0xF100	Test LEDs / Read HS500E Info	Runs an LED test and retrieves the software version number from the Ethernet Antenna.
0xF2(XX)	Start/Stop Repetitive Command	Starts (or stops) the repetitive execution of a command. (Where XX represents Commands 02, 03 or 05 for repeating Read, Write of Fill commands).
0xF300	Write IP Address	Writes new IP address configuration settings to the Ethernet Antenna.*
0xF400	Reset Battery Counter Value	Resets the value of a tag's Battery Counter.

* Note: Besides executing Command F3, the HS500E's IP address configuration settings can also be modified by accessing the unit's internal Web browser and integrated Web configuration pages (see section "2.4 - OnDemand Configuration"). Through the use of a Web browser, one can directly access the HS500E's internal configuration parameters and manually modify the IP address settings of the HS500E.

COMMAND 02: READ DATA

DESCRIPTION

Command 02 instructs the Ethernet Antenna to ***Read Data*** from a contiguous area of an RFID tag's memory.

DISCUSSION

The Read Data command is used to read a specified number of bytes from contiguous areas of tag memory. This command consists of the Overall Length (OAL), the Command ID Number, a Timeout Value, a 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 that tag address 0x0000 contains a 1-byte Battery Counter Value. To retrieve this value, the Start Address should be set to 0x0000.

EXAMPLE

In the example below, the Ethernet Antenna will read 4-bytes from the tag beginning at the 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 from Host

Command 02: Read Data – Command Structure			
Field Name	**MSB**	**LSB**	**Word Value**
Overall Length (in words)	00	06	0006
[0xAB] + Command ID Number	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

Response from HS500E

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 Echo
	00	02	0002

MSB = Instance Counter
LSB = Node ID Echo
	00	01	0001

RF Time	XX	XX	XXXX

MSB = RF Retry Counter
LSB = Syntax Error Counter
	01	01	0101

Total Time	YY	YY	YYYY
Return Data (bytes 1, 2)	Data	Data	DATA
Return Data (bytes 3,4)	Data	Data	DATA

- **RF Error Counter** – the number of times that an RF transmission could not be completed.
- **Command Echo** – the Command ID Number returned in the LSB of the second word (this byte may also indicate an error code).
- **Instance Counter** - the first response following power-up will return an Instance Counter value of 0xFF. Additional responses will increment this counter by one (range: 0x00 to 0x7F).
- **RF Time** – the remaining portion of the Timeout Value after the completion of the command.
- **RF Retry Counter** – the number of RF packets that required re-transmission to successfully complete the given command.
- **Syntax User Counter** – the number of improperly formatted commands.
- **Total Time** – the interval of time required to complete the command and response.
- **Return Data** – contains the data that was requested in the command. If an odd number of bytes are retrieved, the LSB of the final Return Data word will contain 0x00.

Command 03: Write Data

DESCRIPTION

Command 03 instructs the Ethernet Antenna to ***Write Data*** to contiguous areas of an RFID tag's memory.

DISCUSSION

This command is used to write segments of data to contiguous addresses of tag 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. When an odd number of bytes are to be written, the LSB of the final Data Byte Value word must contain 0x00.

- **Start Address**: 0x0001 = Starts writing to the first accessible byte of tag memory (byte 0x0000 is reserved for the Battery Counter byte).
- **Write Length**: 0x0001 = 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 code.

EXAMPLE

In this example, the Write Data command will instruct the HS500E to write the specified 8 bytes to the tag beginning at the Start Address of 0x0001. A Timeout value of 5 seconds is set for the completion of this command.

Command from Host

Command 03: Write Data – Command Structure			
Field Name	**MSB**	**LSB**	**Word Value**
Overall Length	00	0A	000A
[0xAB] + Command ID Number	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	08	0008
Data Byte Values (01, 02)	11	22	1122
Data Byte Values (03, 04)	33	44	3344
Data Byte Values (05, 06)	55	66	5566
Data Byte Values (07, 08)	77	88	7788

Response from HS500E

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
	00	01	0001

RF Time	XX	XX	XXXX

MSB = RF Retry Counter
LSB = Syntax Error Counter
	01	01	0101

Total Time	YY	YY	YYYY

COMMAND 05: FILL TAG

DESCRIPTION

Command 05 writes one byte of data across a specified range of tag memory.

DISCUSSION

This command 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 Ethernet Antenna will write the ASCII character “D” (0x44) to 8-bytes of tag memory starting at address 0x0001. A Timeout Value of 5 seconds is set for the completion of this command.

Command from Host

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

Response from HS500E

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
	00	01	0001

RF Time	XX	XX	XXXX

MSB = RF Retry Counter
LSB = Syntax Error Counter
	01	01	0101

Total Time	YY	YY	YYYY

Command F0: Read HS500E Information

DESCRIPTION

Command F0 retrieves the currently installed software version number from the HS500E.

DISCUSSION

This command queries the Ethernet Antenna's flash memory and retrieves its software version number.

EXAMPLE

In this example the software version number (1.0A.8) will be retrieved from the EHS500E. (Note: the "period" between characters is also considered part of the software version number).

Timeout Value, Start Address and Read/Write Length are not applicable for this command, default value for each = 0x00, 0x00.

Command from Host

Command F0: Read HS500E Information – Command Structure			
Field Name	**MSB**	**LSB**	**Word Value**
Overall Length	00	06	0006
Command ID Number + [0x00]	F0	00	F000

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

Response from HS500E

Command F0: Read HS500E Information – Response Structure

Field Name	MSB	LSB	Word Value
Overall Length	00	06	0006

MSB =RF Error Counter
LSB = Command ID Echo
	00	F0	00F0

MSB = Instance Counter
LSB = Node ID Echo
	00	01	0001

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 for this example is 1.0A.8, which is a Hex representation of the ASCII string **31 2E 30 41 2E 38**.

Command F1: Test LEDs / Read HS500E Information

DESCRIPTION

Command F1 tests the HS500E's LEDs and also retrieves its software version number.

DISCUSSION

This command causes the Ethernet Antenna's LEDs to flash a coded diagnostic pattern while also retrieving the installed software version number.

EXAMPLE

In this example the LEDs on the Ethernet Antenna will be tested and its software version number will be retrieved. Timeout Value, Start Address and Read/Write Length parameters are not applicable.

Command from Host

Command F1: Test LEDs / Read HS500E Information – Command Structure

Field Name	MSB	LSB	Word Value
Overall Length	00	06	0006
Command ID Number + [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

Response from HS500E

Command F1: Test LEDs / Read HS500E Information – 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
	00	01	0001

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 for this example is 1.0A.8, which is a Hex representation of the ASCII string **31 2E 30 41 2E 38**.

COMMAND F2: START/STOP REPETITIVE COMMAND

DESCRIPTION

Command F2 repeatedly issues a specified RFID command.

DISCUSSION

This command will instruct the Ethernet Antenna to continuously repeat a specified RFID command. Note that not all RFID commands support the ability to be continuously repeated. Only Commands 02, 03 and 05 support continuous repetition.

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 Ethernet Antenna to repeatedly read 4-bytes of data from address 0x0001 of the tag's memory.

Command from Host

Command F2: Repeat Command (Read Data) – Command Structure

Field Name	MSB	LSB	Word Value
Overall Length	00	06 + number of additional words (Write and Fill Commands only). To stop, set LSB to 0x00.	0006
MSB = Repeat Command Flag (always 0xF2) LSB = Command ID Number to be repeated	F2	02 (03 or 05 for Write and Fill Repeat)	F202
MSB = 0x00 for this command when second word = F202 or F203. MSB is used to indicate Fill Data Byte Value when second word is 0xF205. LSB = Node Number – will always be 0x01 for the HS500E	00	01	0001
Timeout Value	00	32	0032
Start Address	00	01	0001
Read/Write Length	00	04	0004

Data Byte Value(s) for Write (only applicable when word 2 is F203.	ZZ	ZZ	ZZZZ

Response from HS500E

Command F2: Repeat Command (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
	00	01	0001

RF Time	XX	XX	XXXX

MSB = RF Retry Counter
LSB = Syntax Error Counter
	YY	YY	YYYY

Total Time	ZZ	ZZ	ZZZZ
Return Data (bytes 1, 2)*	Data	Data	DATA
Return Data (bytes 3,4)*	Data	Data	DATA

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

Command F3: Write IP Address

DESCRIPTION

Command F3 writes a new IP Address to the HS500E.

DISCUSSION

This command is used to assign a new IP Address to the HS500E.

Writing an IP Address to 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 (ModBus/TCP or Ethernet/IP) to connect to the new IP address (that was assigned to the HS500E in step 1).

EXAMPLE

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

Command from Host

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 session (and therefore the connection with the Host) is terminated.

COMMAND F4: RESET BATTERY COUNTER VALUE

DESCRIPTION

Command F4 resets the value of a tag's Battery Counter to zero (0x00).

DISCUSSION

This command is used to reset the value of the Battery Counter when replacing the batteries in a tag. The Battery Counter stores a one-byte value located at tag address 0x0000. To retrieve the Battery Counter Value, execute Command 02 and note the value stored at address 0x0000 on the tag.

Clearing the Battery Counter Value does not add voltage to the battery. Falsifying battery life by clearing the Battery Counter Value may lead to incorrect battery life values. Reading address ZERO on the tag should be performed by only one station in a typical assembly line. A tag should have its batteries replaced after it has accumulated over 15 hours of use. When this value reaches 0x0F, battery life is in a condition of decay and should be replaced.

Command from Host

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 read the tag at 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 was unable to complete a command. The MSB of the second word (Command Echo word) of the response will contain a 1-byte error code indicating the error that was experienced.

BASIC ERROR TYPES

There are three basic types of error codes.

1. Component failure or damage that may inhibit module usage. An example of this type of error can be a blown fuse.
2. User syntax command error (0x88). This type of error occurs when the user issues an invalid command or attempts to read/write/fill to areas that are not within the range of the tag memory limits.
3. RF response errors. This type of error can occur if the distance from the tag to the antenna exceeds the RF range.

Overall Length Errors

0x89: Overall Length Errors:

1. User sends a command with an overall length value of less than 6 bytes.
2. User miscalculates overall length when executing a Write command (where multiple Data Byte Values are to be written).

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 the user decides to read data near the end of the tag and specifies a length that exceeds the remainder of the tag memory.

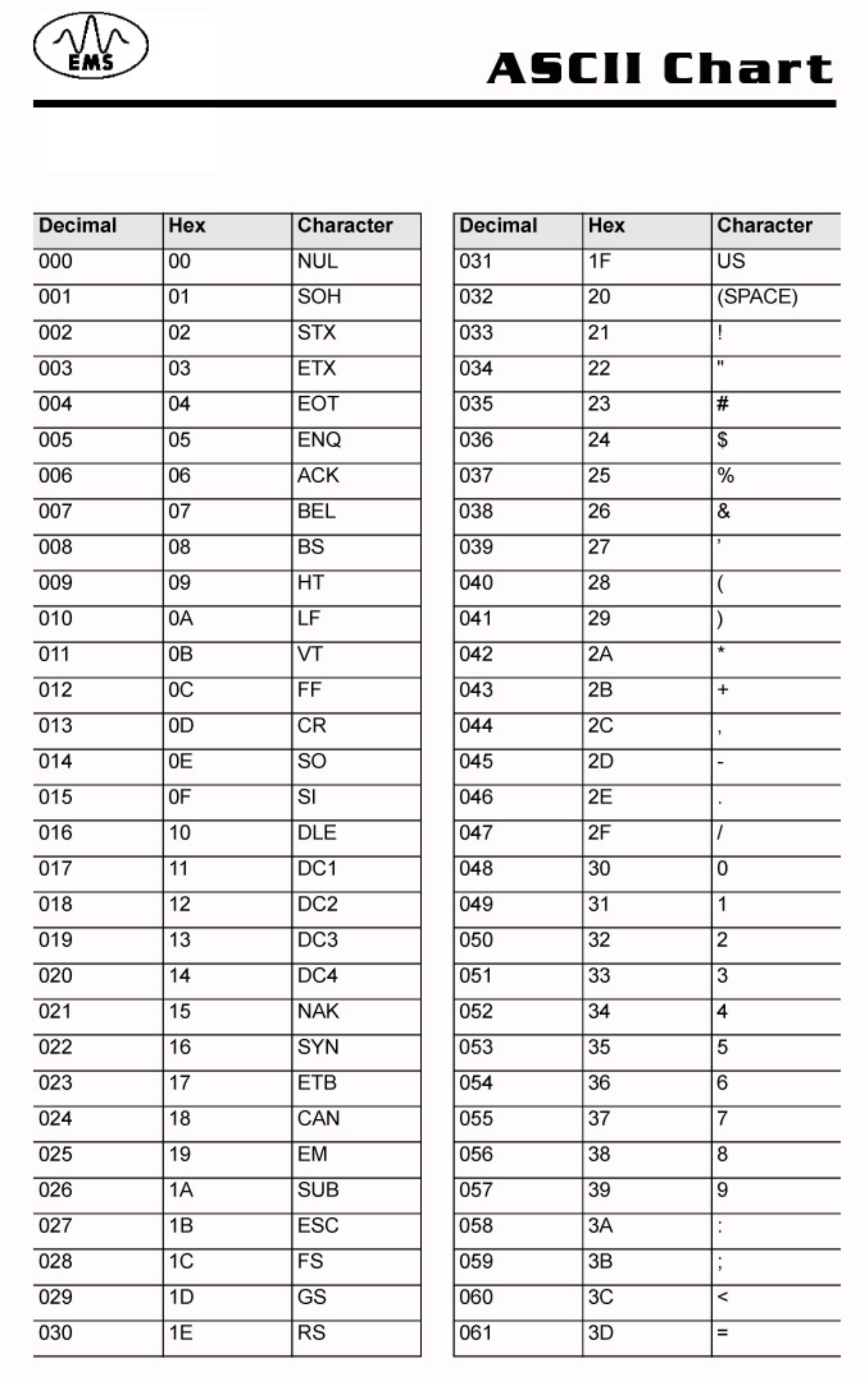
Write Length Limit

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

Timeout Fail Code

0x9F: Timeout Value has been exceeded.

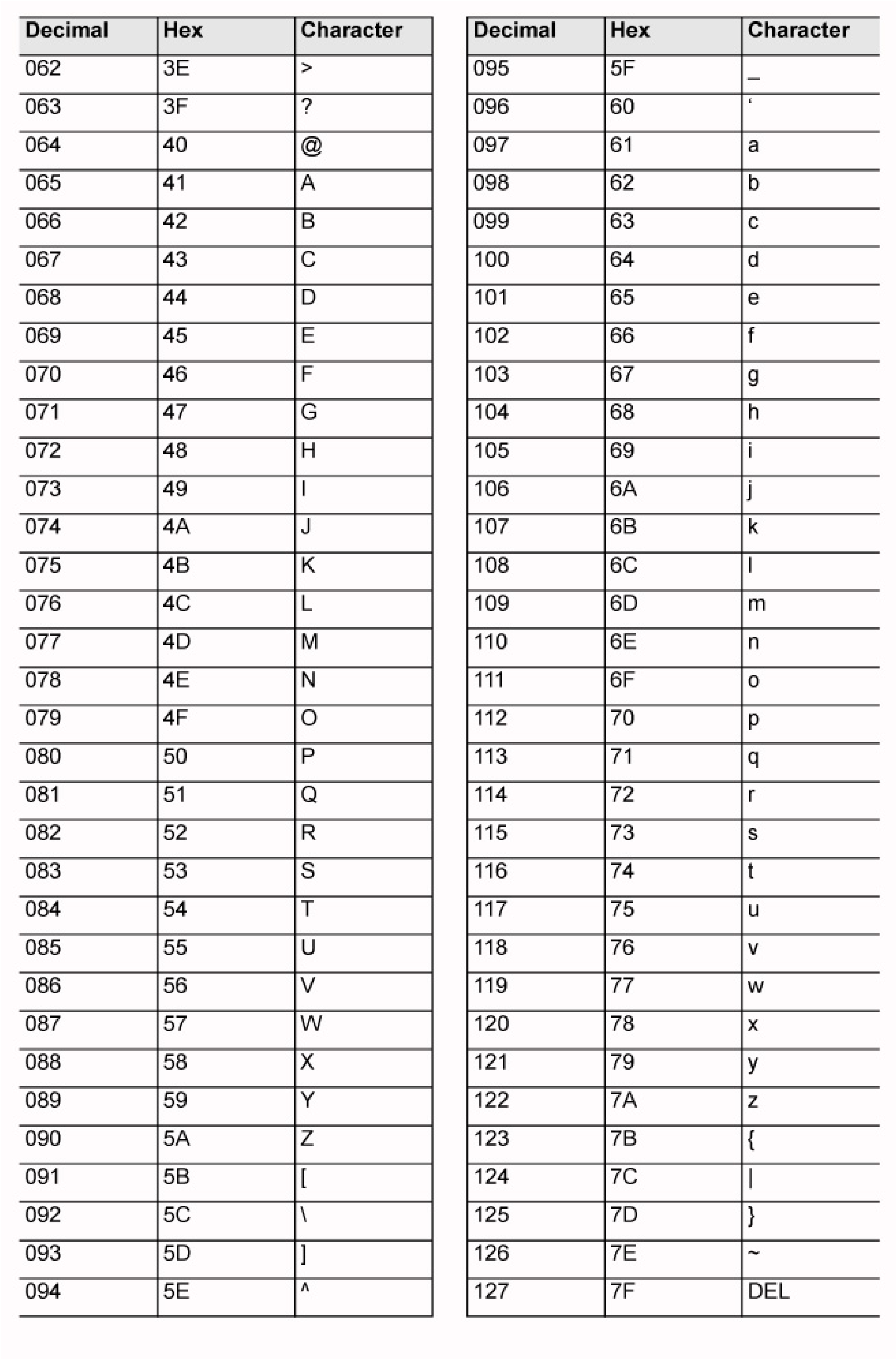
APPENDIX A: ASCII CHART



ASCII Chart

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	=

APPENDIX A: ASCII CHART



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

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 here by 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.

Escort Memory Systems reserves the right to make modifications or improvements 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.

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