WOODWARD

Product Manual 26336
(Revision G, 6/2018)
Original Instructions

Woodward VxWorks®
Real Time Operating System (RTOS)

Software Tools for VxWorks Based Products

Software Manual

General Precautions

Read this entire manual and all other publications pertaining to the work to be performed before installing, operating, or servicing this equipment.

Practice all plant and safety instructions and precautions.

Failure to follow instructions can cause personal injury and/or property damage.

Revisions

This publication may have been revised or updated since this copy was produced. To verify that you have the latest revision, check manual *26455*, *Customer Publication Cross Reference and Revision Status & Distribution Restrictions*, on the *publications page* of the Woodward website:

www.woodward.com/publications

The latest version of most publications is available on the *publications page*. If your publication is not there, please contact your customer service representative to get the latest copy.

Proper Use

Any unauthorized modifications to or use of this equipment outside its specified mechanical, electrical, or other operating limits may cause personal injury and/or property damage, including damage to the equipment. Any such unauthorized modifications: (i) constitute "misuse" and/or "negligence" within the meaning of the product warranty thereby excluding warranty coverage for any resulting damage, and (ii) invalidate product certifications or listings.

Translated Publications

If the cover of this publication states "Translation of the Original Instructions" please note:

The original source of this publication may have been updated since this translation was made. Be sure to check manual *26455*, *Customer Publication Cross Reference and Revision Status & Distribution Restrictions*, to verify whether this translation is up to date. Out-of-date translations are marked with ⚠. Always compare with the original for technical specifications and for proper and safe installation and operation procedures.

Revisions—Changes in this publication since the last revision are indicated by a black line alongside the text.

Woodward reserves the right to update any portion of this publication at any time. Information provided by Woodward is believed to be correct and reliable. However, no responsibility is assumed by Woodward unless otherwise expressly undertaken.

Manual 26336

Contents

The following are trademarks of Woodward, Inc.:

Atlas-II	AtlasPC
505	Flex500
GAP	MicroNet
MicroNet TMR	NetSim
Woodward	

The following are trademarks of their respective companies:
MATLAB/Simulink (The MathWorks, Inc.)
Modbus (Schneider Automation Inc.)
Pentium (Intel Corporation)
The Qt Company (a wholly owned subsidiary of Digia Plc.)
VxWorks (Wind River Systems, Inc.)
Windows (Microsoft Corporation)

Illustrations and Tables

Warnings and Notices

Important Definitions

⚠ This is the safety alert symbol used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

- **DANGER** - Indicates a hazardous situation, which if not avoided, will result in death or serious injury.
- **WARNING** - Indicates a hazardous situation, which if not avoided, could result in death or serious injury.
- **CAUTION** - Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
- **NOTICE** - Indicates a hazard that could result in property damage only (including damage to the control).
- **IMPORTANT** - Designates an operating tip or maintenance suggestion.

⚠WARNING

Overspeed / Overtemperature / Overpressure

The engine, turbine, or other type of prime mover should be equipped with an overspeed shutdown device to protect against runaway or damage to the prime mover with possible personal injury, loss of life, or property damage.

The overspeed shutdown device must be totally independent of the prime mover control system. An overtemperature or overpressure shutdown device may also be needed for safety, as appropriate.

⚠WARNING

Personal Protective Equipment

The products described in this publication may present risks that could lead to personal injury, loss of life, or property damage. Always wear the appropriate personal protective equipment (PPE) for the job at hand. Equipment that should be considered includes but is not limited to:

- **Eye Protection**
- **Hearing Protection**
- **Hard Hat**
- **Gloves**
- **Safety Boots**
- **Respirator**

Always read the proper Material Safety Data Sheet (MSDS) for any working fluid(s) and comply with recommended safety equipment.

⚠WARNING

Start-up

Be prepared to make an emergency shutdown when starting the engine, turbine, or other type of prime mover, to protect against runaway or overspeed with possible personal injury, loss of life, or property damage.

NOTICE

Battery Charging Device

To prevent damage to a control system that uses an alternator or battery-charging device, make sure the charging device is turned off before disconnecting the battery from the system.

Electrostatic Discharge Awareness

NOTICE

Electrostatic Precautions

Electronic controls contain static-sensitive parts. Observe the following precautions to prevent damage to these parts:

- **Discharge body static before handling the control (with power to the control turned off, contact a grounded surface and maintain contact while handling the control).**
- **Avoid all plastic, vinyl, and Styrofoam (except antistatic versions) around printed circuit boards.**
- **Do not touch the components or conductors on a printed circuit board with your hands or with conductive devices.**

To prevent damage to electronic components caused by improper handling, read and observe the precautions in Woodward manual *82715*, *Guide for Handling and Protection of Electronic Controls, Printed Circuit Boards, and Modules*.

Follow these precautions when working with or near the control.

1. Avoid the build-up of static electricity on your body by not wearing clothing made of synthetic materials. Wear cotton or cotton-blend materials as much as possible because these do not store static electric charges as much as synthetics.
2. Do not remove the printed circuit board (PCB) from the control cabinet unless absolutely necessary. If you must remove the PCB from the control cabinet, follow these precautions:
   - Do not touch any part of the PCB except the edges.
   - Do not touch the electrical conductors, the connectors, or the components with conductive devices or with your hands.
   - When replacing a PCB, keep the new PCB in the plastic antistatic protective bag it comes in until you are ready to install it. Immediately after removing the old PCB from the control cabinet, place it in the antistatic protective bag.

Chapter 1.
General Information

General Description

This manual describes the Woodward VxWorks RTOS (Real Time Operating System) software tools available to remotely configure and interact with the MicroNet Plus, 505, Flex500 and Atlas-II control platforms.

The MicroNet Plus, 505, Flex500 and Atlas-II controls are designed so that all interface, maintenance, and troubleshooting is done via the Serial and Ethernet Ports. No local keyboard, monitor, or mouse is available to the user, and thus “headless” operation is accomplished using these tools.

The MicroNet Plus Cyber Secure controls are similar to the MicroNet Plus controls. All exceptions are noted in this manual. The Cyber Secure CPU implements secure file transfers and control communication using SSH encryption.

- The 5466-1045 and 5466-1145, M5200 MicroNet CPUs are Cyber Secure.
- The 5466-1510 P1020 MicroNet CPU is Cyber Secure.
- The 5466-1046 and 5466-1146 RTN_CPUs are Cyber Secure.
- The 8200-1250 gateway and 8200-1253 gateway are Cyber Secure.

The MicroNet Plus Secured Application controls are similar to the MicroNet Plus controls. All exceptions are noted in this manual. A Secured Application prevents execution of the application on unauthorized MicroNet Plus CPUs. A Secured Application also helps to protect recovery of intellectual property through reverse engineering the GAP/Coder output file. The Secured Application CPU is part number 5466-1141. The CPU_MP1020 Secured Application CPU is part number 5466-1520.

IMPORTANT	**Your computer screens may differ slightly from those shown in this manual due to newer software revisions.**

IMPORTANT	**The MicroNet Plus, 505, Flex500 and Atlas-II controls are shipped with static IP addresses! To avoid Ethernet IP Address conflicts, read this manual before connecting the control’s Ethernet Ports to a network.**

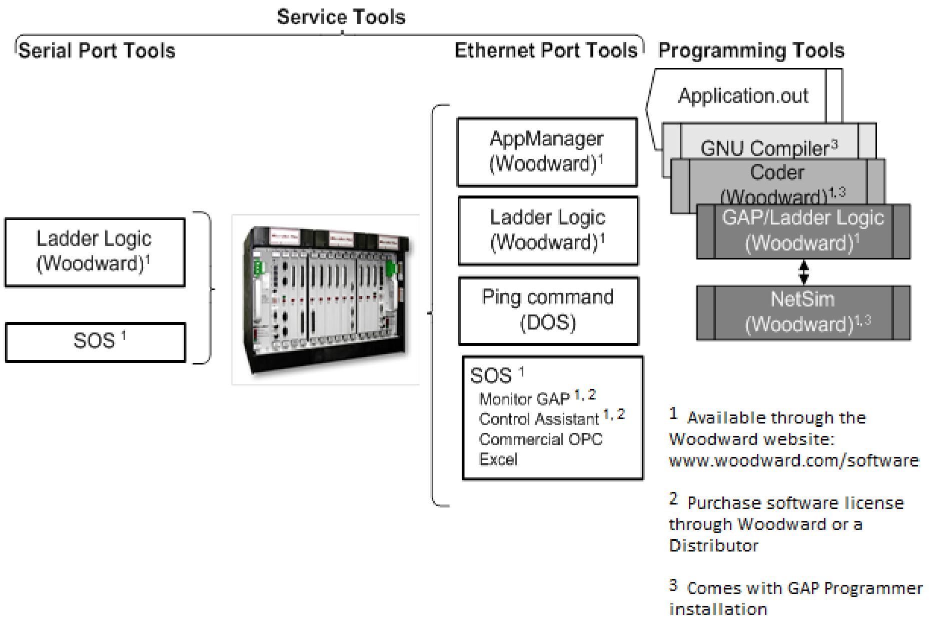
Overview

Programming Tools are used to build a control application. GAP (Graphical Application Programmer) and Ladder Logic are used to create the application. The output is assembled, compiled, and linked with the Coder, and the resulting executable file is loaded into the target control. The Woodward NetSim simulation tool can be used to test the application on a PC.

Service Tools are the interface programs that allow an operator to move files, start and stop the application, configure settings, troubleshoot hardware and software, view status, and ultimately operate the controlled machinery.

See Figure 1-1.

⚠WARNING	**An unsafe condition could occur with improper use of these software tools. Only trained personnel should have access to these tools.**



[1] Available through the Woodward website: www.woodward.com/software

[2] Purchase software license through Woodward or a Distributor

[3] Comes with GAP Programmer installation

Figure 1-1. Software Interface Tools Overview

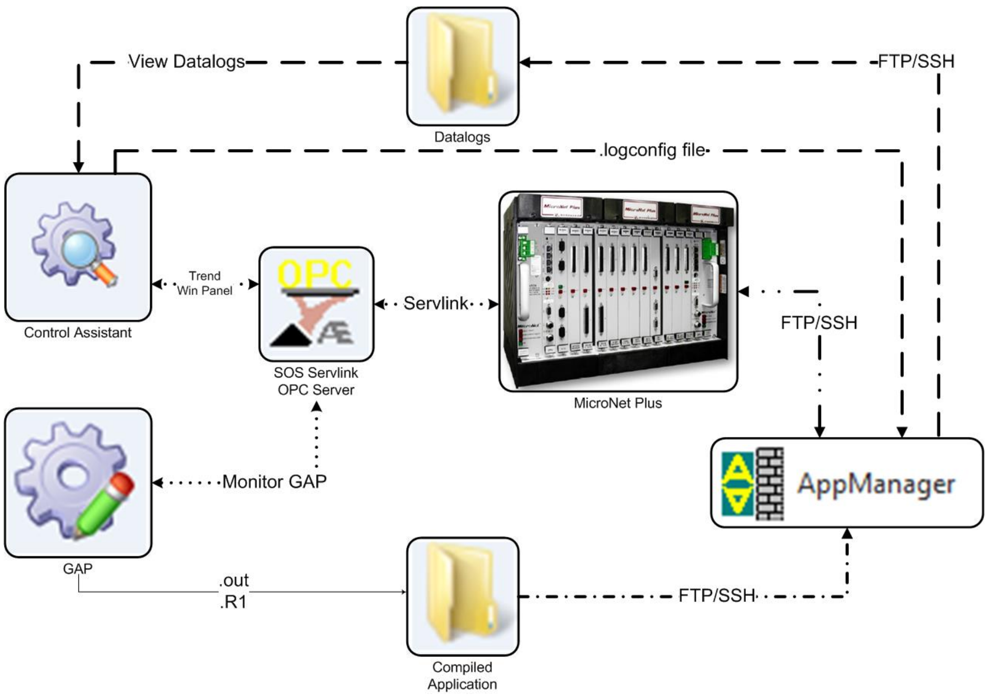


Figure 1-2. Software Tools Connectivity Overview

Programming Tools

These tools are useful for creating new applications or for modifying existing ones.

IMPORTANT

All of the following programming tools will only function in a Windows Operating System such as Windows XP, Vista, 7, 8, or 10. The Windows .NET library version 4.0, which is usually included on such PCs, is required for most of these tools to run.

Woodward GAP

GAP (Graphical Application Programmer) allows users to design their control system logic with an integrated drawing package that runs on a PC in the Windows environment. After graphically entering the control logic, GAP checks the application for correctness and generates a meta-data (.cdr) file for use with Woodward Coder.

Monitor GAP

Monitor GAP is a mode in the GAP program, which allows the engineer to view and tune GAP values in context while the application is running. It interfaces with the Ethernet or serial ports via the Woodward SOS Servlink OPC Server tool.

Woodward Coder

Coder is the program that converts the GAP application into code. If no problems are found, it calls the assembler, compiler, and linker to create the file that can be loaded onto the hardware using AppManager. System created error files assist in debugging if the Coder finds problems.

Secured Application Tool

SAT is a program used to manage Authorization Encryption Files (AEF) and to create Secured Applications from GAP output (.out) files. Secured Applications can only run on Secured Application controls for which they have been programmed.

NetSim

NetSim is Woodward's Windows PC based simulator software used for testing control software. It provides a closed loop simulation environment when connected to a modeling package or open loop testing when run in stand-alone mode. Connections to ACSL based and MATLAB/Simulink modeling packages are supported. The NetSim Control Executive ("NetSim CE") communicates with the Woodward SOS Servlink OPC Server to provide OPC data to tools like Monitor GAP and Control Assistant, which can present it.

Ladder Logic

Woodward Ladder Logic extends a GAP application and permits customer programming and monitoring of a Woodward control. It is easy for anyone familiar with the basic structure of ladder logic to write and use Woodward Ladder Logic. Activate commands by using a simple point and click Windows interface.

The Woodward Ladder Logic program runs on a Windows PC connected to a serial or Ethernet port of a Woodward digital control system. While the hardware is controlling the running prime mover, the Ladder Logic program can be written and changed using the PC. Changes do not take effect until the Ladder Logic program is loaded into the hardware.

IMPORTANT **The MicroNet Plus, 505, Flex500 and Atlas-II controls support only Ladder Logic versions 2.10 or higher.**

Service Tools

These tools are useful for system debugging, variable monitoring, tunable maintenance, real time data collection, data analysis, and remote control. See your Woodward sales engineer for additional information.

IMPORTANT **All of the following service tools will only function in a Windows Operating System such as Windows XP, Vista, 7, 8, or 10. The Windows .NET library version 4.0, which is usually included on such PCs, is required for these tools to run.**

Application Manager

AppManager is a Windows based remote access tool for Woodward CPUs. AppManager allows local and remote access to control applications for transferring files, retrieving files, starting, stopping, and restarting. The MicroNet Plus, 505, Flex500 and Atlas-II are loaded with a service that allows them to interface with AppManager. AppManager can also be used to change Ethernet Network addresses, Administer Accounts, load service packs, and continuously retrieve Datalog files.

IMPORTANT **AppManager will only function in a Windows Operating System such as Windows XP, Vista, 7, 8, or 10.**

Control Assistant

Control Assistant is a Windows program designed to support the following control features via OPC Ethernet communications:

- *Tunable Maintenance:* This feature supports tunable capture, sorting, comparing vs. baseline/GAP, saving, and uploading of new tunable values into the control.
- *Variable Trending:* A strip chart may be used to display live variable information. It requires a software license to run.
- *Datalog Plotting*: This feature supports the capture and plotting of high-speed Datalog information. It requires a software license to run.
- *WinPanel:* An OPC client designed for communication with the Woodward Servlink OPC Server to display and control all control system data. From this interface, variables can be selected for both control and monitoring purposes.
- Variable access through the Servlink OPC Server.
- Loading and saving of different configurations.
- Hierarchical Tree View of available data.
- The WinPanel views support multiple data sheets.
- Tunable modifications.
- Updating of EEPROMs.

Servlink OPC Server (SOS)

The SOS Servlink OPC Server is an OPC server designed to communicate with a control using the Woodward Servlink Protocol over an Ethernet or Serial connection. This protocol allows OPC clients like Control Assistant, Monitor GAP and off-the-shelf HMI programs to access and modify internal control parameters.

ToolKit

ToolKit creates and runs custom administration tools for many Woodward electronic products. Use the resulting tools to configure, calibrate, monitor, and troubleshoot your device over a serial, CAN, or TCP/IP connection.

Obtaining Software Tools

The following software tools are available on the Woodward web site (**www.woodward.com/software**):

- AppManager
  - No license required unless using enterprise version of automatic file retrieval (4+ controls at once)
- Control Assistant
  - License required for graphing/trending features only
- GAP Editor and Monitor
  - Separate licenses required for Editing and Monitoring
- GAP Programmer (Woodward Coder)
  - No license required (license required for GAP Editor)
- Ladder Logic
  - No license required
- NetSim
  - License required
- Secured Application Tool
  - No license required
- SOS Servlink OPC Server
  - No license required
- ToolKit
  - The Basic version requires no license. It may be used to open and work with pre-built tools
  - A Developer license is required for designing custom tools
- Woodward Control Service Packs
  - No license required

Chapter 2.
Setting up the Control

The Woodward control's Computer Name label is located on the top cover of the control. It is unique for each control. It starts with

- "VXM" followed by 8 digits for the MicroNet Plus
- "FLEX" followed by 8 digits for the 505 and Flex500 control
- "VXA" followed by 8 digits for the Atlas-II control

Record the Computer Name:

IMPORTANT **See page 83 for you to record Software Setup Information for future use.**

Factory set IP addresses for the control

Table 2-1. Factory set IP addresses for the MicroNet CPU

Port name	IP address	Subnet Mask
Ethernet #1	172.16.100.1	255.255.0.0
Ethernet #2	192.168.128.20	255.255.255.0
Ethernet #3 (on 6 port CPUs)	192.168.129.20	255.255.255.0
Ethernet #4 (on 6 port CPUs)	192.168.130.20	255.255.255.0
RTN Port #1	172.20.22.10	255.255.255.0
RTN Port #2	172.20.23.10	255.255.255.0
Default Gateway	<none>	

Table 2-2. Factory set IP addresses for the 505 / Flex500 CPU

Port name	IP address	Subnet Mask
Ethernet #1	172.16.100.15	255.255.0.0
Ethernet #2	192.168.128.20	255.255.255.0
Ethernet #3	192.168.129.20	255.255.255.0
Ethernet #4	192.168.130.20	255.255.255.0
Default Gateway	<none>	

Table 2-3. Factory set IP addresses for the Atlas-II CPU

Port name	IP address	Subnet Mask
Ethernet #1	172.16.100.20	255.255.0.0
Ethernet #2	192.168.128.20	255.255.255.0
Ethernet #3	192.168.129.20	255.255.255.0
Ethernet #4	192.168.130.20	255.255.255.0
Default Gateway	<none>	

Factory set network passwords

(See AppManager Help for more information)

The control Operating System enforces security by requiring the user to login with valid permissions before privileged control services can be accessed.

- For controls which do not support account management (older systems), the login is not required until an attempt is made to start or stop an application, or send or retrieve a file.
- For recent control systems, a login is required in order to connect the AppManager tool to the control.

<u>For CPUs which do not support Account Management:</u>

The following login is supported for accessing the control.

Note: The account name and password is case sensitive!

Table 2-4. Factory set account name and password for old controls

Account name	Password	Permissions
ServiceUser	ServiceUser	Read, Write, Execute

<u>For CPUs which support Account Management:</u>

The following logins are the default account settings for accessing the control.

IMPORTANT **The Administrator login is reserved for the system administrator and is only valid when Account Management is enabled**

Use the Administrator account to create, modify, and delete other accounts.

Note: All account names and passwords are case sensitive!

Table 2-5. Factory set account names and passwords for newer controls

Account name	Password	Level	Permissions
Administrator	**Admin@1**	**15**	**Read, Write, Execute**
ServiceUser	**ServiceUser@1**	**11**	**Read, Write, Execute**
Datalog	**Datalog@1**	**1**	**Read**

Network setup instructions for the control

Here is a simple flowchart, which shows the steps for configuring the control's network settings to work on your network. See Tables 2-1, 2-2 and 2-3 above for factory set IP addresses for each control type and the flowchart below for additional detailed instructions:

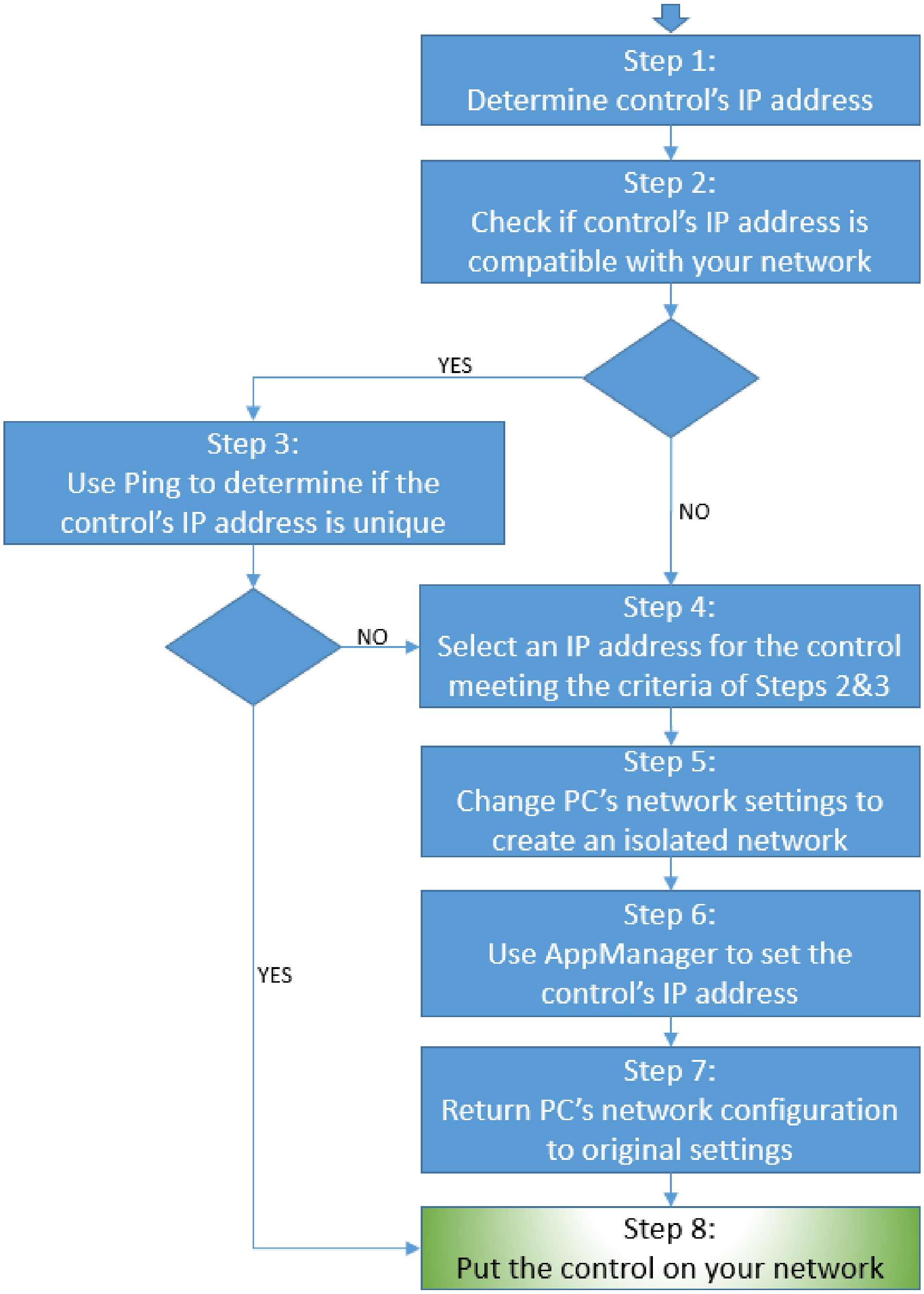

Step 1:
Determine control's IP address
Step 2:
Check if control's IP address is compatible with your network
YES
NO
Step 3:
Use Ping to determine if the control's IP address is unique
NO
YES
Step 4:
Select an IP address for the control meeting the criteria of Steps 2&3
Step 5:
Change PC's network settings to create an isolated network
Step 6:
Use AppManager to set the control's IP address
Step 7:
Return PC's network configuration to original settings
Step 8:
Put the control on your network

Figure 2-1. Network Setup Flowchart

Detailed network procedure for the control

Execute the following steps (up to 8) to configure your control to work with your network. The control's primary IP address must be compatible with your network, and must be unique on your network.

> **NOTE:** More information about networking and a glossary of network terms are available in Chapter 8 Ethernet Networking.

STEP 1:
Get control's current IP address
Determine the current IP address of your control. See "Ethernet #1" in Tables 2-1, 2-2 or 2-3 at the beginning of this chapter for the current address.

STEP 2:
Check control's IP address for network compatibility
Determine if the control's primary IP address is compatible with your network. This compatibility can be determined by looking at the IP address and subnet mask on your PC. These can be viewed by running "ipconfig" from a cmd window on your PC (to open a cmd window, click on "Run…" in the Start menu and type in "cmd"). . You are likely to be interested in the values for the Local Area Connection.

If you translate the Subnet Mask of your PC to binary, you can see which values of the control IP address must match the PC's IP address. For example, if the subnet address is "255.255.0.0", then the first two octets must match:

- **172.16**.99.4 *matches* **172.16**.100.1
- **172.**18.100.1 *does not match* **172.16**.100.2

For example, if the subnet address is "255.255.240.0", then the first two octets must match and the first 4 bits of the third octet must match (240 is 11110000 in binary and "1"s indicate a required bit position match):

- **172.16**.107.4 *matches* **172.16.100**.1 because 110 is "**0110**0100" in binary and 107 is "**0110**1011" in binary
- **172.16**.116.4 *does not match* **172.16.100**.1 because 100 is "**0110**0100" in binary and 116 is "**0111**0100" in binary

If you are not sure what the PC's IP address or subnet mask are or if your network has some other complexity, consult with your network administrator for help in determining or establishing a compatible IP address for the control.

Is the control's primary IP address compatible with the PC's network?
If NO, or if you need to change the network settings for another reason, go to STEP 4 below.
If YES, continue to STEP 3 below.

STEP 3:
Check control's IP address for uniqueness
Determine if the current IP address of your control (from STEP 1) is already used in your network. To see if it is already used, Ping the IP address from a PC on the network. The Ping command is described in Chapter 8 *Ethernet Networking*. If it does not respond with "Destination host unreachable.", the IP address is already used and is not available for the new control. If this is the case, skip to STEP 4 where you will change the control's primary IP address.

Is the control's IP address already in use?
If YES, or if you need to change the network settings for another reason, go to STEP 4 below.
If NO, jump to STEP 8.

STEP 4:
Select a new IP address for the control's Ethernet #1 port
If your network contains many devices, you should consult with your network administrator to find an available IP address for you to claim and use. If your network is simple or you do not have an administrator, you could try guessing a suitable IP address by taking your PC's IP address and changing the final octet to a different number until you find an available IP address (see STEP 3). For example, if your PC's IP address is "10.14.129.37", you could try "10.14.129.38", "10.14.129.39", etc. Keep trying different values until you find one that works.

NOTE: Any IP address you choose must still match the subnet mask of the PC, as described in STEP 2.

STEP 5:
Create an isolated network between the PC and the control

To avoid IP address conflicts on your network, isolate the control and the PC that you will be using for setting up the control from the network. Figure 2-2 shows examples of two recommended methods.

1. On your PC, shut down your network applications but do not log off.
2. Temporarily change your PC’s IP address to be compatible with the current IP address of the control (from STEP 1). A simple compatible IP address would be to take the control’s address and add 1 to the final octet (e.g. use “172.16.100.2” to connect with a control at “172.16.100.1”. Keep a record of your PC’s current IP address.
3. Connect as shown in Figure 2-2 and power up the Woodward control.

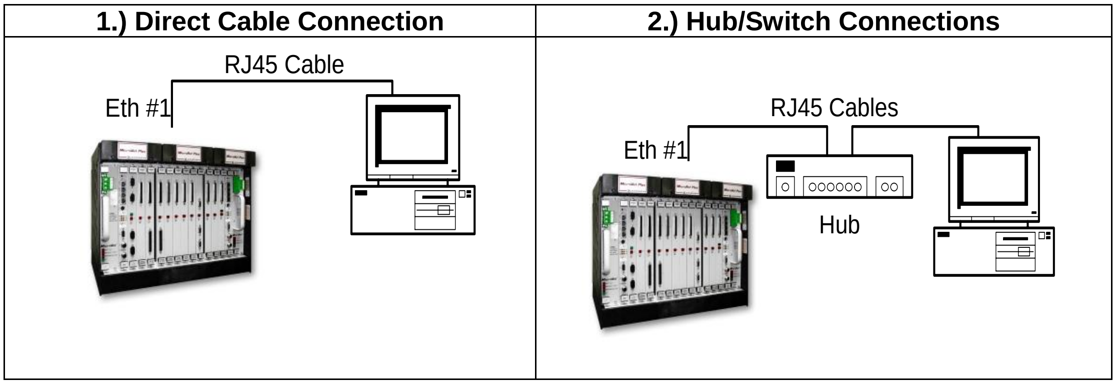


Figure 2-2. Network Cable Connections

- When you have the proper connection between the Woodward control’s Ethernet Port #1 and your PC, you will see the green “Link” LED remain on (solid) on your PC *and* on the control.
- CPUs equipped with six Ethernet ports display link activity as shown in the following table

Table 2-6. Ethernet port blink behavior

Speed	GbE 1/2	ENET 1/2	RTN 1/2
10 Mb/s	Yellow LED blinking	Yellow LED blinking	Yellow LED blinking
100 Mb/s	Green LED blinking	Green LED blinking	Green LED blinking
1000 Mb/s	Green and Yellow LED blinking	N/A	N/A

IMPORTANT

A Hub/Switch will cause your PC’s Link light to be on even when a control is not connected. The MicroNet Plus, 505, Flex500, and Atlas-II have two LEDs for each connector.

IMPORTANT

If you cannot see the control in AppManager, open a DOS Command Prompt window on your PC and try to “ping” the control’s IP address of the port to which you are connected. See the “Pinging the Network” section of the Ethernet Networking chapter. If pinging is successful, your PC’s networking settings may need to be changed. Contact your Network Administrator.

STEP 6:

Configure the Ethernet port

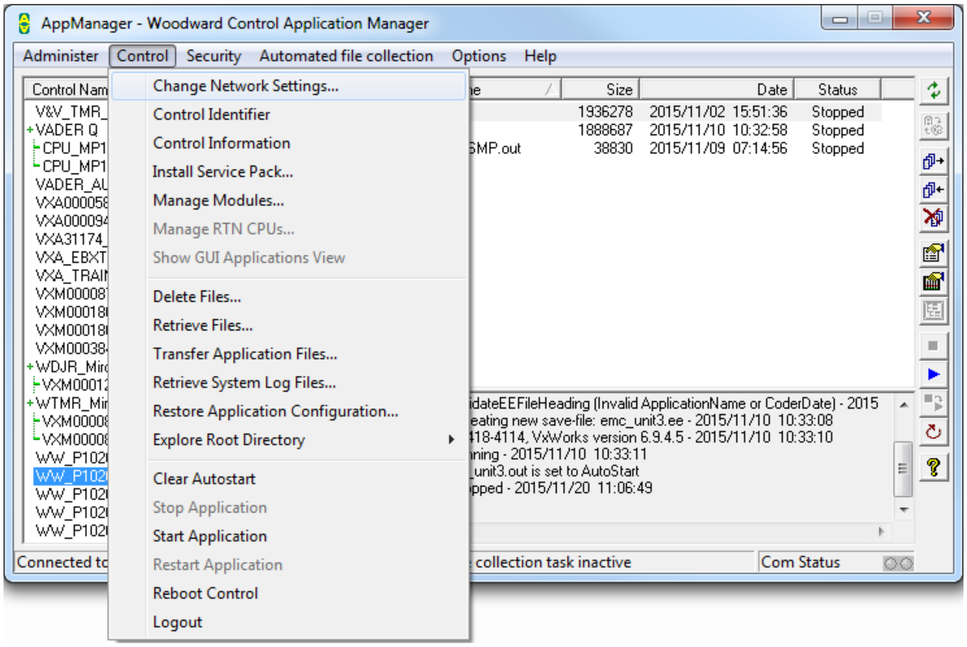
Some Woodward controls (e.g. the 505) have applications that allow the Ethernet IP settings to be changed from within the application. (The procedure below will also work for these controls after stopping all control applications).

For all other controls, the Woodward software tool “AppManager” is needed to change the Woodward control’s Ethernet IP settings to make the control’s Ethernet port accessible to your local PC. This tool can be downloaded from the Woodward website. See Chapter 1, “Obtaining Software Tools” section. Install AppManager on your PC if it is not already there.

Changing an IP address with control on the local network

Use AppManager to change the control network settings following the steps below:

1) On your PC, open AppManager.exe.
2) You should see the Woodward control’s Computer Name in the AppManager window. Select the Computer Name of the control. If necessary, login using the credentials from Tables 2-4 or 2-5. If the control name is not listed, check your connections and verify that the Link lights are on. If clicking on the control produces an error, verify that you have chosen a compatible IP address for your PC in STEP 5.
3) Click “Control” in the top header of the AppManager window, use the pull down menu, and select “Change Network Settings”.

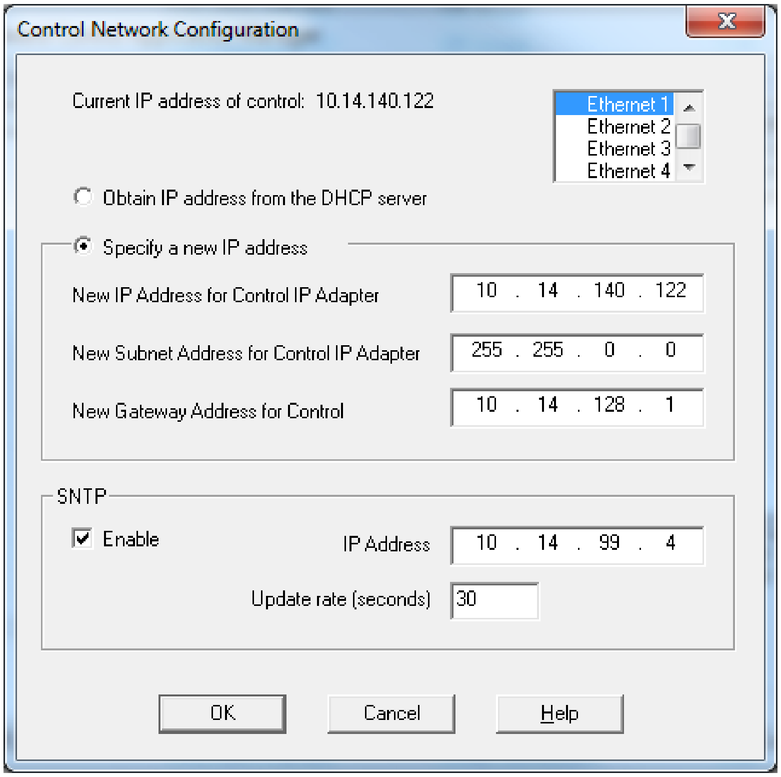


```
ne                  Size        Date                 Status
                 1936278  2015/11/02  15:51:36   Stopped
                 1888687  2015/11/10  10:32:58   Stopped
SMP.out            38830  2015/11/09  07:14:56   Stopped
```

```
idateEEFileHeading (Invalid ApplicationName or CoderDate) - 2015
eating new save-file: emc_unit3.ee - 2015/11/10  10:33:08
418-4114, VxWorks version 6.9.4.5 - 2015/11/10  10:33:10
nning - 2015/11/10  10:33:11
_unit3.out is set to AutoStart
pped - 2015/11/20  11:06:49
```

Figure 2-3. AppManager Control Menu

Select the desired Ethernet port (adapter) and the desired IP Address settings to make desired changes. Port 1 is the only port that supports a Default Gateway, and Port 1 is the only port that supports DHCP. On MicroNet Plus CPUs with six Ethernet ports, Ethernet 3 and Ethernet 4 IP addresses may also be changed.



Control Network Configuration

Current IP address of control: 10.14.140.122

Ethernet 1
Ethernet 2
Ethernet 3
Ethernet 4

○ Obtain IP address from the DHCP server

● Specify a new IP address

New IP Address for Control IP Adapter: 10 . 14 . 140 . 122

New Subnet Address for Control IP Adapter: 255 . 255 . 0 . 0

New Gateway Address for Control: 10 . 14 . 128 . 1

SNTP

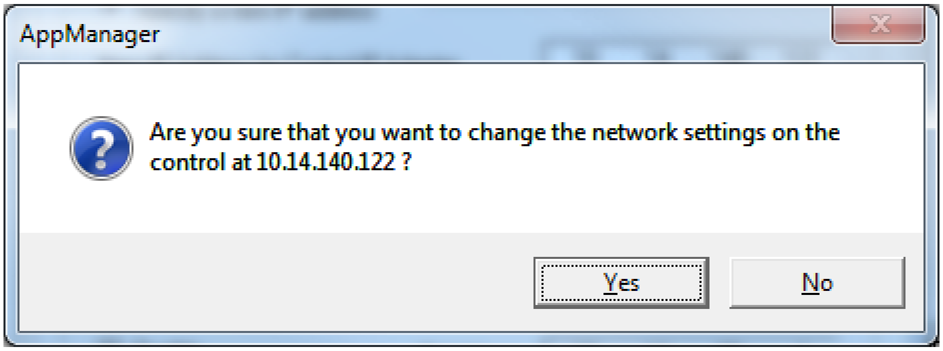
☑ Enable

IP Address: 10 . 14 . 99 . 4

Update rate (seconds): 30

Figure 2-4. Control Network Configuration Page

4) Select “Yes” to change the settings

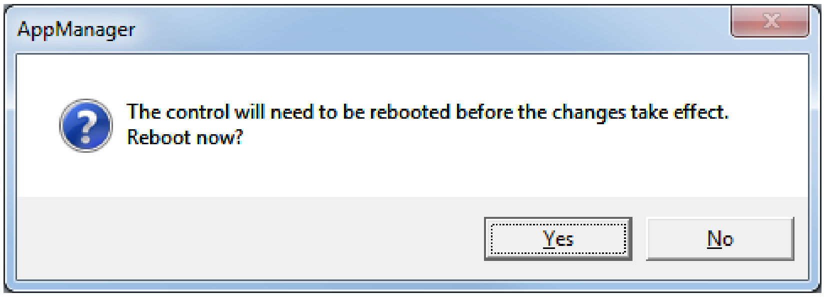


AppManager

Are you sure that you want to change the network settings on the control at 10.14.140.122 ?

Figure 2-5. Change Verification Window

AppManager reports changes in the control settings and prompts the user to reboot the control. Changes will not invoke until the control reboots.



The control will need to be rebooted before the changes take effect.
Reboot now?

Figure 2-6. AppManager Control Reboot Prompt

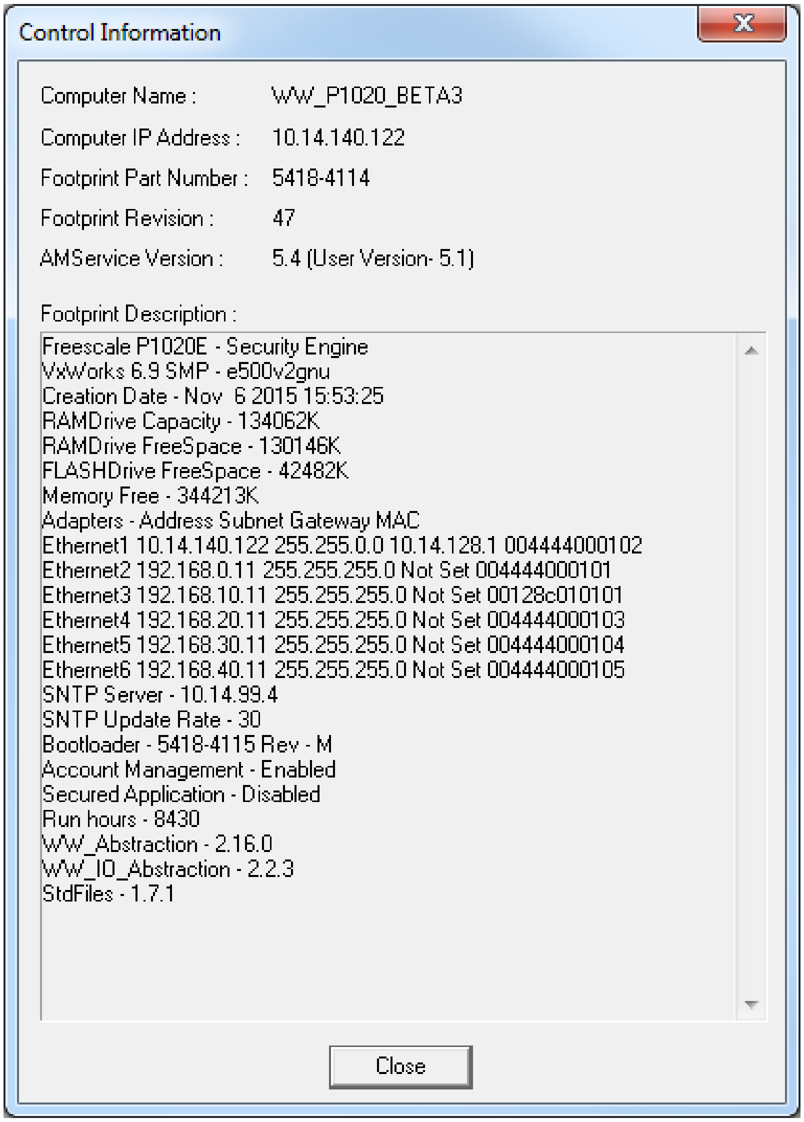
STEP 7:
Configure the PC's network configuration to its original settings
When the control has rebooted, it will have the IP address changes that you specified. This may cause the control incompatibility with your current PC settings. If you had changed your PC network settings, you should now revert to the previous settings. If everything worked correctly, the control will now be compatible with your PC's network.

STEP 8:
Connect the PC and the control to the network
Physically reconnect the PC and control to your network. Confirm that the control has the correct network settings using the Control Information feature of AppManager:

AppManager—Control Information screen

The AppManager Control Information screen shows information about the CPU board and its hard drive and confirms the network configurations previously applied.

Select the control in the Control Window (login if required). Then select *Control Information* from the *Control* menu or press the Control Information button in the toolbar:



Computer Name : WW_P1020_BETA3

Computer IP Address : 10.14.140.122

Footprint Part Number : 5418-4114

Footprint Revision : 47

AMService Version : 5.4 (User Version- 5.1)

Footprint Description :

```
Freescale P1020E - Security Engine
VxWorks 6.9 SMP - e500v2gnu
Creation Date - Nov  6 2015 15:53:25
RAMDrive Capacity - 134062K
RAMDrive FreeSpace - 130146K
FLASHDrive FreeSpace - 42482K
Memory Free - 344213K
Adapters - Address Subnet Gateway MAC
Ethernet1 10.14.140.122 255.255.0.0 10.14.128.1 004444000102
Ethernet2 192.168.0.11 255.255.255.0 Not Set 004444000101
Ethernet3 192.168.10.11 255.255.255.0 Not Set 00128c010101
Ethernet4 192.168.20.11 255.255.255.0 Not Set 004444000103
Ethernet5 192.168.30.11 255.255.255.0 Not Set 004444000104
Ethernet6 192.168.40.11 255.255.255.0 Not Set 004444000105
SNTP Server - 10.14.99.4
SNTP Update Rate - 30
Bootloader - 5418-4115 Rev - M
Account Management - Enabled
Secured Application - Disabled
Run hours - 8430
WW_Abstraction - 2.16.0
WW_IO_Abstraction - 2.2.3
StdFiles - 1.7.1
```

Figure 2-7. Control Information Window

IMPORTANT **For MicroNet Plus CPUs, GbE1 and GbE2 ports (if equipped) and ENET1 and ENET2 ports can be changed on the control with AppManager. RTN1 and RTN2 ports are pre-configured and can only be changed with switch settings on the CPU (see hardware manual).**

Chapter 3.
Application Setup and Configuration

Introduction

Create and load the application program for the control, before the control will perform any useful function. This section describes what steps the system engineer must perform to properly create, load, and maintain software on the control.

Creating the Application

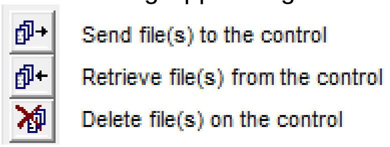
Create the application software using Woodward GAP and Coder tools described in Chapter 1. The GAP application defines the I/O location, configuration, and range settings, simplex or redundant selections, as well as the signal flow of the control application. If Ladder Logic is used, define and link this application to the GAP. When the application is complete, GAP performs a completeness check. This result is an output called the .CDR file, which the Coder tool uses to create the target software (.OUT files). This file is then loaded into the control's non-volatile memory.

IMPORTANT **Use the appropriate Coder version to build the application. Consult with Woodward if unsure which version to use.**

Downloading and Running the Application

Use the AppManager tool to transfer the application to the control. First, install AppManager on a PC that is networked to the control. Then, use the AppManager "Transfer Application Files" command to move the .OUT file to the control's non-volatile flash memory (flash disk). AppManager ensures application file transfer to the proper area on the control for execution. Some applications require more than just the ".OUT" file to run; AppManager ensures transfer of these files.

The following AppManager toolbar buttons may be used to send, retrieve, and delete files:



Send file(s) to the control

Retrieve file(s) from the control

Delete file(s) on the control

IMPORTANT **After an application is transferred to the control, it will copy the file to the Flash file system. This is indicated in AppManager by the words "Synchronizing file to Flash – <application name>.out". While "Synchronizing file to flash" is displayed in AppManager, the file is NOT saved in non-volatile memory and will not be preserved if the CPU is powered off. You must wait until "Synchronizing file to flash" is no longer displayed in AppManager before powering off the CPU.**

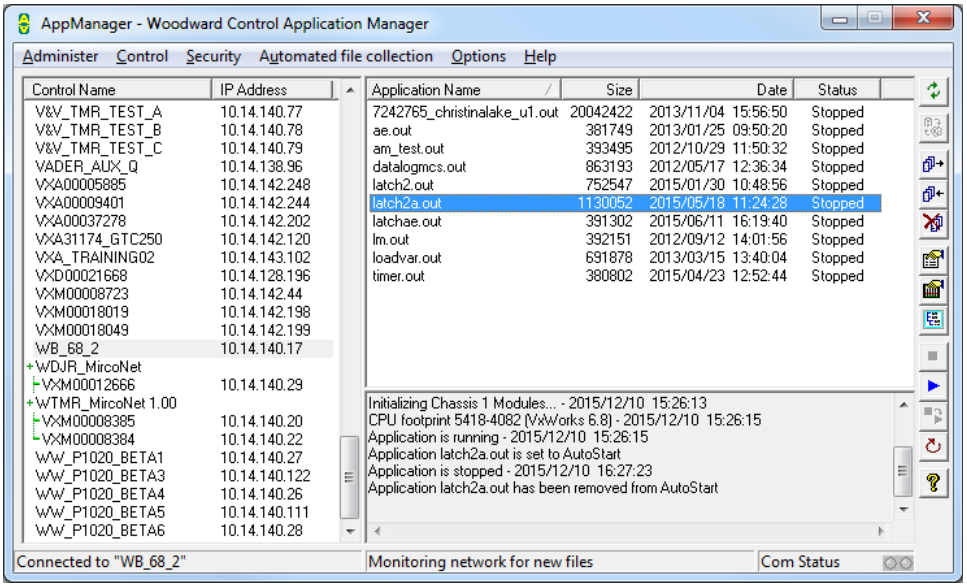
IMPORTANT **AppManager requires a valid Login to the control before the application can be manipulated by a new user or workstation. See Chapter 2, "Network Passwords" section, Table 2-1 (a, b).**

Once transfer of the application file (.OUT) to the control is successful, follow these steps to start the application:

1. Select the Control Name. The Control List displays the computer names of all controls attached to the network. When you select a control name from the list, an updated Application List (right window) appears. You may have to first supply login credentials for the control. See Tables 2-4 or 2-5 for the factory set login credentials descriptions.

2. Select the application you want to start by selecting a line in the Application List. The selected application is highlighted as displayed in Figure 3-1.

3. Press the [Start Application] button ▶ to run the application. AppManager will start the application software. Initialization Status messages will be displayed in the lower right window. You can also double-click the application name to start or stop the application. (If the system is configured for redundant operation repeat steps 1-3 for the other CPU).


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help

Control Name	IP Address
V&V_TMR_TEST_A	10.14.140.77
V&V_TMR_TEST_B	10.14.140.78
V&V_TMR_TEST_C	10.14.140.79
VADER_AUX_Q	10.14.138.96
VXA00005885	10.14.142.248
VXA00009401	10.14.142.244
VXA00037278	10.14.142.202
VXA31174_GTC250	10.14.142.120
VXA_TRAINING02	10.14.143.102
VXD00021668	10.14.128.196
VXM00008723	10.14.142.44
VXM00018019	10.14.142.198
VXM00018049	10.14.142.199
WB_68_2	10.14.140.17
+WDJR_MircoNet	
VXM00012666	10.14.140.29
+WTMR_MircoNet 1.00	
VXM00008385	10.14.140.20
VXM00008384	10.14.140.22
WW_P1020_BETA1	10.14.140.27
WW_P1020_BETA3	10.14.140.122
WW_P1020_BETA4	10.14.140.26
WW_P1020_BETA5	10.14.140.111
WW_P1020_BETA6	10.14.140.28

Application Name	Size	Date	Status
7242765_christinalake_u1.out	20042422	2013/11/04 15:56:50	Stopped
ae.out	381749	2013/01/25 09:50:20	Stopped
am_test.out	393495	2012/10/29 11:50:32	Stopped
datalogmcs.out	863193	2012/05/17 12:36:34	Stopped
latch2.out	752547	2015/01/30 10:48:56	Stopped
latch2a.out	1130052	2015/05/18 11:24:28	Stopped
latchae.out	391302	2015/06/11 16:19:40	Stopped
lm.out	392151	2012/09/12 14:01:56	Stopped
loadvar.out	691878	2013/03/15 13:40:04	Stopped
timer.out	380802	2015/04/23 12:52:44	Stopped

```
Initializing Chassis 1 Modules... - 2015/12/10  15:26:13
CPU footprint 5418-4082 (VxWorks 6.8) - 2015/12/10  15:26:15
Application is running - 2015/12/10  15:26:15
Application latch2a.out is set to AutoStart
Application is stopped - 2015/12/10  16:27:23
Application latch2a.out has been removed from AutoStart
```

Connected to "WB_68_2" Monitoring network for new files Com Status

Figure 3-1. Control Application Manager Page

Once the application is running, the Status LEDs on the boards configured in GAP will turn off, and AppManager will indicate that the application is marked as the Autostart application. This means that if the control's power is cycled, or if the control goes down for any reason, the current application will automatically restart when the control comes back up. This feature eliminates the need to connect to the control with AppManager every time the control is powered up to get the application software running.

When an application stops by using AppManager's *Stop Application* command ■ AppManager un-marks the application as part of the Autostart application.

IMPORTANT **The first time the application starts, an .EE file is created which holds all of the tunable values in the application program. This file is located in the same folder as the .OUT file. See the "Tunables management" section at the end of this chapter.**

IMPORTANT

Recommend keeping a backup of the applications files used on the control in the event that the HD1Flash drive needs to be restored. Use either

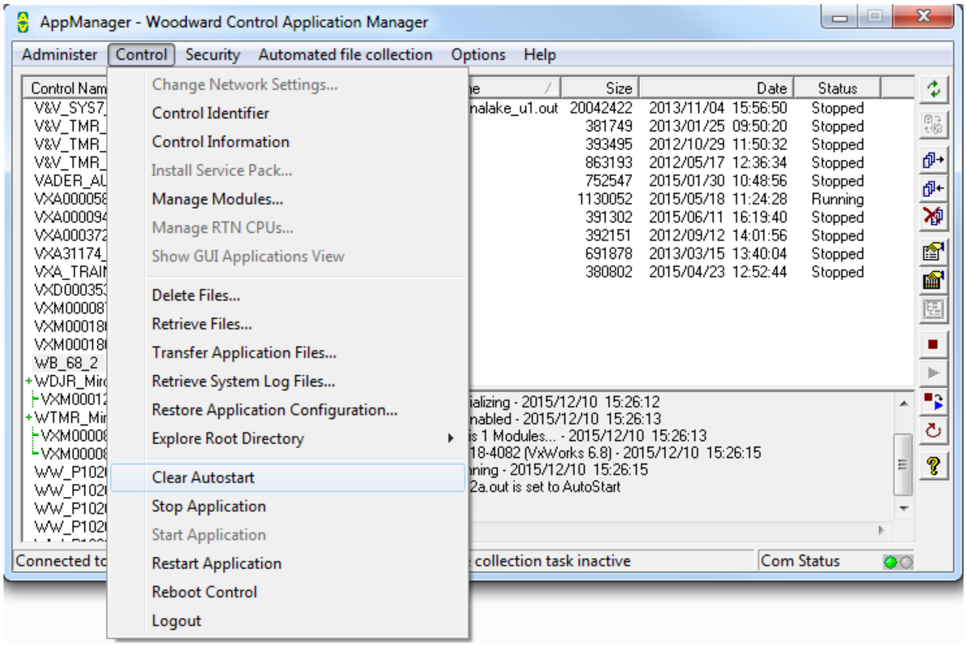
- **The Application Files Backup feature of AppManager or**
- **The Retrieve function in AppManager and select file type – "All files *.*". Select all the files in the dialog box and press *Retrieve*.**

Application files may include the following file types - .out, .out.enc, .ee, .nlg, .ll, .vlv, .logconfig.

Clear Autostart (not available in all versions)

Using AppManager, clear the Autostart function per the following:

1. On your PC, open AppManager.exe.
2. You should see the Woodward control's Computer Name in the AppManager window. Select the Computer Name of the control. If the control name is not on the list, check your connections and verify that the Link lights are on.
3. If required, login to the Control with a valid account name and password.
4. Click "Control" in the top header of the AppManager window, use the pull down menu, and select "Clear Autostart".



e	Size	Date	Status
nalake_u1.out	20042422	2013/11/04 15:56:50	Stopped
	381749	2013/01/25 09:50:20	Stopped
	393495	2012/10/29 11:50:32	Stopped
	863193	2012/05/17 12:36:34	Stopped
	752547	2015/01/30 10:48:56	Stopped
	1130052	2015/05/18 11:24:28	Running
	391302	2015/06/11 16:19:40	Stopped
	392151	2012/09/12 14:01:56	Stopped
	691878	2013/03/15 13:40:04	Stopped
	380802	2015/04/23 12:52:44	Stopped

```
ializing - 2015/12/10 15:26:12
nabled - 2015/12/10 15:26:13
s 1 Modules... - 2015/12/10 15:26:13
18-4082 (VxWorks 6.8) - 2015/12/10 15:26:15
nning - 2015/12/10 15:26:15
2a.out is set to AutoStart
```

Connected tc | collection task inactive | Com Status

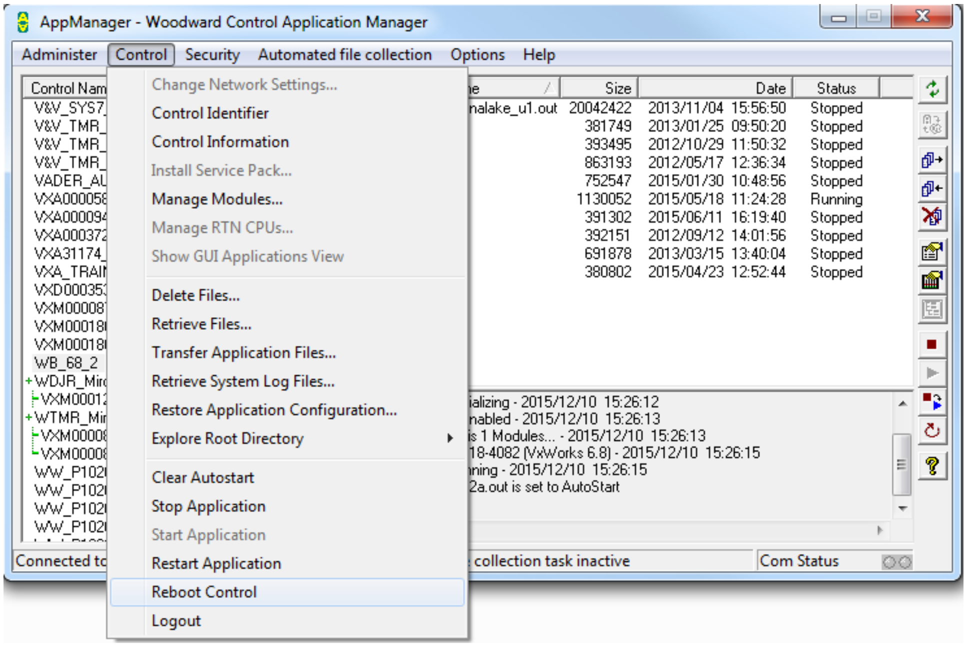
Figure 3-2. AppManager Control Menu – Clear Autostart

5. After the Clear Autostart routine completes, the next time the CPU is reset the Application will not start automatically. See Application Setup and Configuration section.
6. This means that if the control's power cycles, or if the control goes down for any reason, the current application will NOT automatically restart when the control comes back up. The user will have to use AppManager after the control powers up to get the application software running. If the Application stopped and then started after auto start is disabled, auto start will be re-enabled.

Rebooting the CPU

Using AppManager, re-boot the CPU per the following:

1. On your PC, open AppManager.exe.
2. You should see the Woodward control's Computer Name in the AppManager window. Select the Computer Name of the control. If the control name is not on the list, check your connections and verify that the Link lights are on.
3. If required, login to the Control with a valid account name and password.
4. Click "Control" in the top header of the AppManager window, use the pull down menu, and select "Reboot Control".



```
Control Nam          e                /   Size        Date          Status
V&V_SYS7_            nalake_u1.out  20042422  2013/11/04 15:56:50  Stopped
V&V_TMR_                              381749  2013/01/25 09:50:20  Stopped
V&V_TMR_                              393495  2012/10/29 11:50:32  Stopped
V&V_TMR_                              863193  2012/05/17 12:36:34  Stopped
VADER_AL                              752547  2015/01/30 10:48:56  Stopped
VXA000058                            1130052  2015/05/18 11:24:28  Running
VXA000094                             391302  2015/06/11 16:19:40  Stopped
VXA000372                             392151  2012/09/12 14:01:56  Stopped
VXA31174_                             691878  2013/03/15 13:40:04  Stopped
VXA_TRAIN                             380802  2015/04/23 12:52:44  Stopped
VXD00035
VXM00008
VXM00018
VXM00018
WB_68_2
+WDJR_Mir
 VXM0001
+WTMR_Mir
 VXM0000
 VXM0000
WW_P102
WW_P102
WW_P102
WW_P102

ializing - 2015/12/10 15:26:12
nabled - 2015/12/10 15:26:13
s 1 Modules... - 2015/12/10 15:26:13
18-4082 (VxWorks 6.8) - 2015/12/10 15:26:15
ning - 2015/12/10 15:26:15
2a.out is set to AutoStart
```

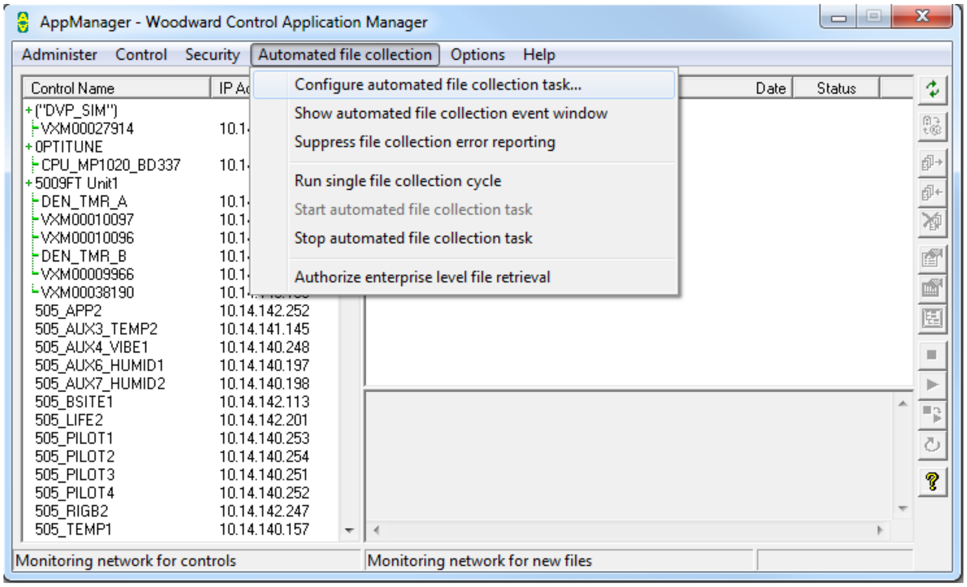
Figure 3-3. AppManager Control Menu – Reboot Control

5. This will cause the CPU to shut down and reboot.

IMPORTANT **Rebooting the CPU will cause all the I/O to go to the "IO_LOCK" failsafe state. Do not reboot the control unless the controlled device is in a safe non-running state and all Tunable values are saved.**

Backing up Application Files

After commissioning the control, recommend backing up all the application files running on the control. To engage the AppManager program to collect application and related files, use the automated file collection feature:


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help
Configure automated file collection task...
Show automated file collection event window
Suppress file collection error reporting
Run single file collection cycle
Start automated file collection task
Stop automated file collection task
Authorize enterprise level file retrieval
Date
Status

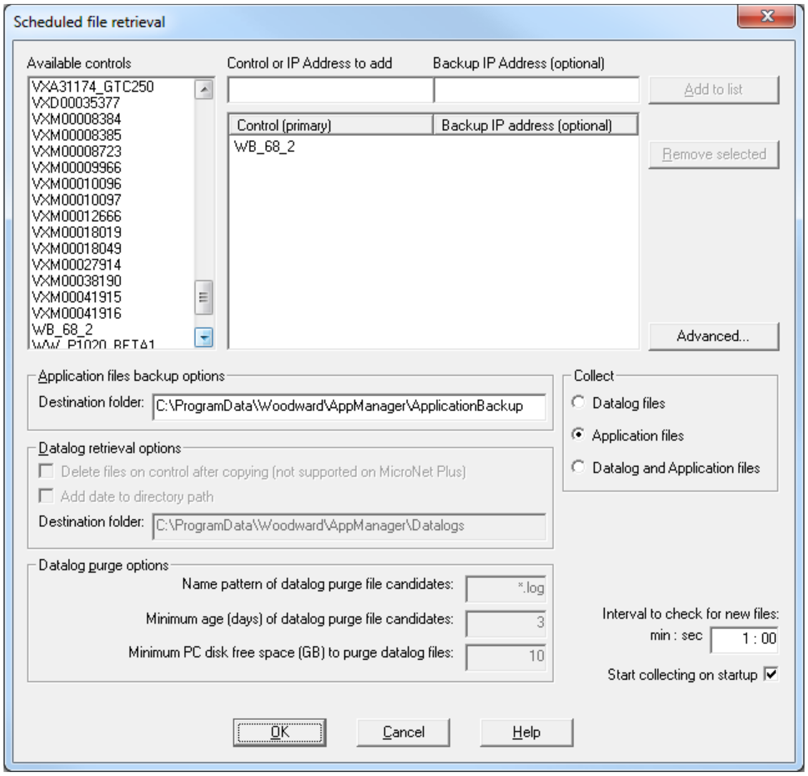
Control Name	IP Ac
+ ("DVP_SIM")	
VXM00027914	10.1
+ OPTITUNE	
CPU_MP1020_BD337	10.1
+ 5009FT Unit1	
DEN_TMR_A	10.1
VXM00010097	10.1
VXM00010096	10.1
DEN_TMR_B	10.1
VXM00009966	10.1
VXM00038190	10.1
505_APP2	10.14.142.252
505_AUX3_TEMP2	10.14.141.145
505_AUX4_VIBE1	10.14.140.248
505_AUX6_HUMID1	10.14.140.197
505_AUX7_HUMID2	10.14.140.198
505_BSITE1	10.14.142.113
505_LIFE2	10.14.142.201
505_PILOT1	10.14.140.253
505_PILOT2	10.14.140.254
505_PILOT3	10.14.140.251
505_PILOT4	10.14.140.252
505_RIGB2	10.14.142.247
505_TEMP1	10.14.140.157

Monitoring network for controls

Monitoring network for new files

Figure 3-4.AppManager Automated File Collection Menu

This will open the automated file collection configuration window:



Available controls

VXA31174_GTC250
VXD00035377
VXM00008384
VXM00008385
VXM00008723
VXM00009966
VXM00010096
VXM00010097
VXM00012666
VXM00018019
VXM00018049
VXM00027914
VXM00038190
VXM00041915
VXM00041916
WB_68_2
WW_P1020_BETA1

Control or IP Address to add:

Backup IP Address (optional):

Control (primary)	Backup IP address (optional)
WB_68_2	

Application files backup options

Destination folder: C:\ProgramData\Woodward\AppManager\ApplicationBackup

Collect

○ Datalog files

● Application files

○ Datalog and Application files

Datalog retrieval options

□ Delete files on control after copying (not supported on MicroNet Plus)

□ Add date to directory path

Destination folder: C:\ProgramData\Woodward\AppManager\Datalogs

Datalog purge options

Name pattern of datalog purge file candidates: *.log

Minimum age (days) of datalog purge file candidates: 3

Minimum PC disk free space (GB) to purge datalog files: 10

Interval to check for new files: min : sec 1 : 00

Start collecting on startup ☑

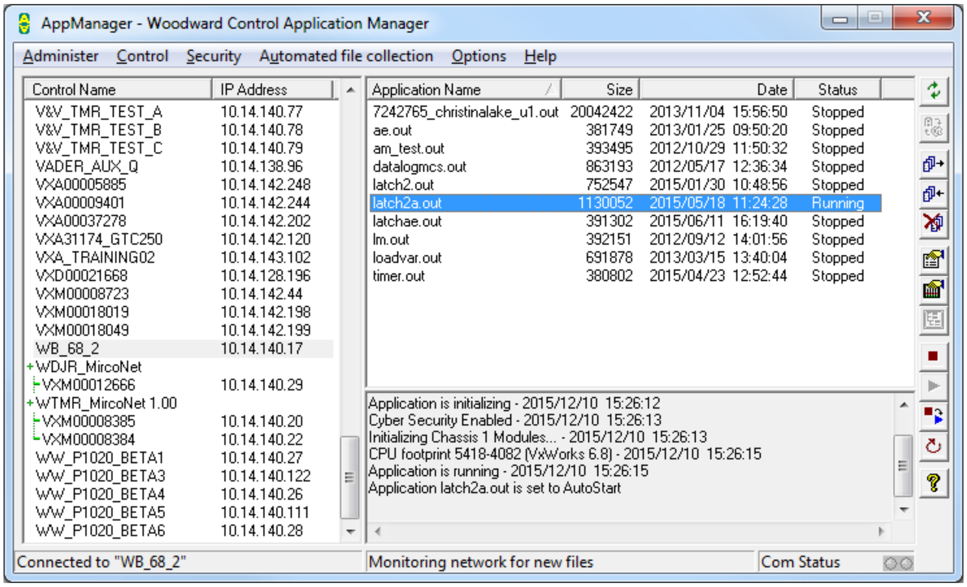
Figure 3-5. File Collection Configuration Window

The controls (which will be collected from) are specified in the “Control (primary)” item list. Use controls from the list at the left to populate the *Control or IP Address to add* edit window, which in turn is used to build the *Control (primary)* list. Select the option to Collect “Application files” or Collect “Datalog and Application files”. After configuring these options and pressing the OK button, automatic file backup will commence. If left running in this mode, AppManager will ensure that new application files on the control are automatically retrieved to the connected PC, as long as AppManager continues to run. Turn off the feature once all the current files have been collected. This could take some time, so it is best to let AppManager run for several minutes in this mode before turning off the collection. If there are many or large files, it may be necessary to wait longer.

IMPORTANT **It is also possible to manually backup the application files by using the interactive application file retrieval function of AppManager (Control menu / Retrieve files…) and selecting a file filter of “All files”.**

Changing the Application

To change an application that is running, highlight the running application name, and then press the [Stop Application] button. ■


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help

Control Name	IP Address
V&V_TMR_TEST_A	10.14.140.77
V&V_TMR_TEST_B	10.14.140.78
V&V_TMR_TEST_C	10.14.140.79
VADER_AUX_Q	10.14.138.96
VXA00005885	10.14.142.248
VXA00009401	10.14.142.244
VXA00037278	10.14.142.202
VXA31174_GTC250	10.14.142.120
VXA_TRAINING02	10.14.143.102
VXD00021668	10.14.128.196
VXM00008723	10.14.142.44
VXM00018019	10.14.142.198
VXM00018049	10.14.142.199
WB_68_2	10.14.140.17
+WDJR_MircoNet	
VXM00012666	10.14.140.29
+WTMR_MircoNet 1.00	
VXM00008385	10.14.140.20
VXM00008384	10.14.140.22
WW_P1020_BETA1	10.14.140.27
WW_P1020_BETA3	10.14.140.122
WW_P1020_BETA4	10.14.140.26
WW_P1020_BETA5	10.14.140.111
WW_P1020_BETA6	10.14.140.28

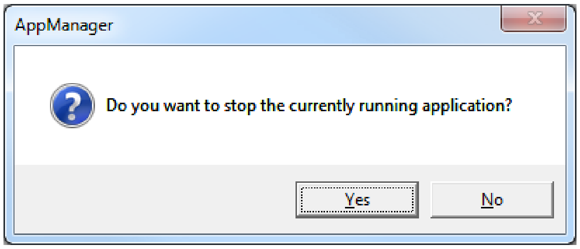
Application Name	Size	Date	Status
7242765_christinalake_u1.out	20042422	2013/11/04 15:56:50	Stopped
ae.out	381749	2013/01/25 09:50:20	Stopped
am_test.out	393495	2012/10/29 11:50:32	Stopped
datalogmcs.out	863193	2012/05/17 12:36:34	Stopped
latch2.out	752547	2015/01/30 10:48:56	Stopped
latch2a.out	1130052	2015/05/18 11:24:28	Running
latchae.out	391302	2015/06/11 16:19:40	Stopped
lm.out	392151	2012/09/12 14:01:56	Stopped
loadvar.out	691878	2013/03/15 13:40:04	Stopped
timer.out	380802	2015/04/23 12:52:44	Stopped

```
Application is initializing - 2015/12/10  15:26:12
Cyber Security Enabled - 2015/12/10  15:26:13
Initializing Chassis 1 Modules... - 2015/12/10  15:26:13
CPU footprint 5418-4082 (VxWorks 6.8) - 2015/12/10  15:26:15
Application is running - 2015/12/10  15:26:15
Application latch2a.out is set to AutoStart
```

Connected to "WB_68_2" | Monitoring network for new files | Com Status

Figure 3-6. Application Name Highlighted

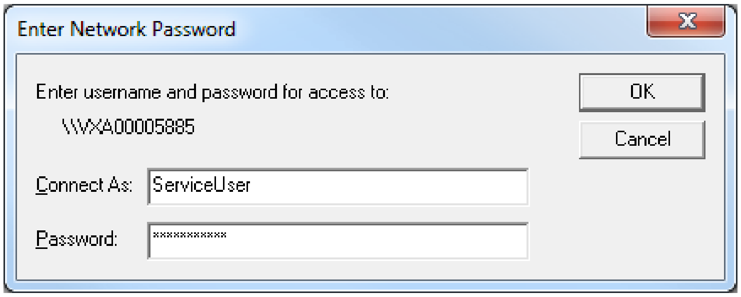
AppManager will confirm that you want to stop the currently running application. Select [YES].



Do you want to stop the currently running application?

Figure 3-7. Stop Application Run Confirmation Window

Newer Woodward controls require a login at connection. Some older controls do not require a login at connection time. For these older controls, AppManager requires a login before starting, stopping, or transferring files:



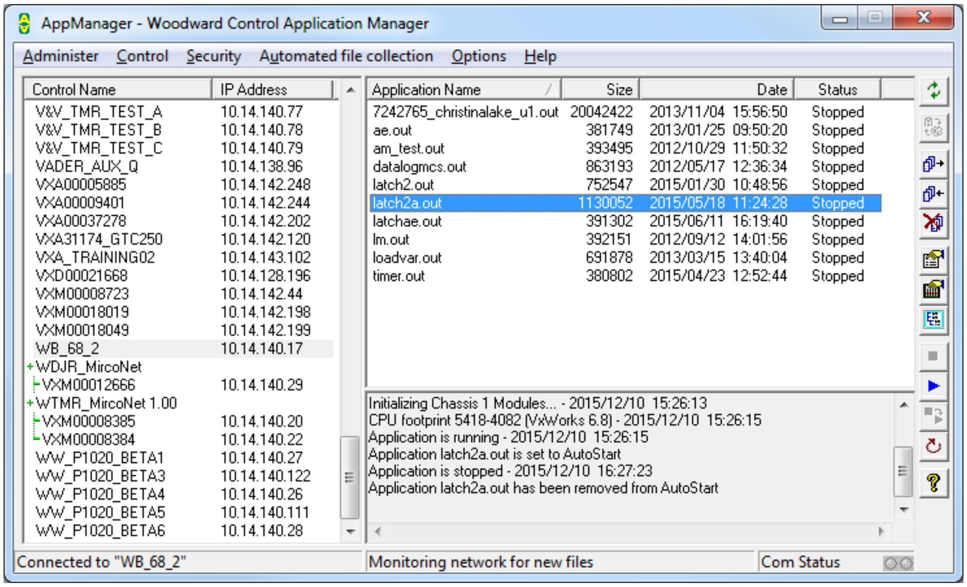
Enter username and password for access to:
\\VXA00005885

Connect As: ServiceUser

Password: ***********

Figure 3-8. Network Password Entry Window

The Status Message Display and Application List will indicate when the application has stopped and has been removed from the Autostart list.


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help

Control Name	IP Address
V&V_TMR_TEST_A	10.14.140.77
V&V_TMR_TEST_B	10.14.140.78
V&V_TMR_TEST_C	10.14.140.79
VADER_AUX_Q	10.14.138.96
VXA00005885	10.14.142.248
VXA00009401	10.14.142.244
VXA00037278	10.14.142.202
VXA31174_GTC250	10.14.142.120
VXA_TRAINING02	10.14.143.102
VXD00021668	10.14.128.196
VXM00008723	10.14.142.44
VXM00018019	10.14.142.198
VXM00018049	10.14.142.199
WB_68_2	10.14.140.17
+WDJR_MircoNet	
VXM00012666	10.14.140.29
+WTMR_MircoNet 1.00	
VXM00008385	10.14.140.20
VXM00008384	10.14.140.22
WW_P1020_BETA1	10.14.140.27
WW_P1020_BETA3	10.14.140.122
WW_P1020_BETA4	10.14.140.26
WW_P1020_BETA5	10.14.140.111
WW_P1020_BETA6	10.14.140.28

Application Name	Size	Date	Status
7242765_christinalake_u1.out	20042422	2013/11/04 15:56:50	Stopped
ae.out	381749	2013/01/25 09:50:20	Stopped
am_test.out	393495	2012/10/29 11:50:32	Stopped
datalogmcs.out	863193	2012/05/17 12:36:34	Stopped
latch2.out	752547	2015/01/30 10:48:56	Stopped
latch2a.out	1130052	2015/05/18 11:24:28	Stopped
latchae.out	391302	2015/06/11 16:19:40	Stopped
lm.out	392151	2012/09/12 14:01:56	Stopped
loadvar.out	691878	2013/03/15 13:40:04	Stopped
timer.out	380802	2015/04/23 12:52:44	Stopped

```
Initializing Chassis 1 Modules... - 2015/12/10 15:26:13
CPU footprint 5418-4082 (VxWorks 6.8) - 2015/12/10 15:26:15
Application is running - 2015/12/10 15:26:15
Application latch2a.out is set to AutoStart
Application is stopped - 2015/12/10 16:27:23
Application latch2a.out has been removed from AutoStart
```

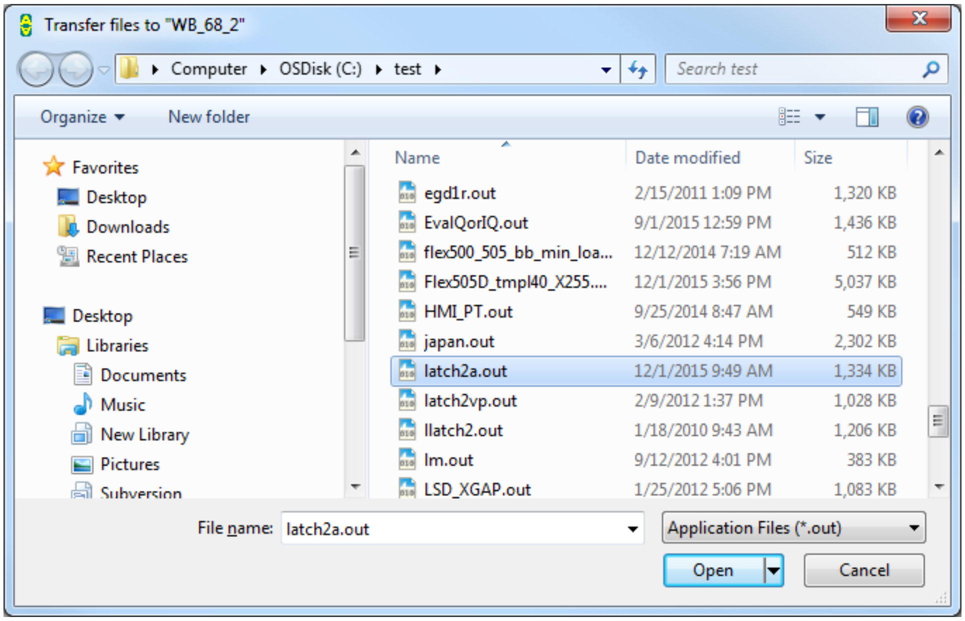
Connected to "WB_68_2" | Monitoring network for new files | Com Status

Figure 3-9. Status Message Display and Application List Page

Next, you will need to transfer an application to the control (skip this step if the application is already available in the Application List). Use the [Transfer App Files] button to move the application from your local PC to the control's flash memory.

If the application has not yet been loaded to the control:

- Make sure you have the proper control selected in the Control List, and then press the [Transfer App Files] button. A dialog box will appear that allows you to select an application to load to the control:



Name	Date modified	Size
egd1r.out	2/15/2011 1:09 PM	1,320 KB
EvalQorIQ.out	9/1/2015 12:59 PM	1,436 KB
flex500_505_bb_min_loa...	12/12/2014 7:19 AM	512 KB
Flex505D_tmpl40_X255....	12/1/2015 3:56 PM	5,037 KB
HMI_PT.out	9/25/2014 8:47 AM	549 KB
japan.out	3/6/2012 4:14 PM	2,302 KB
latch2a.out	12/1/2015 9:49 AM	1,334 KB
latch2vp.out	2/9/2012 1:37 PM	1,028 KB
llatch2.out	1/18/2010 9:43 AM	1,206 KB
lm.out	9/12/2012 4:01 PM	383 KB
LSD_XGAP.out	1/25/2012 5:06 PM	1,083 KB

File name: latch2a.out

Application Files (*.out)

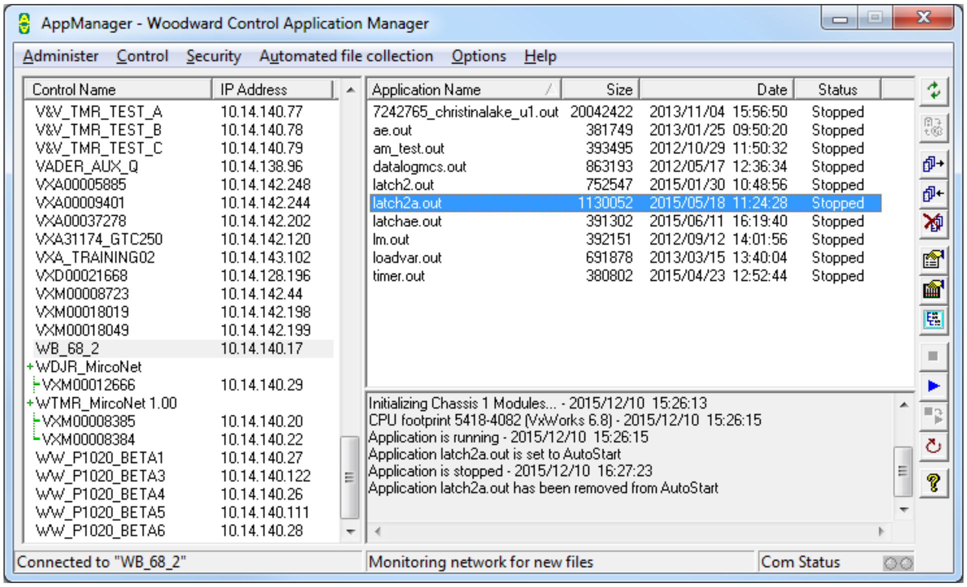
Figure 3-10. Application Selection Window

- Select the .OUT file of the application you want to transfer and press *Open*. AppManager will transfer the .OUT file to the control, as well as any related files it finds in the same folder (e.g. files ending in “.r1”, “.r2”, etc.). You will be prompted to verify your action is proper before overwriting existing files. You cannot overwrite an application that is currently running.

IMPORTANT

After an application transfers to the control, it will copy the file to the Flash file system. This is indicated in AppManager by the words “Synchronizing file to Flash – <application name>.out”. While “Synchronizing file to flash” is displayed in AppManager, the file is NOT saved in non-volatile memory and will not be preserved if the CPU is powered off. You must wait until “Synchronizing file to flash” is no longer displayed in AppManager before powering down the CPU.

- Once the application transfers, it is displayed in the Application list. Highlight the one you want to start and press the *Start Application* button ▶ to start the selected application


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help

Control Name	IP Address
V&V_TMR_TEST_A	10.14.140.77
V&V_TMR_TEST_B	10.14.140.78
V&V_TMR_TEST_C	10.14.140.79
VADER_AUX_Q	10.14.138.96
VXA00005885	10.14.142.248
VXA00009401	10.14.142.244
VXA00037278	10.14.142.202
VXA31174_GTC250	10.14.142.120
VXA_TRAINING02	10.14.143.102
VXD00021668	10.14.128.196
VXM00008723	10.14.142.44
VXM00018019	10.14.142.198
VXM00018049	10.14.142.199
WB_68_2	10.14.140.17
+WDJR_MircoNet	
VXM00012666	10.14.140.29
+WTMR_MircoNet 1.00	
VXM00008385	10.14.140.20
VXM00008384	10.14.140.22
WW_P1020_BETA1	10.14.140.27
WW_P1020_BETA3	10.14.140.122
WW_P1020_BETA4	10.14.140.26
WW_P1020_BETA5	10.14.140.111
WW_P1020_BETA6	10.14.140.28

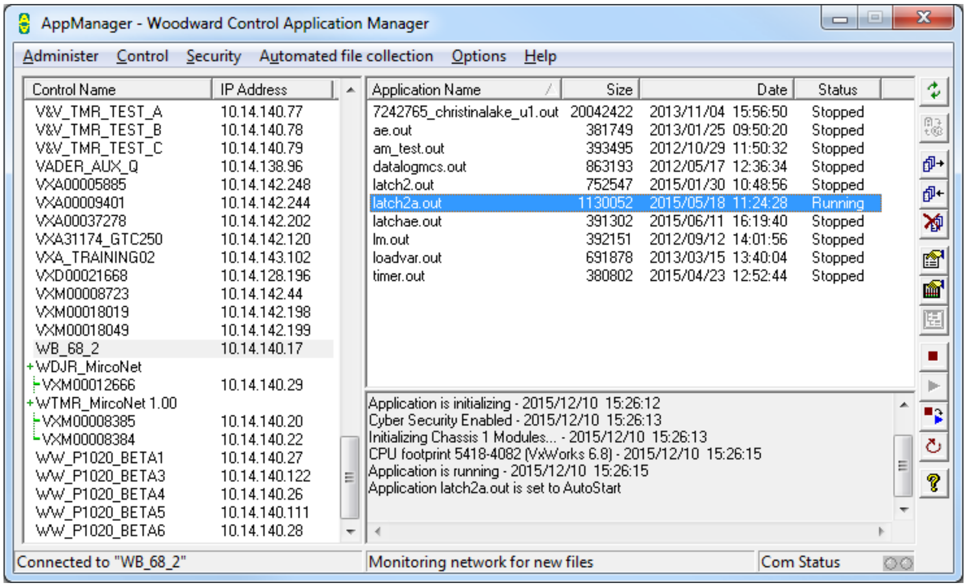
Application Name	Size	Date	Status
7242765_christinalake_u1.out	20042422	2013/11/04 15:56:50	Stopped
ae.out	381749	2013/01/25 09:50:20	Stopped
am_test.out	393495	2012/10/29 11:50:32	Stopped
datalogmcs.out	863193	2012/05/17 12:36:34	Stopped
latch2.out	752547	2015/01/30 10:48:56	Stopped
latch2a.out	1130052	2015/05/18 11:24:28	Stopped
latchae.out	391302	2015/06/11 16:19:40	Stopped
lm.out	392151	2012/09/12 14:01:56	Stopped
loadvar.out	691878	2013/03/15 13:40:04	Stopped
timer.out	380802	2015/04/23 12:52:44	Stopped

```
Initializing Chassis 1 Modules... - 2015/12/10 15:26:13
CPU footprint 5418-4082 (VxWorks 6.8) - 2015/12/10 15:26:15
Application is running - 2015/12/10 15:26:15
Application latch2a.out is set to AutoStart
Application is stopped - 2015/12/10 16:27:23
Application latch2a.out has been removed from AutoStart
```

Connected to "WB_68_2" | Monitoring network for new files | Com Status

Figure 3-11. Application Highlighted and Started

The Status Message Display will indicate that the Application is initializing and show status of the initialization process.


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help

Control Name	IP Address
V&V_TMR_TEST_A	10.14.140.77
V&V_TMR_TEST_B	10.14.140.78
V&V_TMR_TEST_C	10.14.140.79
VADER_AUX_Q	10.14.138.96
VXA00005885	10.14.142.248
VXA00009401	10.14.142.244
VXA00037278	10.14.142.202
VXA31174_GTC250	10.14.142.120
VXA_TRAINING02	10.14.143.102
VXD00021668	10.14.128.196
VXM00008723	10.14.142.44
VXM00018019	10.14.142.198
VXM00018049	10.14.142.199
WB_68_2	10.14.140.17
+WDJR_MircoNet	
VXM00012666	10.14.140.29
+WTMR_MircoNet 1.00	
VXM00008385	10.14.140.20
VXM00008384	10.14.140.22
WW_P1020_BETA1	10.14.140.27
WW_P1020_BETA3	10.14.140.122
WW_P1020_BETA4	10.14.140.26
WW_P1020_BETA5	10.14.140.111
WW_P1020_BETA6	10.14.140.28

Application Name	Size	Date	Status
7242765_christinalake_u1.out	20042422	2013/11/04 15:56:50	Stopped
ae.out	381749	2013/01/25 09:50:20	Stopped
am_test.out	393495	2012/10/29 11:50:32	Stopped
datalogmcs.out	863193	2012/05/17 12:36:34	Stopped
latch2.out	752547	2015/01/30 10:48:56	Stopped
latch2a.out	1130052	2015/05/18 11:24:28	Running
latchae.out	391302	2015/06/11 16:19:40	Stopped
lm.out	392151	2012/09/12 14:01:56	Stopped
loadvar.out	691878	2013/03/15 13:40:04	Stopped
timer.out	380802	2015/04/23 12:52:44	Stopped

```
Application is initializing - 2015/12/10 15:26:12
Cyber Security Enabled - 2015/12/10 15:26:13
Initializing Chassis 1 Modules... - 2015/12/10 15:26:13
CPU footprint 5418-4082 (VxWorks 6.8) - 2015/12/10 15:26:15
Application is running - 2015/12/10 15:26:15
Application latch2a.out is set to AutoStart
```

Connected to "WB_68_2" | Monitoring network for new files | Com Status

Figure 3-12. Status Message Display

Once the application is finished initializing, the Status Message Display will indicate that the Application is running and will Autostart.

If desired, delete the old, stopped application from the control's flash memory by selecting the [Delete App Files] button.

IMPORTANT

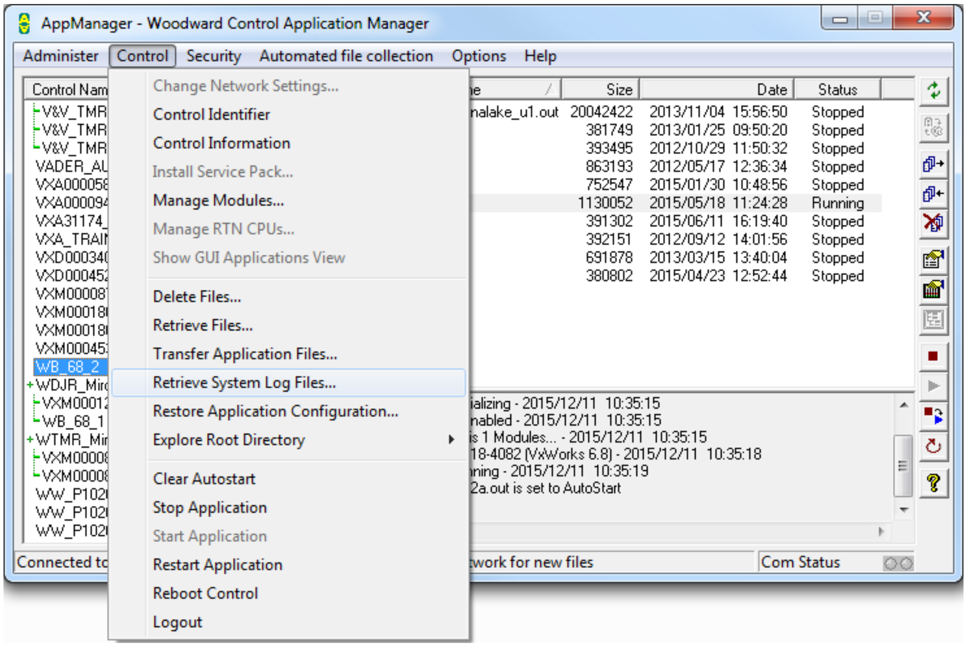
When the Woodward control is configured for redundant operation, you must stop both CPUs before loading the new application. When both CPUs have the new application, both CPUs must be started within 30 seconds of each other to enable redundant mode. If the CPUs are not started within 30 seconds of each other, the first CPU started will be the system controller with a missing backup CPU. When the second CPU starts, it will synchronize to the system and become the system backup.

Retrieving System Log Files

Use system logs to record events on the CPU. This includes login information and fault status information. If you need the login history (failed or successful) or if you are asked to provide the system logs for a CPU to assist in trouble shooting a problem, use this command.

Using AppManager, System Log files can be retrieved per the following steps:

1. On your PC, open AppManager.exe.
2. You should see the Woodward control's Computer Name in the AppManager window. Select the Computer Name of the control. If the control name does not appear on the list, check your connections and verify that the Link lights are on.
3. Login to the Control with a valid Account name and password.
4. Click "Control" in the top header of the AppManager window, use the pull down menu, and select "Retrieve System Log Files".



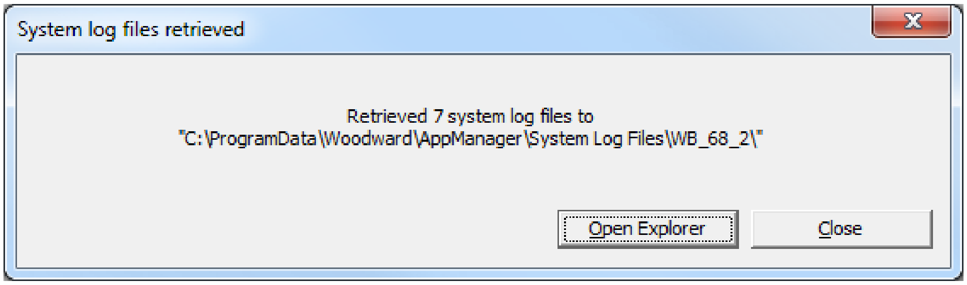
```
ne            Size        Date          Status
nalake_u1.out 20042422   2013/11/04 15:56:50   Stopped
               381749   2013/01/25 09:50:20   Stopped
               393495   2012/10/29 11:50:32   Stopped
               863193   2012/05/17 12:36:34   Stopped
               752547   2015/01/30 10:48:56   Stopped
              1130052   2015/05/18 11:24:28   Running
               391302   2015/06/11 16:19:40   Stopped
               392151   2012/09/12 14:01:56   Stopped
               691878   2013/03/15 13:40:04   Stopped
               380802   2015/04/23 12:52:44   Stopped
```

```
ializing - 2015/12/11  10:35:15
nabled - 2015/12/11  10:35:15
is 1 Modules... - 2015/12/11  10:35:15
18-4082 (VxWorks 6.8) - 2015/12/11  10:35:18
nning - 2015/12/11  10:35:19
2a.out is set to AutoStart
```

```
twork for new files
```

Figure 3-13. AppManager Control Menu – Retrieve System Log Files

5. All system log files will be copied from the selected CPU to the PC where AppManager is running in a directory like the following: c:\ProgramData\Woodward\System Log Files\<Group name (if used)>\<Name of Main CPU>*.log.



System log files retrieved

Retrieved 7 system log files to "C:\ProgramData\Woodward\AppManager\System Log Files\WB_68_2\"

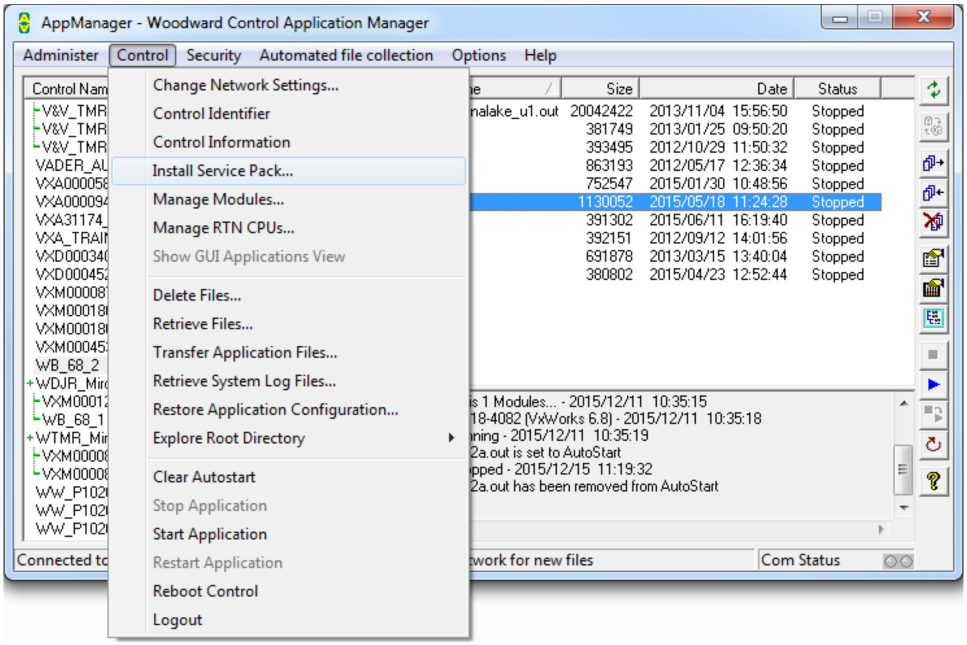
Figure 3-14. System Log Files Retrieved Verification Window

Installing Service Packs

When updates are made to the footprint of a MicroNet, 505, Flex500, or Atlas II CPU, service pack updates are created. Check the Woodward site for service packs updates.

Using AppManager, install new service packs as follows:

1. On your PC, open AppManager.exe.
2. You should see the Woodward control's Computer Name in the AppManager window. Select the Computer Name of the control. If the control name does not appear on the list, check your connections and verify that the Link lights are on.
3. Login to the Control with a valid Account name and password, which have "Execute control Service Pack" permission.
4. Click "Control" in the top header of the AppManager window, use the pull down menu, and select "Install Service Pack…" :

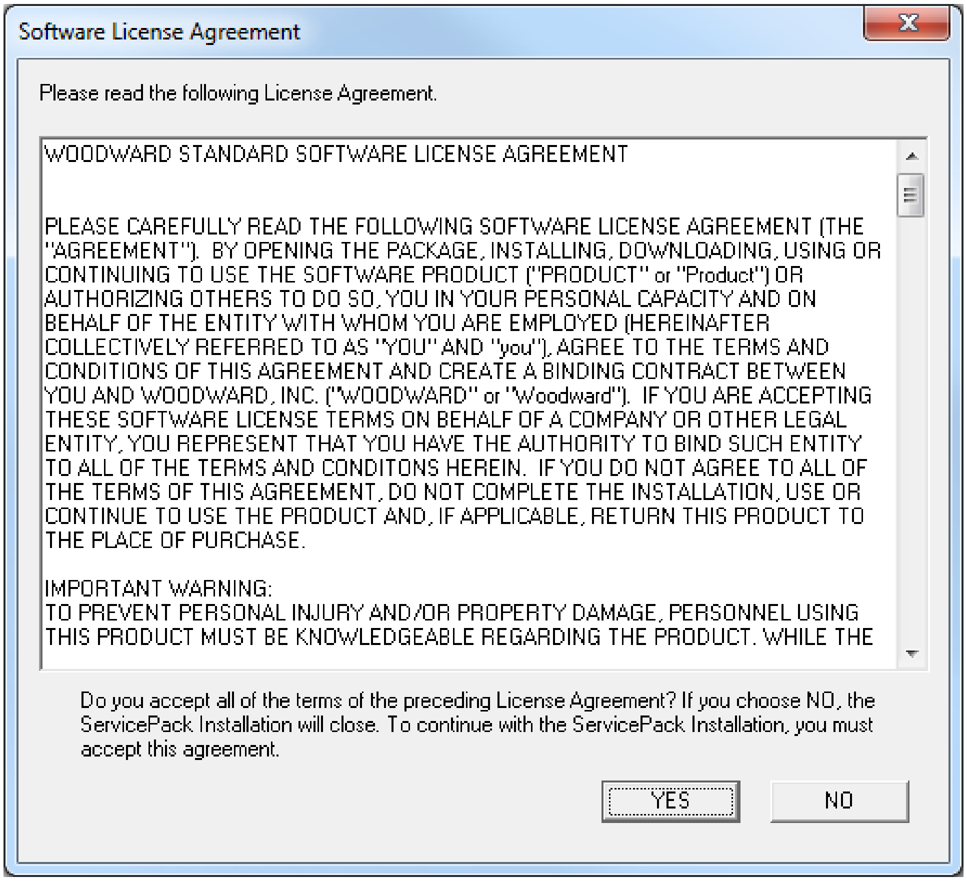


e	Size	Date	Status
nalake_u1.out	20042422	2013/11/04 15:56:50	Stopped
	381749	2013/01/25 09:50:20	Stopped
	393495	2012/10/29 11:50:32	Stopped
	863193	2012/05/17 12:36:34	Stopped
	752547	2015/01/30 10:48:56	Stopped
	1130052	2015/05/18 11:24:28	Stopped
	391302	2015/06/11 16:19:40	Stopped
	392151	2012/09/12 14:01:56	Stopped
	691878	2013/03/15 13:40:04	Stopped
	380802	2015/04/23 12:52:44	Stopped

```
is 1 Modules... - 2015/12/11  10:35:15
18-4082 (VxWorks 6.8) - 2015/12/11  10:35:18
nning - 2015/12/11  10:35:19
2a.out is set to AutoStart
pped - 2015/12/15  11:19:32
2a.out has been removed from AutoStart
```

Figure 3-15. AppManager Control Menu –Install Service Pack

5. Read the license agreement and select YES if you agree. If you select NO, AppManager will not install the Service Pack.



Please read the following License Agreement.

WOODWARD STANDARD SOFTWARE LICENSE AGREEMENT

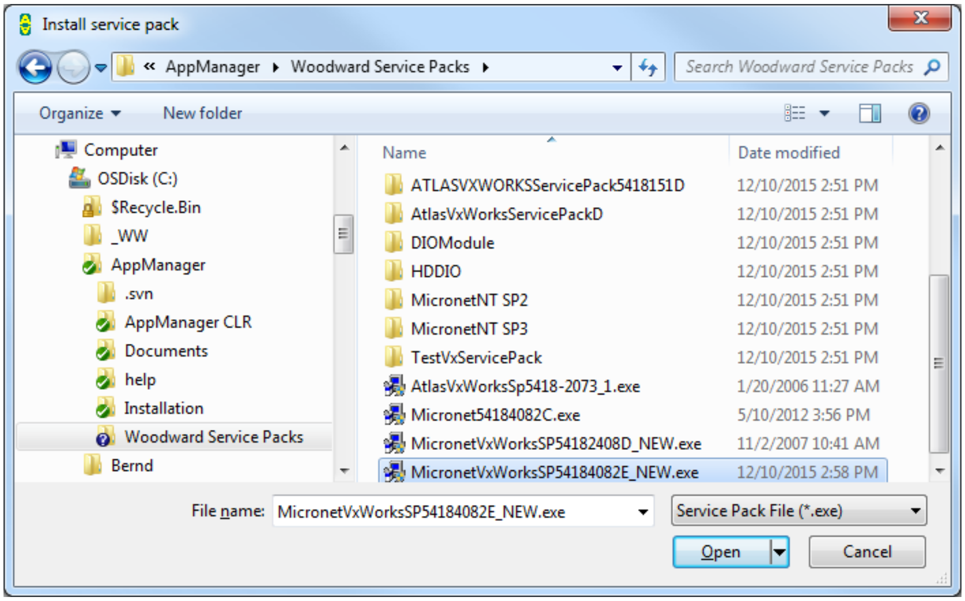
PLEASE CAREFULLY READ THE FOLLOWING SOFTWARE LICENSE AGREEMENT (THE "AGREEMENT"). BY OPENING THE PACKAGE, INSTALLING, DOWNLOADING, USING OR CONTINUING TO USE THE SOFTWARE PRODUCT ("PRODUCT" or "Product") OR AUTHORIZING OTHERS TO DO SO, YOU IN YOUR PERSONAL CAPACITY AND ON BEHALF OF THE ENTITY WITH WHOM YOU ARE EMPLOYED (HEREINAFTER COLLECTIVELY REFERRED TO AS "YOU" AND "you"), AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT AND CREATE A BINDING CONTRACT BETWEEN YOU AND WOODWARD, INC. ("WOODWARD" or "Woodward"). IF YOU ARE ACCEPTING THESE SOFTWARE LICENSE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO ALL OF THE TERMS AND CONDITONS HEREIN. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT COMPLETE THE INSTALLATION, USE OR CONTINUE TO USE THE PRODUCT AND, IF APPLICABLE, RETURN THIS PRODUCT TO THE PLACE OF PURCHASE.

IMPORTANT WARNING:
TO PREVENT PERSONAL INJURY AND/OR PROPERTY DAMAGE, PERSONNEL USING THIS PRODUCT MUST BE KNOWLEDGEABLE REGARDING THE PRODUCT. WHILE THE

Do you accept all of the terms of the preceding License Agreement? If you choose NO, the ServicePack Installation will close. To continue with the ServicePack Installation, you must accept this agreement.

Figure 3-16. License Agreement Window

6. Explore to the service pack downloaded from the Woodward web site and click install.



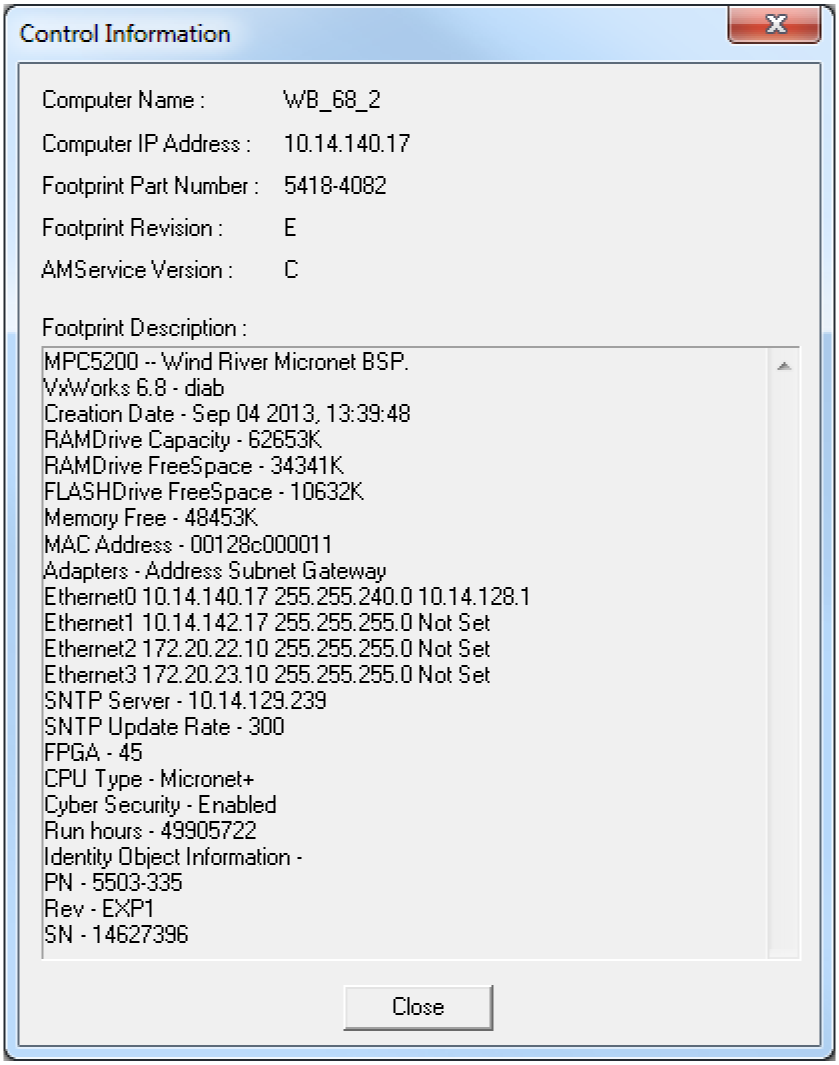
Name	Date modified
ATLASVXWORKSServicePack5418151D	12/10/2015 2:51 PM
AtlasVxWorksServicePackD	12/10/2015 2:51 PM
DIOModule	12/10/2015 2:51 PM
HDDIO	12/10/2015 2:51 PM
MicronetNT SP2	12/10/2015 2:51 PM
MicronetNT SP3	12/10/2015 2:51 PM
TestVxServicePack	12/10/2015 2:51 PM
AtlasVxWorksSp5418-2073_1.exe	1/20/2006 11:27 AM
Micronet54184082C.exe	5/10/2012 3:56 PM
MicronetVxWorksSP54182408D_NEW.exe	11/2/2007 10:41 AM
MicronetVxWorksSP54184082E_NEW.exe	12/10/2015 2:58 PM

File name: MicronetVxWorksSP54184082E_NEW.exe

Service Pack File (*.exe)

Figure 3-17. Service Pack Installation Window

7. AppManager will install the new service pack on the selected CPU. This will take some time, and AppManager will report progress as files transfer. When AppManager is finished transferring files, it will suggest a reboot. When the CPU reboots, the new service pack installs.
8. Confirm the new service pack installation by checking the current revision of the footprint by using AppManager Control->Control Information screen.



Computer Name : WB_68_2

Computer IP Address : 10.14.140.17

Footprint Part Number : 5418-4082

Footprint Revision : E

AMService Version : C

Footprint Description :

```
MPC5200 -- Wind River Micronet BSP.
VxWorks 6.8 - diab
Creation Date - Sep 04 2013, 13:39:48
RAMDrive Capacity - 62653K
RAMDrive FreeSpace - 34341K
FLASHDrive FreeSpace - 10632K
Memory Free - 48453K
MAC Address - 00128c000011
Adapters - Address Subnet Gateway
Ethernet0 10.14.140.17 255.255.240.0 10.14.128.1
Ethernet1 10.14.142.17 255.255.255.0 Not Set
Ethernet2 172.20.22.10 255.255.255.0 Not Set
Ethernet3 172.20.23.10 255.255.255.0 Not Set
SNTP Server - 10.14.129.239
SNTP Update Rate - 300
FPGA - 45
CPU Type - Micronet+
Cyber Security - Enabled
Run hours - 49905722
Identity Object Information -
PN - 5503-335
Rev - EXP1
SN - 14627396
```

Figure 3-18. AppManager Control, Control Information Screen

IMPORTANT **On some controls, it may take several minutes after a service pack reboot for all of the control's peripheral units to update. The status LEDs may be blinking during this period. Do not power off the control during this time.**

Account Management

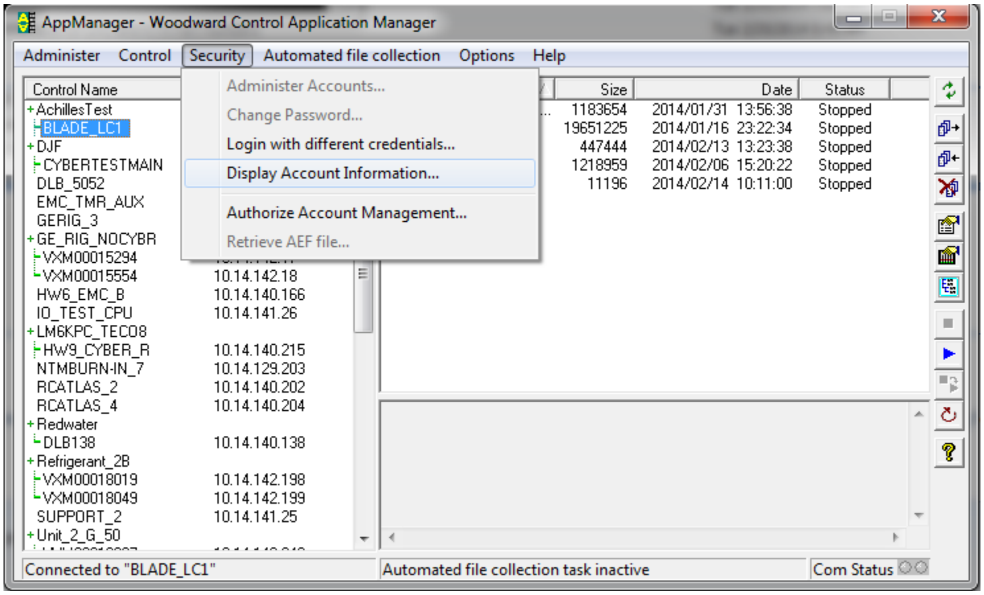
Certain controls support Account Management, which allows customization of the accounts on the control.

- The 5466-1141, 5466-1145, 5466-1245, 5466-1510 and 5466-1520 CPUs support Account Management.
- The 5466-1146 and 5466-1246 RTN_CPUs support Account Management.
- The 8200-1252 non-cyber gateway and 8200-1253 cyber gateway support Account Management.
- The 5466-1045 supports Account Management only after it is enabled

Enabling Account Management

Note: This section only applies to 5466-1045 CPU Modules. The Account Management features of this CPU are available only when they are enabled. Other CPUs are fixed either as supporting account management or not.

- Logon to the CPU (use ServiceUser account).
- Check to see if Account Management is enabled by selecting "Display Account Information…" from the Security menu in AppManager.

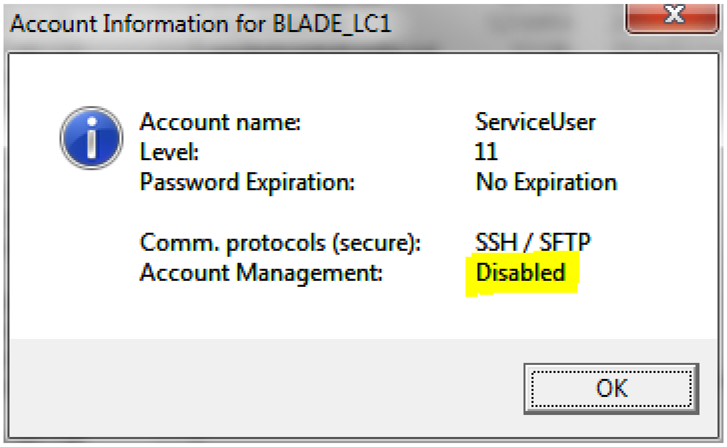

AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help
Administer Accounts...
Change Password...
Login with different credentials...
Display Account Information...
Authorize Account Management...
Retrieve AEF file...

Control Name	
+AchillesTest	
BLADE_LC1	
+DJF	
CYBERTESTMAIN	
DLB_5052	
EMC_TMR_AUX	
GERIG_3	
+GE_RIG_NOCYBR	
VXM00015294	
VXM00015554	10.14.142.18
HW6_EMC_B	10.14.140.166
IO_TEST_CPU	10.14.141.26
+LM6KPC_TECO8	
HW9_CYBER_R	10.14.140.215
NTMBURN-IN_7	10.14.129.203
RCATLAS_2	10.14.140.202
RCATLAS_4	10.14.140.204
+Redwater	
DLB138	10.14.140.138
+Refrigerant_2B	
VXM00018019	10.14.142.198
VXM00018049	10.14.142.199
SUPPORT_2	10.14.141.25
+Unit_2_G_50	

Size	Date	Status
1183654	2014/01/31 13:56:38	Stopped
19651225	2014/01/16 23:22:34	Stopped
447444	2014/02/13 13:23:38	Stopped
1218959	2014/02/06 15:20:22	Stopped
11196	2014/02/14 10:11:00	Stopped

Connected to "BLADE_LC1"
Automated file collection task inactive
Com Status

Figure 3-19. AppManager Security Menu – Display Account Information



Account Information for BLADE_LC1

Account name: ServiceUser
Level: 11
Password Expiration: No Expiration

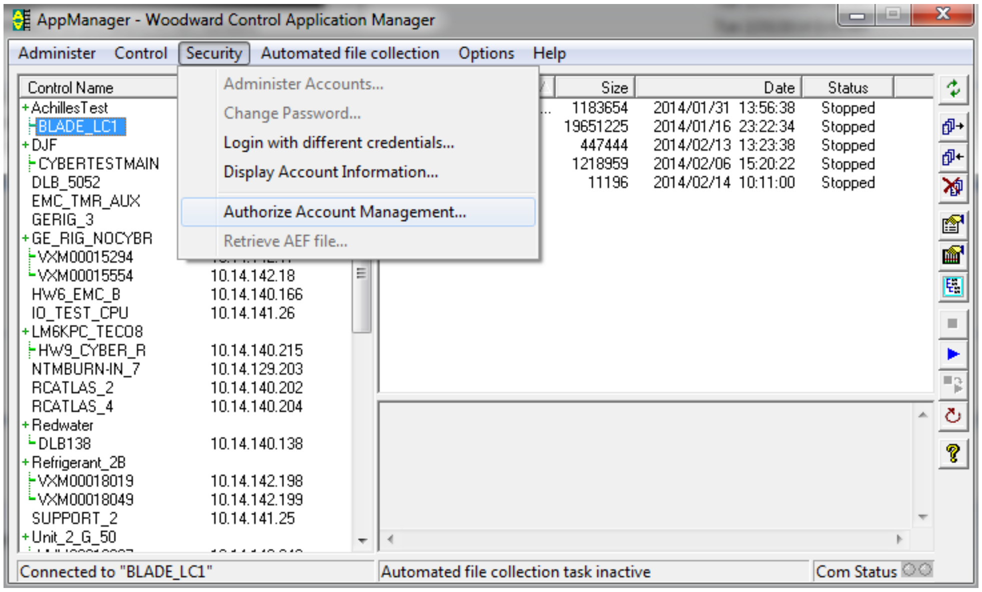
Comm. protocols (secure): SSH / SFTP
Account Management: Disabled

Figure 3-20. Account Information Window

If Account Management is disabled, enable it by using the Authorize Account Management feature in AppManager.

Authorize Account Management by selecting “Authorize Account Management…” from the Security menu in AppManager.

> **Note**: Log into the control with the ServiceUser credentials and all applications must be “Stopped” before you will be allowed to authorize Account Management.


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help
Administer Accounts...
Change Password...
Login with different credentials...
Display Account Information...
Authorize Account Management...
Retrieve AEF file...

Control Name	
+AchillesTest	
BLADE_LC1	
+DJF	
CYBERTESTMAIN	
DLB_5052	
EMC_TMR_AUX	
GERIG_3	
+GE_RIG_NOCYBR	
VXM00015294	
VXM00015554	10.14.142.18
HW6_EMC_B	10.14.140.166
IO_TEST_CPU	10.14.141.26
+LM6KPC_TEC08	
HW9_CYBER_R	10.14.140.215
NTMBURN-IN_7	10.14.129.203
RCATLAS_2	10.14.140.202
RCATLAS_4	10.14.140.204
+Redwater	
DLB138	10.14.140.138
+Refrigerant_2B	
VXM00018019	10.14.142.198
VXM00018049	10.14.142.199
SUPPORT_2	10.14.141.25
+Unit_2_G_50	

	Size	Date	Status
...	1183654	2014/01/31 13:56:38	Stopped
	19651225	2014/01/16 23:22:34	Stopped
	447444	2014/02/13 13:23:38	Stopped
	1218959	2014/02/06 15:20:22	Stopped
	11196	2014/02/14 10:11:00	Stopped

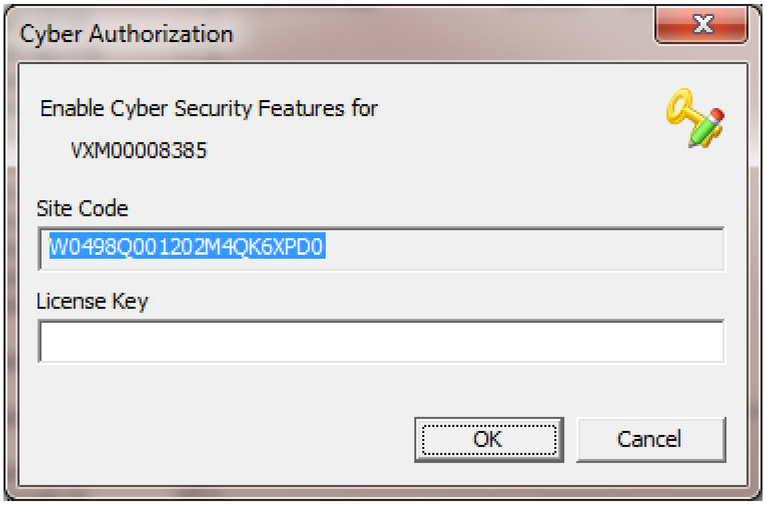
Connected to "BLADE_LC1"

Automated file collection task inactive

Com Status

Figure 3-21. AppManager Security Menu – Authorize Account Management

AppManager will prompt you to supply a “License Key” which can be obtained after purchasing a serial number through the Woodward software authorization process at www.woodward.com. For more information about the Woodward software authorization process, consult the AppManager help document.



Enable Cyber Security Features for

VXM00008385

Site Code

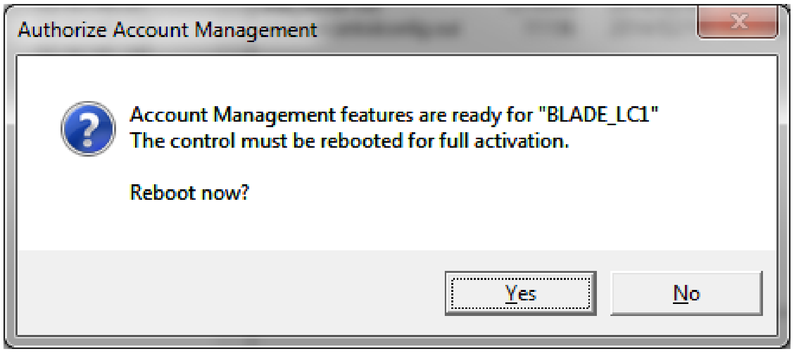
W0498Q001202M4QK6XPD0

License Key

Figure 3-22. Cyber Authorization Window

Enter the License Key then select OK.

AppManager will present the Site Code and then prompt for the License Key to authorize the CPU. If the CPU successfully authorizes the License Key, it will prompt you to reboot the CPU for the change to take effect. Select *Yes* and wait for the CPU to reboot.

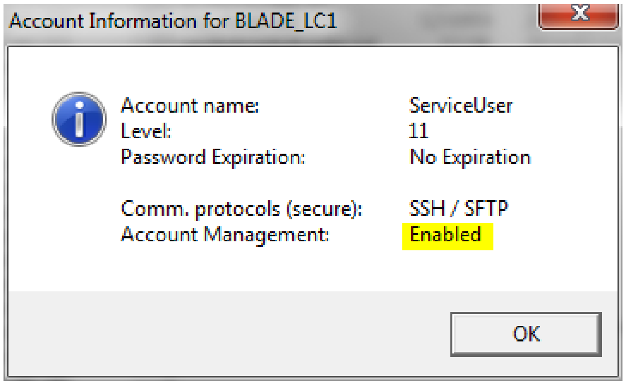

Authorize Account Management

Account Management features are ready for "BLADE_LC1"
The control must be rebooted for full activation.

Reboot now?

Figure 3-23. Account Manager Reboot Authorization Window

After the CPU reboots, verify Account Management is enabled by selecting “Display Account Information…” from the Security menu in AppManager.


Account Information for BLADE_LC1

Account name:	ServiceUser
Level:	11
Password Expiration:	No Expiration
Comm. protocols (secure):	SSH / SFTP
Account Management:	Enabled

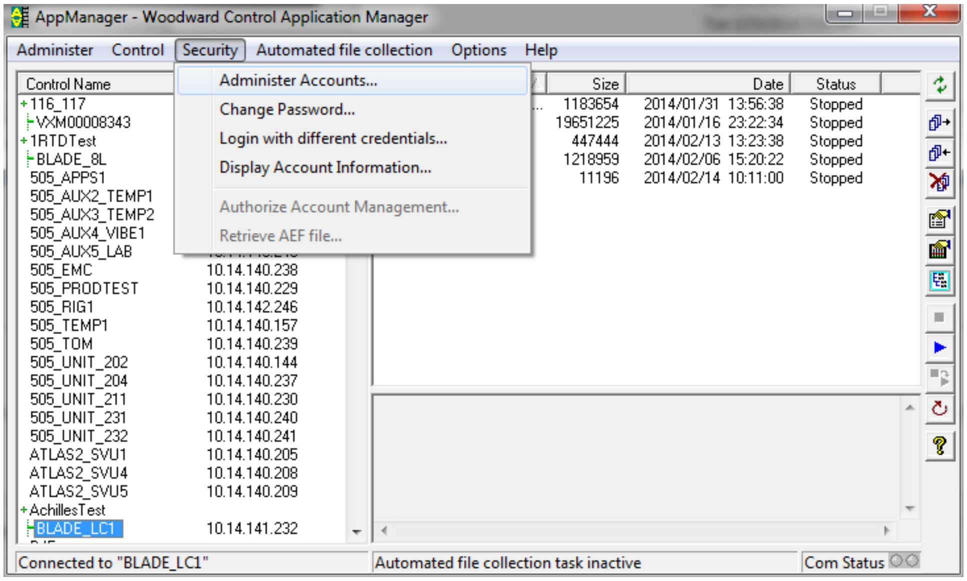
Figure 3-24. Account Management Enabled Verification Window

> **Note:** The following features are available only when Account Management is enabled (see section on “Enabling Account Management”).

Using AppManager, change the accounts settings as follows:

1. On your PC, open AppManager.exe.
2. You should see the Woodward control’s Computer Name in the AppManager window. Select the Computer Name of the control. If the control name does not appear on the list, check your connections and verify that the Link lights are on.
3. Login to the Control using the Administrator account name and password.

4. Click “Security” in the top header of the AppManager window. Use the pull down menu, and select “Administer Accounts”.
Note: You must login as the Administrator to administer accounts.


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help
Administer Accounts...
Change Password...
Login with different credentials...
Display Account Information...
Authorize Account Management...
Retrieve AEF file...

Control Name	
+116_117	
VXM00008343	
+1RTDTest	
BLADE_8L	
505_APPS1	
505_AUX2_TEMP1	
505_AUX3_TEMP2	
505_AUX4_VIBE1	
505_AUX5_LAB	
505_EMC	10.14.140.238
505_PRODTEST	10.14.140.229
505_RIG1	10.14.142.246
505_TEMP1	10.14.140.157
505_TOM	10.14.140.239
505_UNIT_202	10.14.140.144
505_UNIT_204	10.14.140.237
505_UNIT_211	10.14.140.230
505_UNIT_231	10.14.140.240
505_UNIT_232	10.14.140.241
ATLAS2_SVU1	10.14.140.205
ATLAS2_SVU4	10.14.140.208
ATLAS2_SVU5	10.14.140.209
+AchillesTest	
BLADE_LC1	10.14.141.232

Size	Date	Status
1183654	2014/01/31 13:56:38	Stopped
19651225	2014/01/16 23:22:34	Stopped
447444	2014/02/13 13:23:38	Stopped
1218959	2014/02/06 15:20:22	Stopped
11196	2014/02/14 10:11:00	Stopped

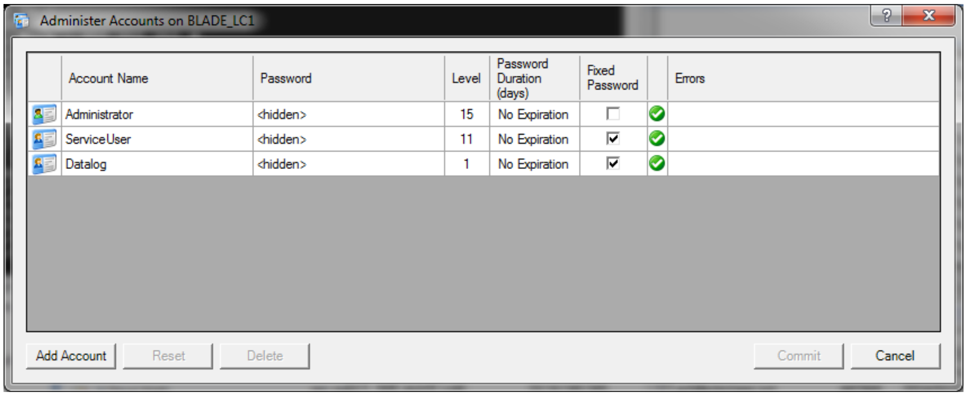
Connected to "BLADE_LC1"

Automated file collection task inactive

Com Status

Figure 3-25. AppManager Security Menu – Administer Accounts

5. To delete an account, select the account, then select the “Delete” button, then select the “Commit” button.



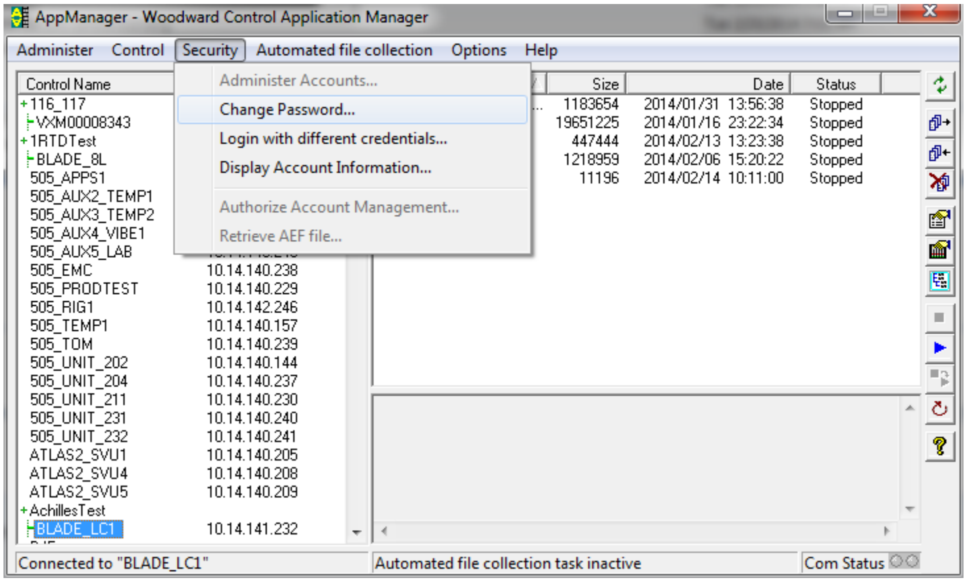
Account Name	Password	Level	Password Duration (days)	Fixed Password		Errors
Administrator	<hidden>	15	No Expiration	☐	✓	
ServiceUser	<hidden>	11	No Expiration	☑	✓	
Datalog	<hidden>	1	No Expiration	☑	✓	

Figure 3-26. Account Deletion Window

6. To enter a new account, select “Add Account” and fill in the Account Name, the Default Password, the Level, Password Duration in days, and the Fixed Password field then select the “Commit” button.
   a. Account Name must be at least four characters and no longer than 30 characters, and can contain letter and non-letter values.
   b. Default Password for the new account can use the “Default@1” value or enter your own value. Must be at least six characters and no longer than 30 characters and must contain at least two letter characters and two non-letter characters.
   c. The Level defines the permissions granted to this account. AppManager requires Level 1 for read file permission, Level 11 to write files, start / stop Applications and apply service packs. The GAP application (SYS_INFO Block) defines the Levels required to read and write each application variable.
   d. Password duration for the account can be set to any positive integer value for number of days until changing the password. The value of zero will set the account to have no expiration of the password.
   e. If the Fixed Password is “checked”, the account cannot change its own password. Use this for shared accounts when only the administrator has permission to change the password.
   Note: If Fixed Password is “checked”, the account will expire in the number of days defined by Password duration. Only the Administrator can change this password.
7. Reset account is the same as Delete account, then Add Account. It will keep the same settings as the selected account except for the password. Change other values at this time if desired.

Using AppManager, change the account’s password as follows:

1. On your PC, open AppManager.exe.
2. You should see the Woodward control’s Computer Name in the AppManager window. Select the Computer Name of the control. If the control name does not appear on the list, check your connections and verify that the Link lights are on.
3. Login to the Control using a valid Account name and password.
4. Click “Security” in the top header of the AppManager window, use the pull down menu, and select “Change Password…”.


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help
Administer Accounts...
Change Password...
Login with different credentials...
Display Account Information...
Authorize Account Management...
Retrieve AEF file...

Control Name	
+116_117	
VXM00008343	
+1RTDTest	
BLADE_8L	
505_APPS1	
505_AUX2_TEMP1	
505_AUX3_TEMP2	
505_AUX4_VIBE1	
505_AUX5_LAB	
505_EMC	10.14.140.238
505_PRODTEST	10.14.140.229
505_RIG1	10.14.142.246
505_TEMP1	10.14.140.157
505_TOM	10.14.140.239
505_UNIT_202	10.14.140.144
505_UNIT_204	10.14.140.237
505_UNIT_211	10.14.140.230
505_UNIT_231	10.14.140.240
505_UNIT_232	10.14.140.241
ATLAS2_SVU1	10.14.140.205
ATLAS2_SVU4	10.14.140.208
ATLAS2_SVU5	10.14.140.209
+AchillesTest	
BLADE_LC1	10.14.141.232

Size	Date	Status
1183654	2014/01/31 13:56:38	Stopped
19651225	2014/01/16 23:22:34	Stopped
447444	2014/02/13 13:23:38	Stopped
1218959	2014/02/06 15:20:22	Stopped
11196	2014/02/14 10:11:00	Stopped

Connected to "BLADE_LC1"

Automated file collection task inactive

Com Status

Figure 3-27. Security Menu – Change Password

Note: If the current account does not allow the Password to change, the “Password Change Not Allowed” message will be displayed.

5. Enter the New Password and enter the same Password in the Confirm New Password box. (New Password and Confirm New Password must match or AppManager will not accept the change.)

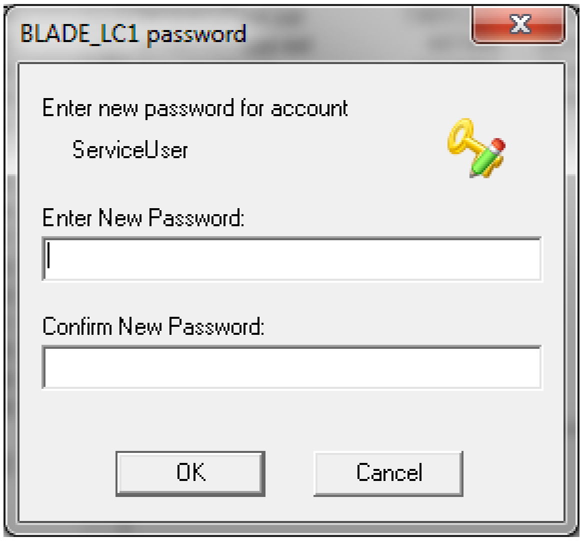


Figure 3-28. New Password Confirmation Box

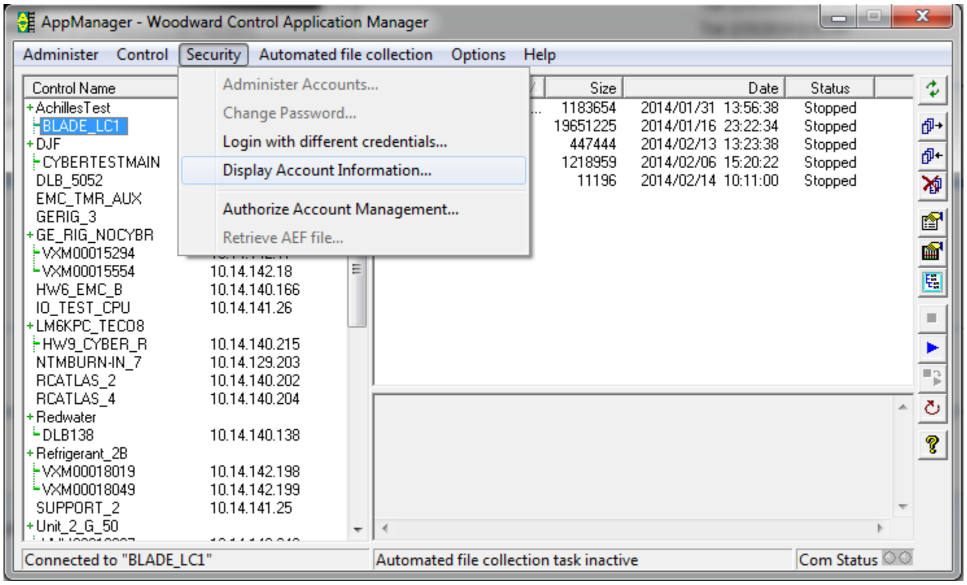
6. Select the OK button to change the password value.

IMPORTANT **If an account's password is lost, the Administrator can "Reset" the account to create a new password. If the Administrator password is lost, there is no way to recover it. Take extreme care to keep track of the Administrator password when changed from the default value.**

Using AppManager, the account information can be viewed as follows:

1. On your PC, open AppManager.exe.
2. You should see the Woodward control's Computer Name in the AppManager window. Select the Computer Name of the control. If the control name is not listed, check your connections and verify that the Link lights are on.
3. Login to the Control using a valid Account name and password.

4. Click “Security” in the top header of the AppManager window, use the pull down menu, and select “Display Account Information”.


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help
Administer Accounts...
Change Password...
Login with different credentials...
Display Account Information...
Authorize Account Management...
Retrieve AEF file...

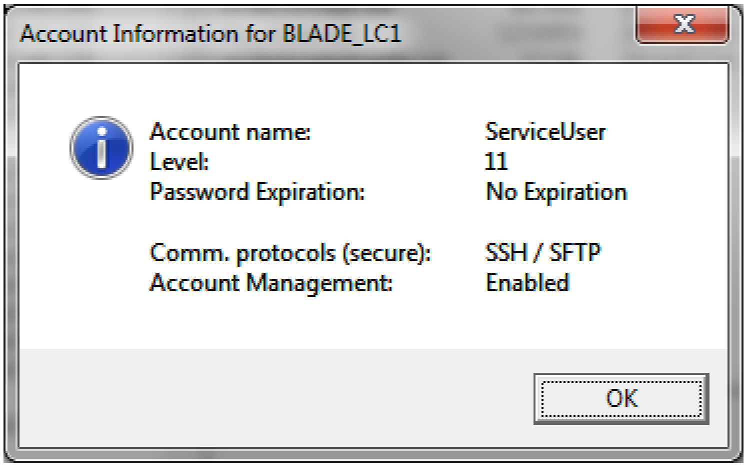
Control Name	
+AchillesTest	
BLADE_LC1	
+DJF	
CYBERTESTMAIN	
DLB_5052	
EMC_TMR_AUX	
GERIG_3	
+GE_RIG_NOCYBR	
VXM00015294	
VXM00015554	10.14.142.18
HW6_EMC_B	10.14.140.166
IO_TEST_CPU	10.14.141.26
+LM6KPC_TECO8	
HW9_CYBER_R	10.14.140.215
NTMBURN-IN_7	10.14.129.203
RCATLAS_2	10.14.140.202
RCATLAS_4	10.14.140.204
+Redwater	
DLB138	10.14.140.138
+Refrigerant_2B	
VXM00018019	10.14.142.198
VXM00018049	10.14.142.199
SUPPORT_2	10.14.141.25
+Unit_2_G_50	

Size	Date	Status
1183654	2014/01/31 13:56:38	Stopped
19651225	2014/01/16 23:22:34	Stopped
447444	2014/02/13 13:23:38	Stopped
1218959	2014/02/06 15:20:22	Stopped
11196	2014/02/14 10:11:00	Stopped

Connected to "BLADE_LC1"   Automated file collection task inactive   Com Status

Figure 3-29. Security Menu – Display Account Information

5. The account name, level, and password expiration for the current account is displayed in AppManager.



Account name: ServiceUser
Level: 11
Password Expiration: No Expiration

Comm. protocols (secure): SSH / SFTP
Account Management: Enabled

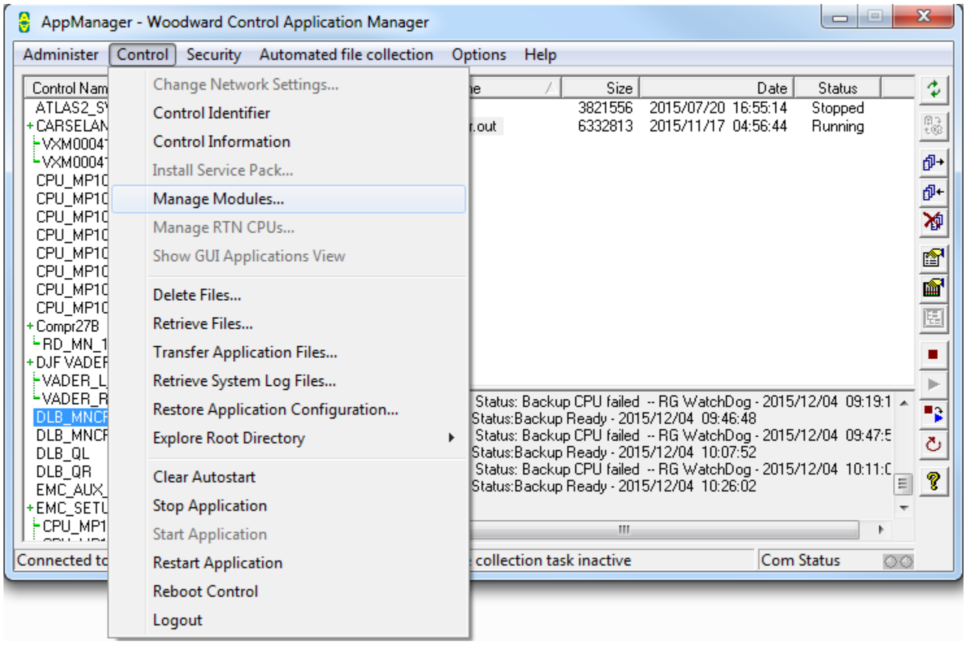
Figure 3-30. Account Information Box

Managing Modules (MicroNet Plus only)

Using AppManager, installed modules can be viewed per the following:

1. On your PC, open AppManager.exe.
2. You should see the Woodward control’s Computer Name in the AppManager window. Select the Computer Name of the control. If the control name does not appear on the list, check your connections and verify that the Link lights are on.
3. Login to the Control with a valid Account name and password.

4. Click “Control” in the top header of the AppManager window, use the pull down menu, and select “Manage Modules”:



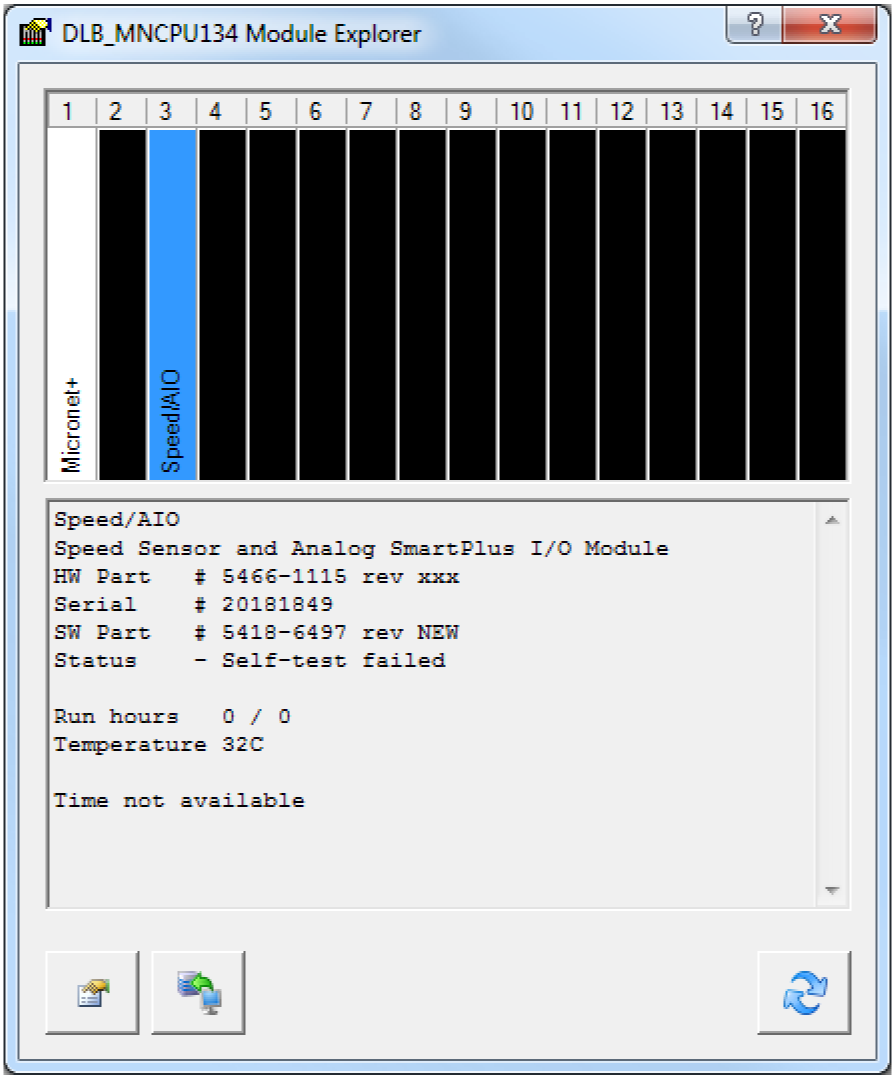
e /	Size	Date	Status
	3821556	2015/07/20 16:55:14	Stopped
.out	6332813	2015/11/17 04:56:44	Running

```
Status: Backup CPU failed -- RG WatchDog - 2015/12/04 09:19:1
Status:Backup Ready - 2015/12/04 09:46:48
Status: Backup CPU failed -- RG WatchDog - 2015/12/04 09:47:5
Status:Backup Ready - 2015/12/04 10:07:52
Status: Backup CPU failed -- RG WatchDog - 2015/12/04 10:11:0
Status:Backup Ready - 2015/12/04 10:26:02
```

Figure 3-31. Control Menu – Manage Modules

IMPORTANT **Only the SYSCON CPU can perform the manage modules task.**

A window like the following will be displayed.



```
Speed/AIO
Speed Sensor and Analog SmartPlus I/O Module
HW Part   # 5466-1115 rev xxx
Serial    # 20181849
SW Part   # 5418-6497 rev NEW
Status    - Self-test failed

Run hours   0 / 0
Temperature 32C

Time not available
```

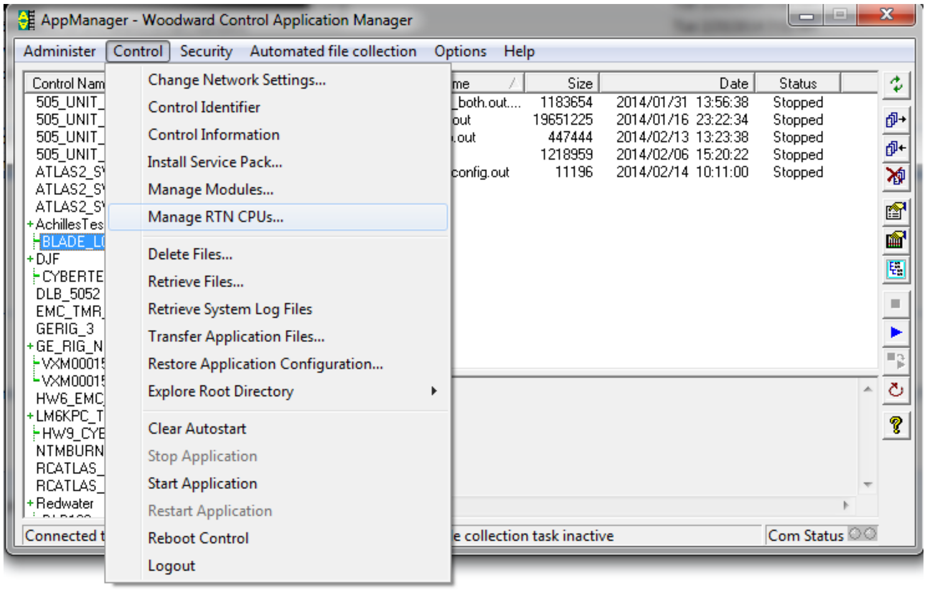
Figure 3-32. Module Explorer Window (Example)

IMPORTANT **The chassis always shows 16 slots. The CPU and new SmartPlus modules will show detailed information in the display. Black boxes indicate empty slots. Depending on the control version, other modules may show the string “<unidentified VME module>” or somewhat more detailed information.**

Manage RTN Controllers (MicroNet Plus only)

Using AppManager, RTN_CPU modules information can be viewed as follows:

1. On your PC, open AppManager.exe.
2. You should see the Woodward control's Computer Name in the AppManager window. Select the Computer Name of the control. If the control name does not appear on the list, check your connections and verify that the Link lights are on.
3. Login to the Control with a valid Account name and password.
4. Click "Control" in the top header of the AppManager window, use the pull down menu, and select "Manage RTN CPUs".



me	Size	Date	Status
both.out....	1183654	2014/01/31 13:56:38	Stopped
out	19651225	2014/01/16 23:22:34	Stopped
.out	447444	2014/02/13 13:23:38	Stopped
	1218959	2014/02/06 15:20:22	Stopped
config.out	11196	2014/02/14 10:11:00	Stopped

Figure 3-33. Control Menu – Manage RTN CPUs

IMPORTANT **Only the SYSCON CPU can perform the Manage RTN CPUs task and all Applications must be stopped.**

IMPORTANT **The SYSCON_CPU is the CPU in control of the VME bus. In Redundant systems there is a Backup CPU and a SYSCON_CPU, the SYSCON will have the green SCON LED lit on the CPU.**

5. The SYSCON CPU will use the RTN Ethernet ports to find all RTN_CPUs on the network and display them.

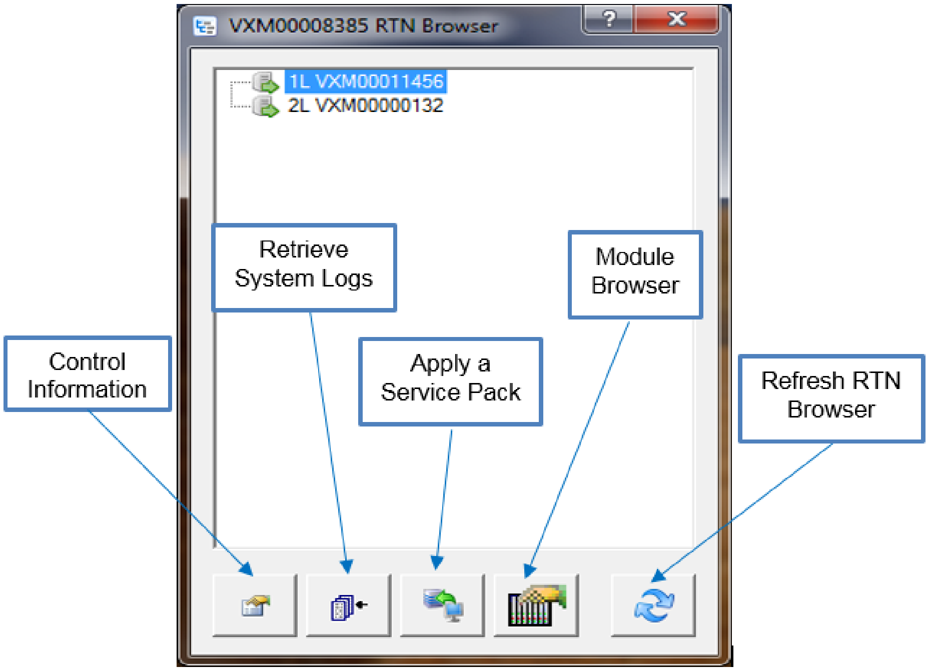
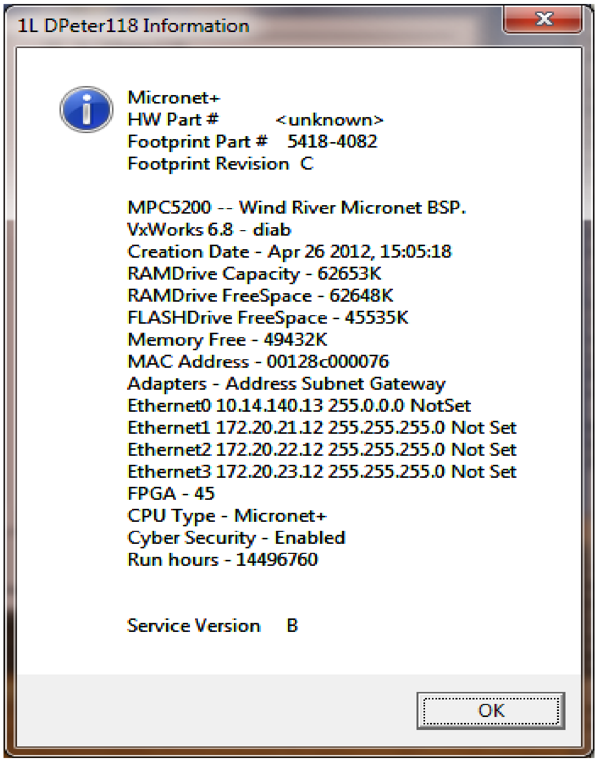


Figure 3-34. RTN Browser Window

6. Select the RTN_CPU you want, then select and click the leftmost button to show the control information for the selected RTN_CPU.


1L DPeter118 Information

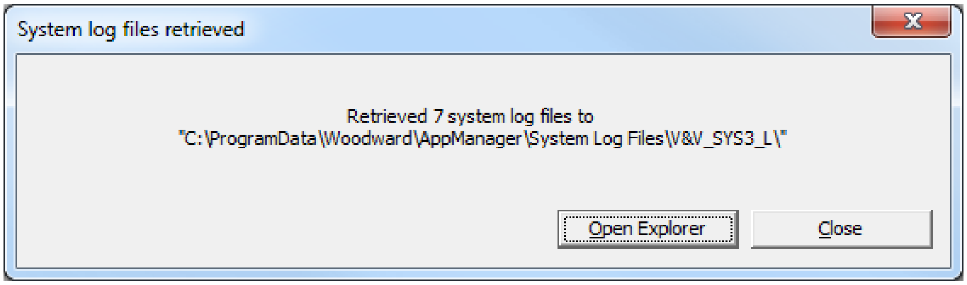
```
Micronet+
HW Part #          <unknown>
Footprint Part #    5418-4082
Footprint Revision  C

MPC5200 -- Wind River Micronet BSP.
VxWorks 6.8 - diab
Creation Date - Apr 26 2012, 15:05:18
RAMDrive Capacity - 62653K
RAMDrive FreeSpace - 62648K
FLASHDrive FreeSpace - 45535K
Memory Free - 49432K
MAC Address - 00128c000076
Adapters - Address Subnet Gateway
Ethernet0 10.14.140.13 255.0.0.0 NotSet
Ethernet1 172.20.21.12 255.255.255.0 Not Set
Ethernet2 172.20.22.12 255.255.255.0 Not Set
Ethernet3 172.20.23.12 255.255.255.0 Not Set
FPGA - 45
CPU Type - Micronet+
Cyber Security - Enabled
Run hours - 14496760

Service Version    B
```

Figure 3-35. RTN_CPU Information (Selected RTN_CPU)

7. Select the RTN_CPU you want, then select and click the second button from the left to retrieve all the system logs from the selected RTN_CPU. The files will be copied from the selected CPU to a PC folder like the following: <ProgramData folder>\Woodward\AppManager\System Log Files\<Name of RTN_CPU>*.log. (See section "***Retrieving Log Files***".)


System log files retrieved

Retrieved 7 system log files to
"C:\ProgramData\Woodward\AppManager\System Log Files\V&V_SYS3_L\"

Figure 3-36. System Logs PC Folder Location Window

8. Use the third button to install a new service pack on the selected RTN_CPU. See section "***Install Service Packs***".
9. Use the fourth button to browse the VME modules installed in the chassis. See section "***Managing Modules***". **NOTE**: Only the SYSCON RTN_CPU can view the VME modules.
10. Select the RTN_CPU you want, then "right mouse click" on it. In the pull down menu, select "Security" to display account information, enable Account Management, modify the accounts in the RTN_CPU, or change the password of the current account on the RTN_CPU (See sections "Enable Account Management" and "Network Passwords" for more information).
NOTE: You must login as the Administrator to administer accounts, and the Administrator account is only valid when Account Management is enabled.

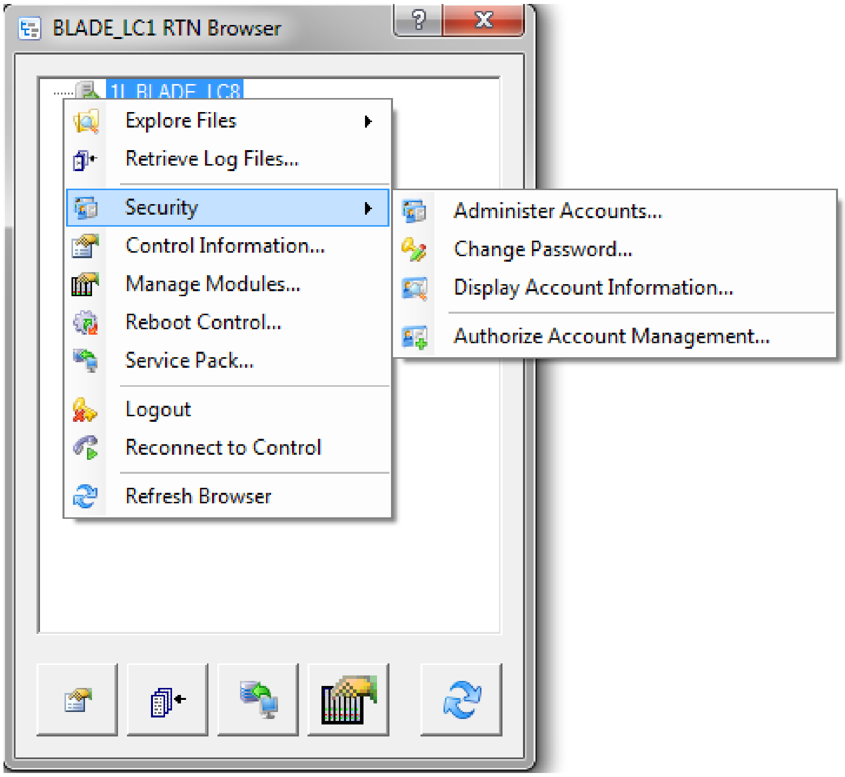


Figure 3-37. RTN Browser Window – Security Menu

IMPORTANT **While the dialog box for managing RTNs is open, the main AppManager screens will not be functional.**

Chapter 4.
GUI Application Management
(505 / Flex500 only)

Overview

505 and Flex500 controls typically come with an on-board GUI application made from Digia/Qt components. This controls all the screen information that is displayed to the user. It links to the GAP via an internal communication link to pass all required interface variables to and from the display.

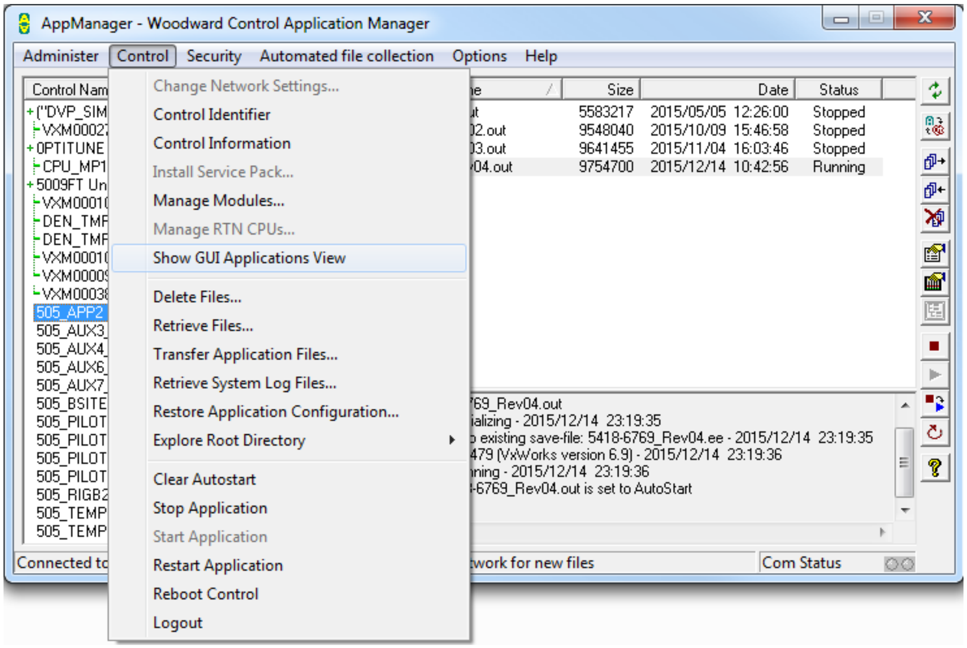
This program is automatically launched when the GAP application starts (e.g. at power-up). The GAP program MUST always be executing to run the turbine. However, the GUI program may be stopped and restarted at any time without affecting GAP or the turbine operation. This unique and useful feature of the 505/Flex500 allows the following operations to be accomplished (if needed or desired) while the 505/Flex500 control is operating the turbine:

- Change the language on the screen
- Update the GUI program (newer build revisions with improvements/enhancements)
- Upgrade the GUI program – load a custom version that may be created for a specific OEM or customer jobsite

Using AppManager to Change the GUI Application

AppManager has a mode for managing the GUI application on a 505/Flex500 control. To enter this mode, select the control in the AppManager controls list and login.

Enter the GUI Applications View by pressing the Swap Views Toolbar button or selecting "Show GUI Applications View" from the Control menu:

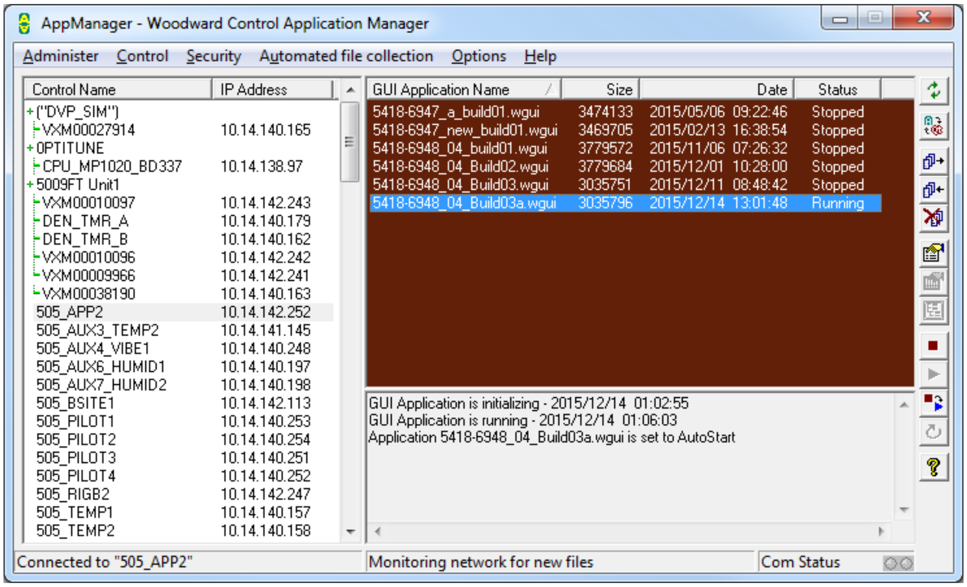


ie	Size	Date	Status
ıt	5583217	2015/05/05 12:26:00	Stopped
)2.out	9548040	2015/10/09 15:46:58	Stopped
)3.out	9641455	2015/11/04 16:03:46	Stopped
/04.out	9754700	2015/12/14 10:42:56	Running

```
'69_Rev04.out
ializing - 2015/12/14  23:19:35
o existing save-file: 5418-6769_Rev04.ee - 2015/12/14  23:19:35
479 (VxWorks version 6.9) - 2015/12/14  23:19:36
nning - 2015/12/14  23:19:36
-6769_Rev04.out is set to AutoStart
```

Figure 4-1. Control Menu – Show GUI Applications View

This will change the applications window to show GUI application files instead of GAP application files. In addition, to emphasize this distinction, the window colors are changed as shown in Figure 4-2:


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help

Control Name	IP Address
+ ("DVP_SIM")	
VXM00027914	10.14.140.165
+ OPTITUNE	
CPU_MP1020_BD337	10.14.138.97
+ 5009FT Unit1	
VXM00010097	10.14.142.243
DEN_TMR_A	10.14.140.179
DEN_TMR_B	10.14.140.162
VXM00010096	10.14.142.242
VXM00009966	10.14.142.241
VXM00038190	10.14.140.163
505_APP2	10.14.142.252
505_AUX3_TEMP2	10.14.141.145
505_AUX4_VIBE1	10.14.140.248
505_AUX6_HUMID1	10.14.140.197
505_AUX7_HUMID2	10.14.140.198
505_BSITE1	10.14.142.113
505_PILOT1	10.14.140.253
505_PILOT2	10.14.140.254
505_PILOT3	10.14.140.251
505_PILOT4	10.14.140.252
505_RIGB2	10.14.142.247
505_TEMP1	10.14.140.157
505_TEMP2	10.14.140.158

GUI Application Name	Size	Date	Status
5418-6947_a_build01.wgui	3474133	2015/05/06 09:22:46	Stopped
5418-6947_new_build01.wgui	3469705	2015/02/13 16:38:54	Stopped
5418-6948_04_build01.wgui	3779572	2015/11/06 07:26:32	Stopped
5418-6948_04_Build02.wgui	3779684	2015/12/01 10:28:00	Stopped
5418-6948_04_Build03.wgui	3035751	2015/12/11 08:48:42	Stopped
5418-6948_04_Build03a.wgui	3035796	2015/12/14 13:01:48	Running

```
GUI Application is initializing - 2015/12/14  01:02:55
GUI Application is running - 2015/12/14  01:06:03
Application 5418-6948_04_Build03a.wgui is set to AutoStart
```

Connected to "505_APP2" | Monitoring network for new files | Com Status

Figure 4-2. Applications Window GUI Applications Files

The menu commands, which are used to transfer, start and stop GAP application files have analogous menu items for transferring, starting, and stopping GUI application files (files that end in ".wgui"):

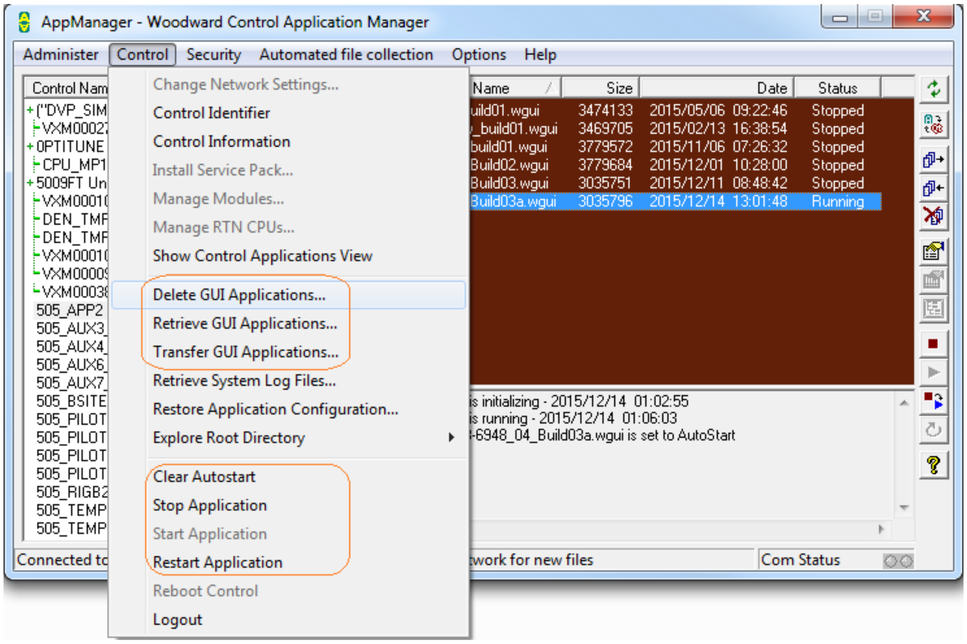

AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help
Change Network Settings...
Control Identifier
Control Information
Install Service Pack...
Manage Modules...
Manage RTN CPUs...
Show Control Applications View
Delete GUI Applications...
Retrieve GUI Applications...
Transfer GUI Applications...
Retrieve System Log Files...
Restore Application Configuration...
Explore Root Directory
Clear Autostart
Stop Application
Start Application
Restart Application
Reboot Control
Logout

Figure 4-3. Control Menu – GUI Applications Files Menu Items

The “Send”/”Retrieve”/”Delete” toolbar buttons for sending, retrieving and deleting GAP applications are mapped to GUI applications in this mode:

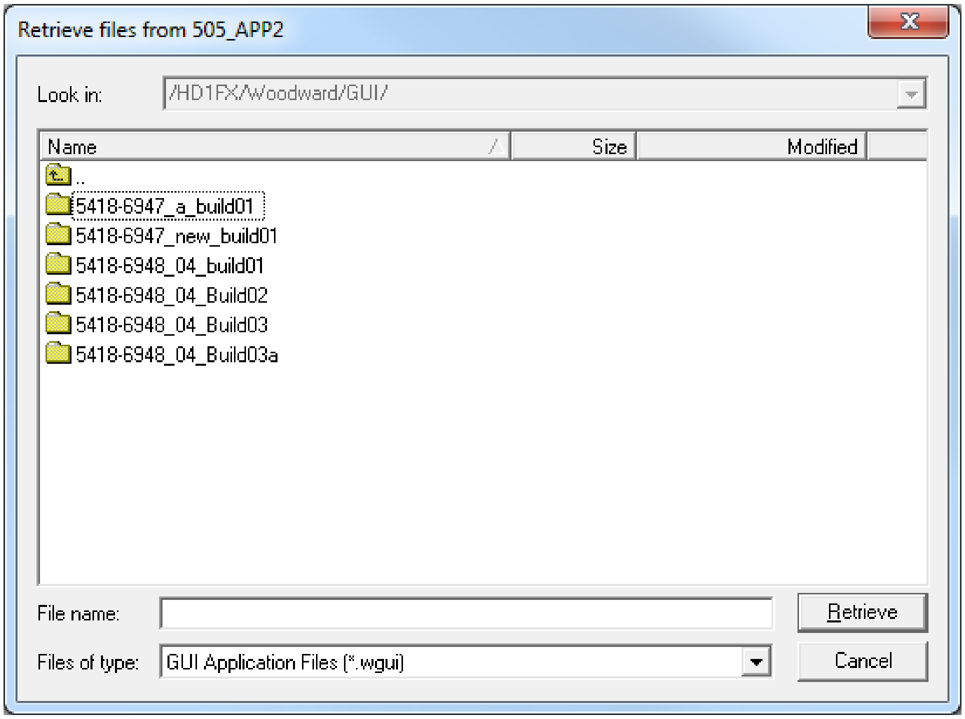
Similarly, the “Stop”/“Start”/”Restart” toolbar buttons for starting, stopping and restarting (stopping then starting) GAP applications are mapped to GUI applications in this mode:

Sending GUI Application Files

When sending GUI application files, you should send files with the “.wgui” extension. Additional files may include settings (“.ini”) files and custom tag name files. These will automatically be sent to the correct folder on the control (<ROOT>/Woodward/GUI).

Retrieving GUI Application Files

When retrieving GUI application files, a window like Figure 4-4 displays:



Retrieve files from 505_APP2

Look in: /HD1FX/Woodward/GUI/

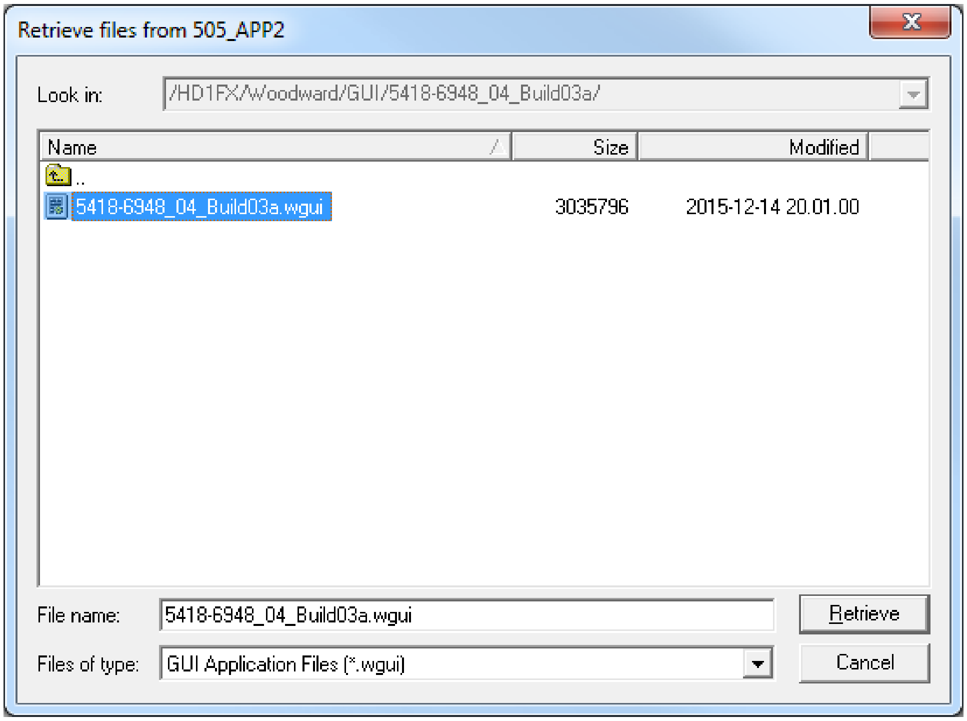
Name	Size	Modified
..		
5418-6947_a_build01		
5418-6947_new_build01		
5418-6948_04_build01		
5418-6948_04_Build02		
5418-6948_04_Build03		
5418-6948_04_Build03a		

File name:

Files of type: GUI Application Files (*.wgui)

Figure 4-4. GUI Application File Retrieval Window

It is necessary to double-click on one of these folders to reveal the file to retrieve (the “.wgui” file):



Retrieve files from 505_APP2

Look in: /HD1FX/Woodward/GUI/5418-6948_04_Build03a/

Name	Size	Modified
..		
5418-6948_04_Build03a.wgui	3035796	2015-12-14 20.01.00

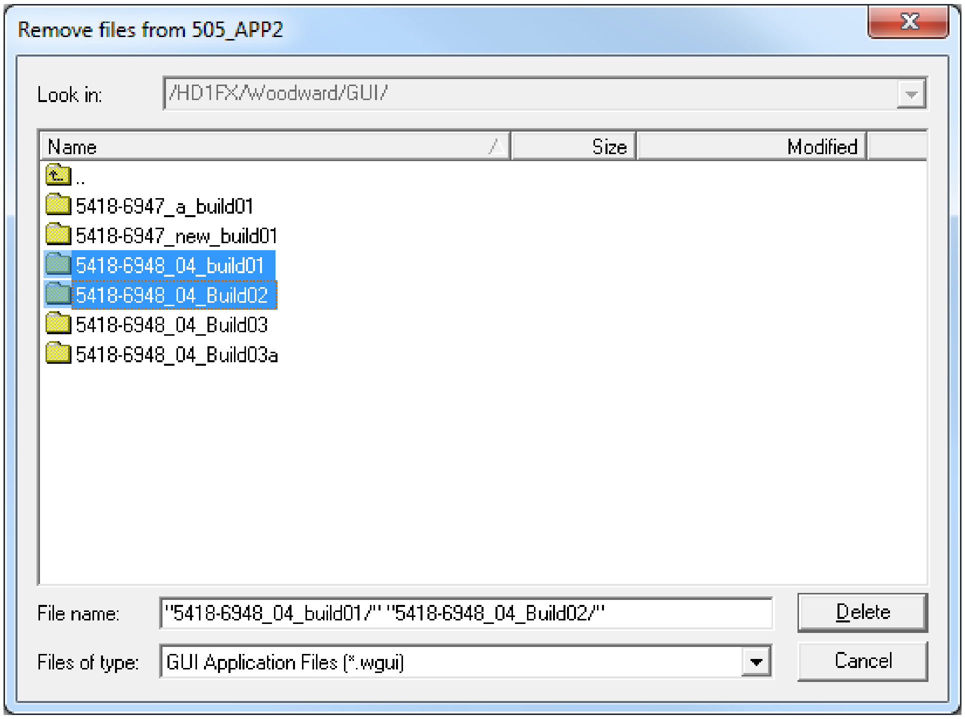
File name: 5418-6948_04_Build03a.wgui

Files of type: GUI Application Files (*.wgui)

Figure 4-5. .wgui File Retrieval Window

Deleting GUI Application Files

When deleting GUI applications, the folders may be directly selected:



Remove files from 505_APP2

Look in: /HD1FX/Woodward/GUI/

Name	Size	Modified
..		
5418-6947_a_build01		
5418-6947_new_build01		
5418-6948_04_build01		
5418-6948_04_Build02		
5418-6948_04_Build03		
5418-6948_04_Build03a		

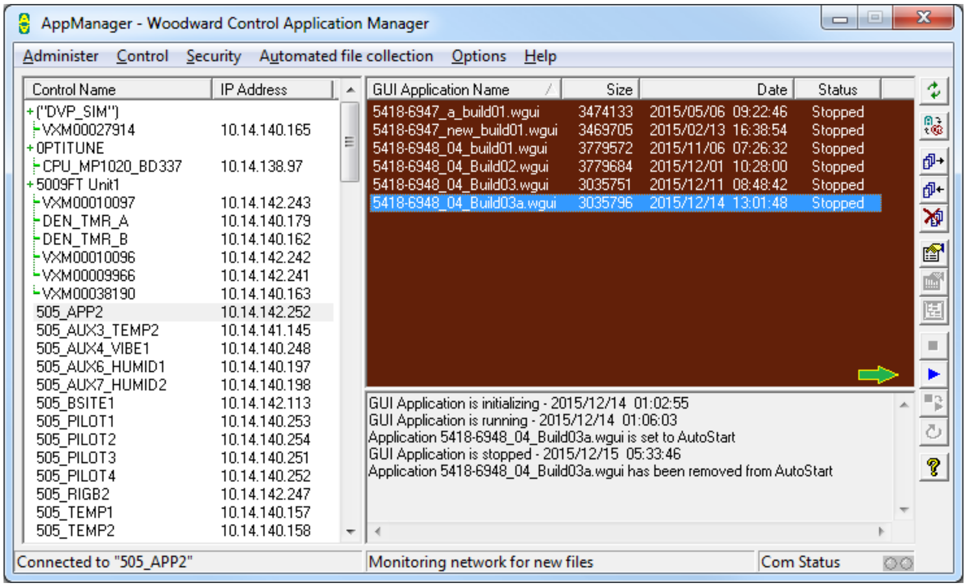
File name: "5418-6948_04_build01/" "5418-6948_04_Build02/"

Files of type: GUI Application Files (*.wgui)

Figure 4-6. GUI Application File Deletion Window

Starting a GUI Application

To start a GUI application, first ensure that all GUI applications are stopped. Then select the desired GUI application and press the start button ▶ (the stop and restart buttons are disabled):


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help

Control Name	IP Address
+("DVP_SIM")	
VXM00027914	10.14.140.165
+OPTITUNE	
CPU_MP1020_BD337	10.14.138.97
+5009FT Unit1	
VXM00010097	10.14.142.243
DEN_TMR_A	10.14.140.179
DEN_TMR_B	10.14.140.162
VXM00010096	10.14.142.242
VXM00009966	10.14.142.241
VXM00038190	10.14.140.163
505_APP2	10.14.142.252
505_AUX3_TEMP2	10.14.141.145
505_AUX4_VIBE1	10.14.140.248
505_AUX6_HUMID1	10.14.140.197
505_AUX7_HUMID2	10.14.140.198
505_BSITE1	10.14.142.113
505_PILOT1	10.14.140.253
505_PILOT2	10.14.140.254
505_PILOT3	10.14.140.251
505_PILOT4	10.14.140.252
505_RIGB2	10.14.142.247
505_TEMP1	10.14.140.157
505_TEMP2	10.14.140.158

GUI Application Name	Size	Date	Status
5418-6947_a_build01.wgui	3474133	2015/05/06 09:22:46	Stopped
5418-6947_new_build01.wgui	3469705	2015/02/13 16:38:54	Stopped
5418-6948_04_build01.wgui	3779572	2015/11/06 07:26:32	Stopped
5418-6948_04_Build02.wgui	3779684	2015/12/01 10:28:00	Stopped
5418-6948_04_Build03.wgui	3035751	2015/12/11 08:48:42	Stopped
5418-6948_04_Build03a.wgui	3035796	2015/12/14 13:01:48	Stopped

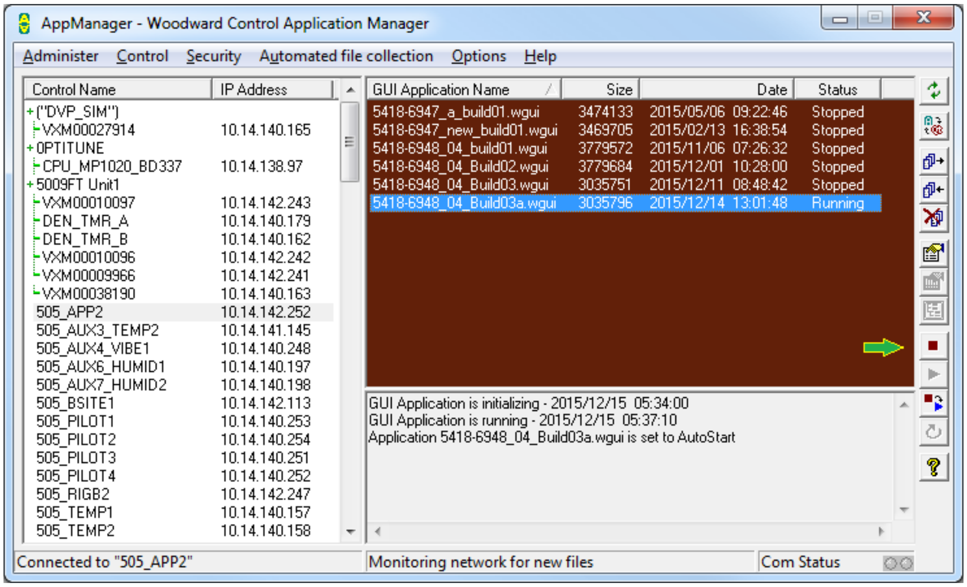
```
GUI Application is initializing - 2015/12/14  01:02:55
GUI Application is running - 2015/12/14  01:06:03
Application 5418-6948_04_Build03a.wgui is set to AutoStart
GUI Application is stopped - 2015/12/15  05:33:46
Application 5418-6948_04_Build03a.wgui has been removed from AutoStart
```

Connected to "505_APP2" | Monitoring network for new files | Com Status

Figure 4-7. GUI Applications Stopped Status

Stopping a GUI Application

To stop a running GUI application, select the running GUI application, and press the stop button ■ (the start button is disabled):


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help

Control Name	IP Address
+("DVP_SIM")	
VXM00027914	10.14.140.165
+OPTITUNE	
CPU_MP1020_BD337	10.14.138.97
+5009FT Unit1	
VXM00010097	10.14.142.243
DEN_TMR_A	10.14.140.179
DEN_TMR_B	10.14.140.162
VXM00010096	10.14.142.242
VXM00009966	10.14.142.241
VXM00038190	10.14.140.163
505_APP2	10.14.142.252
505_AUX3_TEMP2	10.14.141.145
505_AUX4_VIBE1	10.14.140.248
505_AUX6_HUMID1	10.14.140.197
505_AUX7_HUMID2	10.14.140.198
505_BSITE1	10.14.142.113
505_PILOT1	10.14.140.253
505_PILOT2	10.14.140.254
505_PILOT3	10.14.140.251
505_PILOT4	10.14.140.252
505_RIGB2	10.14.142.247
505_TEMP1	10.14.140.157
505_TEMP2	10.14.140.158

GUI Application Name	Size	Date	Status
5418-6947_a_build01.wgui	3474133	2015/05/06 09:22:46	Stopped
5418-6947_new_build01.wgui	3469705	2015/02/13 16:38:54	Stopped
5418-6948_04_build01.wgui	3779572	2015/11/06 07:26:32	Stopped
5418-6948_04_Build02.wgui	3779684	2015/12/01 10:28:00	Stopped
5418-6948_04_Build03.wgui	3035751	2015/12/11 08:48:42	Stopped
5418-6948_04_Build03a.wgui	3035796	2015/12/14 13:01:48	Running

```
GUI Application is initializing - 2015/12/15  05:34:00
GUI Application is running - 2015/12/15  05:37:10
Application 5418-6948_04_Build03a.wgui is set to AutoStart
```

Connected to "505_APP2" | Monitoring network for new files | Com Status

Figure 4-8. Stopping a GUI Application which is Running

Chapter 5.
Secured Application Management
(Secured Applications Only)

Overview

The MicroNet Plus Secured Application controls are similar to the MicroNet Plus controls. All exceptions are noted in this manual. A Secured Application prevents execution of the application on unauthorized MicroNet plus CPUs. A Secured Application also helps to protect recovery of intellectual property through reverse engineering the GAP/Coder output file.

Creating a Secured Application

The process for creating a Secured Application software is the same as in the previous section “Creating the Application” with the following additions. After the .out file is created, the Secured Application tool is used to encrypt the application, authorizing the application to only run on one or more selected CPUs. The following figure illustrates the flow of the AEF and .OUT.ENC files between the CPU, GAP/Coder, AppManager, and the Secured Application Tool.

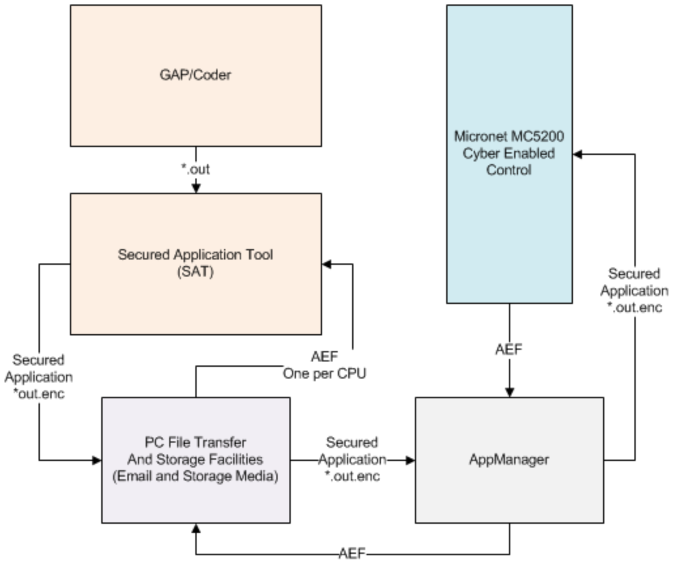


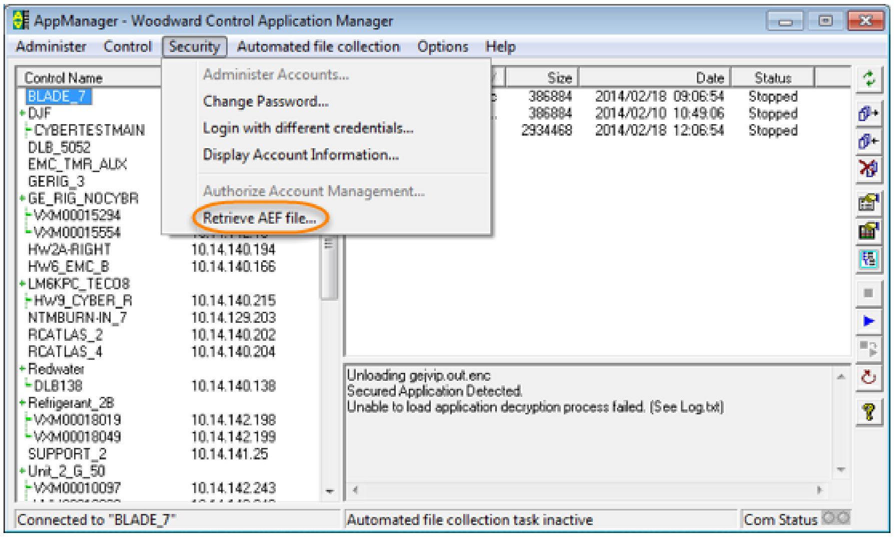
Figure 5-1. Secured Application Configuration

Authorizing a Secured Application

The following steps describe the process for authorizing the application to run on one or more selected CPUs, resulting in the Secured Application.

1. Retrieve the Authorization Encryption Files (AEF) for the CPUs that are authorized to run the Application. AEFs may be retrieved by using AppManager (version 3.06 or later) to connect to the control and retrieve the CPU’s AEF by choosing the “Retrieve AEF file …” under the “Security” menu as shown below.

   Note: AEFs require no special measures to protect their contents from becoming publicly known. They may be stored in locations that make it convenient for later use if access to the CPU is not always available.


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help
Administer Accounts...
Change Password...
Login with different credentials...
Display Account Information...
Authorize Account Management...
Retrieve AEF file...

Control Name	
BLADE_7	
DJF	
CYBERTESTMAIN	
DLB_5052	
EMC_TMR_AUX	
GERIG_3	
GE_RIG_NOCYBR	
VXM00015294	
VXM00015554	
HW2A-RIGHT	10.14.140.194
HW6_EMC_B	10.14.140.166
LM6KPC_TEC08	
HW9_CYBER_R	10.14.140.215
NTMBURN-IN_7	10.14.129.203
RCATLAS_2	10.14.140.202
RCATLAS_4	10.14.140.204
Redwater	
DLB138	10.14.140.138
Refrigerant_28	
VXM00018019	10.14.142.198
VXM00018049	10.14.142.199
SUPPORT_2	10.14.141.25
Unit_2_G_50	
VXM00010097	10.14.142.243

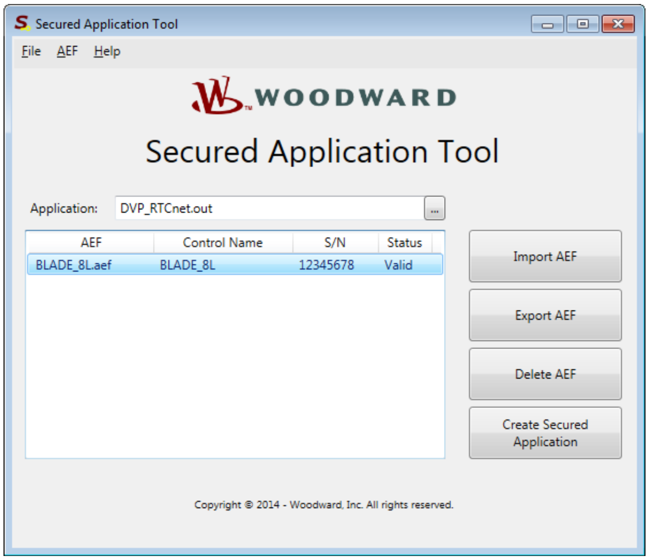
Size	Date	Status
386884	2014/02/18 09:06:54	Stopped
386884	2014/02/10 10:49:06	Stopped
2934468	2014/02/18 12:06:54	Stopped

```
Unloading gejvip.out.enc
Secured Application Detected.
Unable to load application decryption process failed. (See Log.txt)
```

Connected to "BLADE_7" | Automated file collection task inactive | Com Status

Figure 5-2. Security Menu – Retrieve AEF File

2. Run the Secured Application Tool. See the “Getting Started” and “Help” sub-menus under the main “Help” menu on how to generate the Secured Application. The basic steps are to use the “Import AEF” button to import one or more AEFs, select the application to be secured, select from one or more of the previously imported AEF’s by clicking on them, and then use the “Create Secured Application” button to generate the Secured Application.



Application: DVP_RTCnet.out

AEF	Control Name	S/N	Status
BLADE_8L.aef	BLADE_8L	12345678	Valid

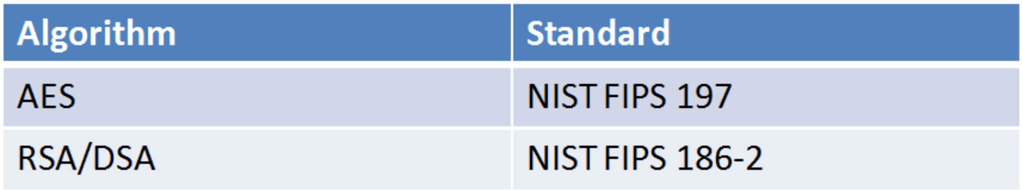
Copyright © 2014 - Woodward, Inc. All rights reserved.

Figure 5-3. Secured Application Tool Window

Cryptographic Technology

The cryptographic algorithms used to create Secured Applications are listed in Table 3-1 along with the applicable NIST FIPS standards. These algorithms form the basis of Public Key Cryptography, which is a well-established technology used by the US Government and many institutions. Public Key Cryptography forms the underpinning for Internet standards for secure communications, which everyone who accesses their bank account online has used. Public Key Cryptography enables protection of the customer's Intellectual Property as well as the ability to authorize the Secured Application to only run on selected CPUs. This is accomplished without needing to share secret information between the Secured Application Tool and the MicroNet Plus Secured Application CPU.

Table 5-1. Standard Cryptographic Algorithms



Algorithm	Standard
AES	NIST FIPS 197
RSA/DSA	NIST FIPS 186-2

User responsibilities for Protecting Secured Applications

The user has the responsibility to administratively control access to the unsecured (not encrypted) files used and produced by GAP/Coder, including the output file that is used to create a Secured Application.

The user has the responsibility to collect, distribute, and manage the Authorization Encryption Files ("AEF") retrieved from Woodward MicroNet Plus Secured Application CPUs. Access to AEFs does not need to be controlled.

The user has the responsibility to manage the administrative process by which the MicroNet Plus Secured Application CPUs are authorized to run a Secured Application.

The user has the responsibility to control physical and communication bus access to the MicroNet Plus Secured Application CPUs.

IMPORTANT

Protecting the Secured Application from unauthorized parties requires the user to control physical and network access to the Secured Application CPU as well as to the files used and produced by GAP/Coder.

Downloading and Running a Secured Application

The process for downloading and running Secured Application software is the same as in the next section "Downloading and Running the Application", with the difference that the Secured Application file ends in .OUT.ENC instead of .OUT.

A Secured Application control will only run files ending in .OUT.ENC that were authorized for that control. A Secured Application control cannot run files ending in .OUT and cannot run .OUT.ENC files that were not authorized for that control.

Chapter 6.
SOS / Control Assistant

Overview

WinPanel is part of Control Assistant and uses the Servlink OPC Server (SOS) to communicate to the control. No action needs to be taken in your GAP application to support this.

WinPanel has the following features:

- Hierarchical Tree View of available data
- Read and write access to variables through SOS
- Loading and saving of different configurations.

IMPORTANT **The Watch Window tools have been deprecated and have been replaced with WinPanel, which is part of Control Assistant.**

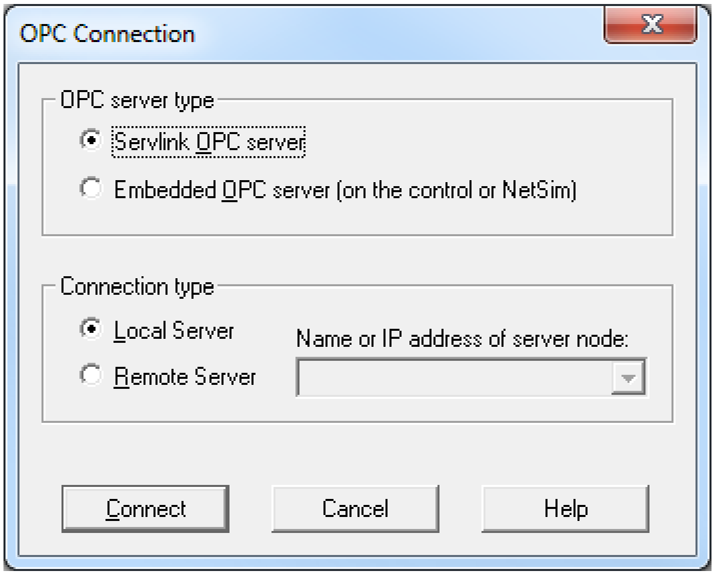
Installing the SOS Servlink OPC Server

The SOS Servlink OPC Server is a stand-alone tool that can be downloaded from the Woodward web site. It does not require a software license to run.

To install the SOS Servlink OPC Server, it is necessary to have the Microsoft ".NET" framework version 4.0 or greater on your PC. The ".NET" framework is generally available on modern PCs. If it is not already on your PC, an install program is available from Microsoft. After installing the Microsoft program, run the installation program for the SOS Servlink OPC Server. The installation program will guide you through various choices in the installation process.

Running the SOS Servlink OPC Server

If you attempt to make an OPC connection with a tool like Monitor GAP or Control Assistant, you will see example dialog in Figure 6-1:



OPC Connection

OPC server type
- ● Servlink OPC server
- ○ Embedded OPC server (on the control or NetSim)

Connection type
- ● Local Server
- ○ Remote Server

Name or IP address of server node:

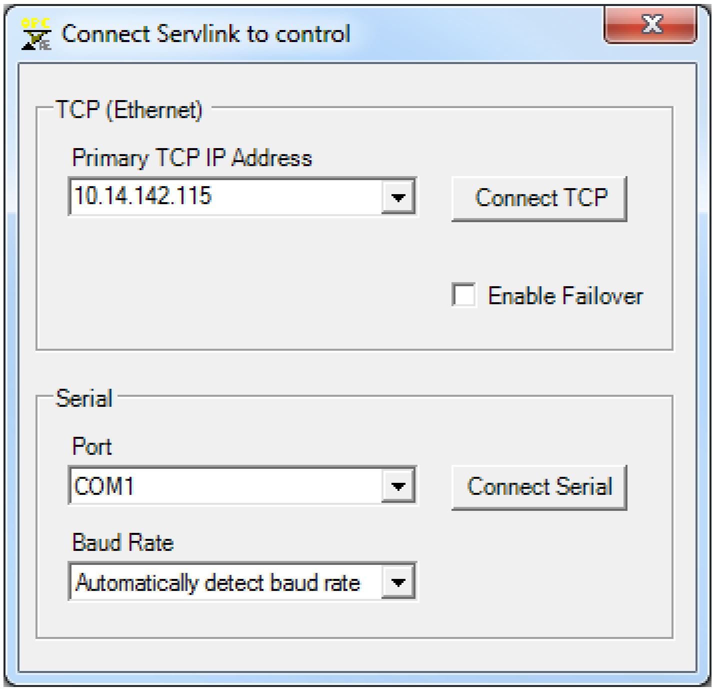
Figure 6-1. OPC Connection Dialog Window

If you select the options, “Servlink OPC server” and “Local Server”, as above, it will cause the SOS Servlink OPC server to run on your machine. If it was already running from a previous use, it will use that instance.

IMPORTANT

SOS and OPC client tools like Control Assistant and Monitor GAP must run at the same “elevation level” in Windows. If you are running these tools in a Windows version like Vista, 7, 8, or 10, each tool must be *run as* Administrator or *not run as* Administrator. By default, each will run as “*not Administrator”*. For more information about program elevation levels, consult your Windows documentation or the SOS Help document.

If this is the first time the SOS Servlink OPC Server has run on your machine, you will see an interface like the following:



10.14.142.115

COM1

Automatically detect baud rate

Figure 6-2. SOS Servlink OPC Server Interface

Most likely, you will want to use the “Connect TCP” option, because it is faster and requires less configuration than the “Connect Serial” option. To connect TCP, it is necessary to type in or select the IP Address of the control(s) you want to communicate with.

After the control has connected, you can close or minimize the Servlink OPC server window. It will go to the system tray (probably at the bottom-right of your PC monitor) where it looks something like this:

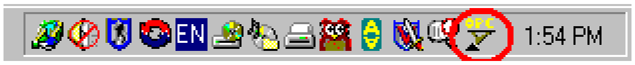
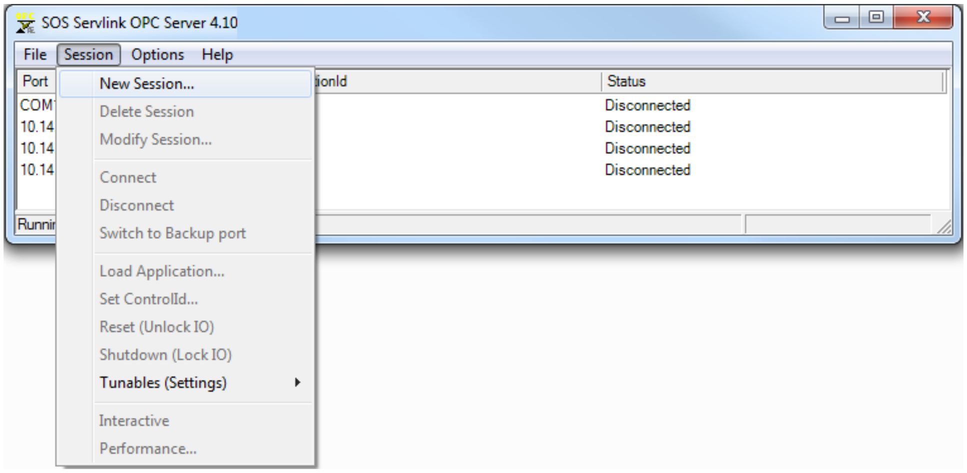


Figure 6-3. System Tray – Servlink OPC Server Window Icon

The next time you run an application that uses the SOS Servlink OPC server; it will attempt to resume connections to the same controls as in the previous session.

If you want to modify the connections or operating parameters of the Servlink OPC Server, double-click on the icon in the system tray at any time. To add or remove connections, select from the Session menu:

The “New Session” command will result in a dialog that allows you to select a new TCP or Serial connection.



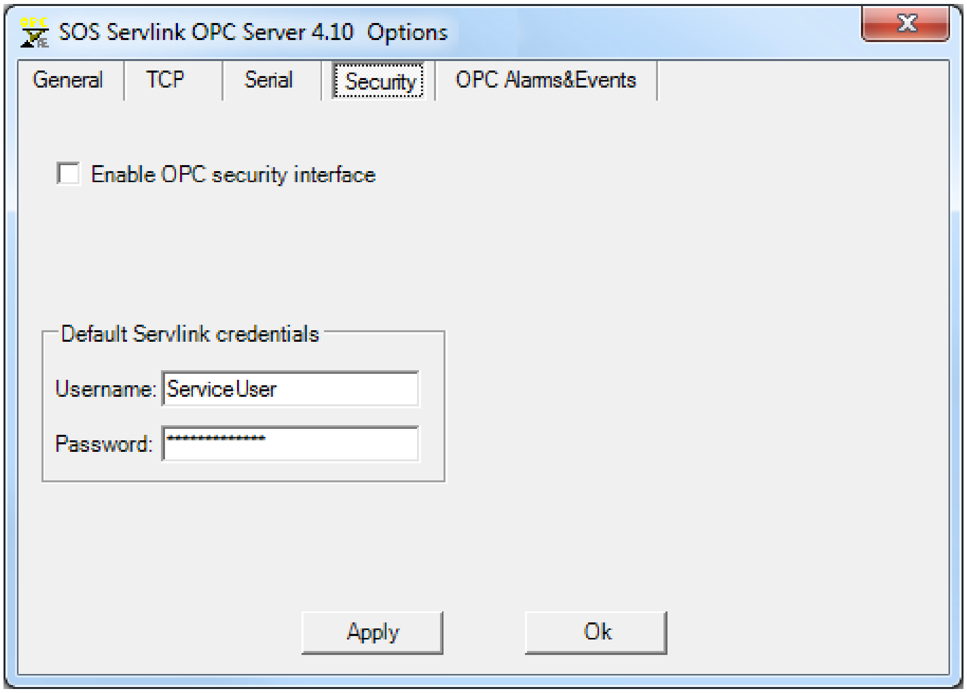
Port	ionId	Status
COM		Disconnected
10.14		Disconnected
10.14		Disconnected
10.14		Disconnected

Figure 6-4. Session Menu New Session Options

The sessions that are running in the Servlink OPC server determine which controls’ values your OPC clients (like Control Assistant and Monitor GAP) will have access to.

Using SOS Servlink OPC Server w/CPUs Supporting Account Management

Under the Options menu, there is a “Security” tab used to interface with CPUs that support Account Management, such as Cyber Secure CPUs.



□ Enable OPC security interface

Default Servlink credentials

Username: ServiceUser

Password: **************

Figure 6-5. Options Menu Security Interface Tab

SOS will establish a connection to the control if a valid Account name and password are supplied and the “Enable OPC security interface” is NOT checked.

If the Enable OPC security interface IS checked, SOS will defer the Account name and password credentials to the connecting OPC client program. Currently GAP3 and Control Assistant 4 support this interface. For tools that are not OPC Security aware, like old versions of Control Assistant or GAP, the Enable OPC security interface should not be checked and a valid Account name and password must be supplied in SOS.

- If the control is Cyber Secure, the connection will be established over a secure SSH connection.
- If the control is non-Cyber Secure, the connection will be established over a standard non-secure (TCP) connection.

IMPORTANT **See the SOS help for additional information.**

Using SOS Servlink OPC Server w/Non-Woodward OPC Client Tools

The client tool should have an interface for selecting an installed OPC server. The name of the Woodward Servlink OPC Server is

“Woodward.ServlinkOpcDa.1”

The HMI tool can launch Woodward’s Servlink OPC Server or it can be launched manually by running the file “SOS.exe” from the install directory. Connections can be managed as in the above example (“Running the SOS Servlink OPC Server”).

The client tool should also have an interface for selecting values. The Servlink OPC values in GAP follow the following naming pattern:

“<Control ID>.<GAP tag name>”

For example “VXM11184.EMDRP_RMP.IN_RAMP.RAMP”

If you previously had a Woodward control with an embedded OPC server connected to an OPC-based HMI, you will have to update the OPC server name and tags to match these conventions.

For more information about using SOS with non-Woodward OPC client tools, please consult the Help in the SOS Servlink OPC Server.

Using WinPanel in Control Assistant

WinPanel is supported by the MicroNet, 505, Flex500, and Atlas-II. First, launch Control Assistant and then activate the WinPanel through the Toolbar item with the eyes:

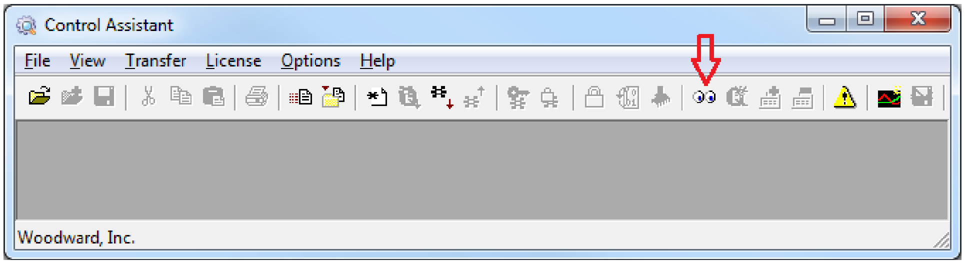
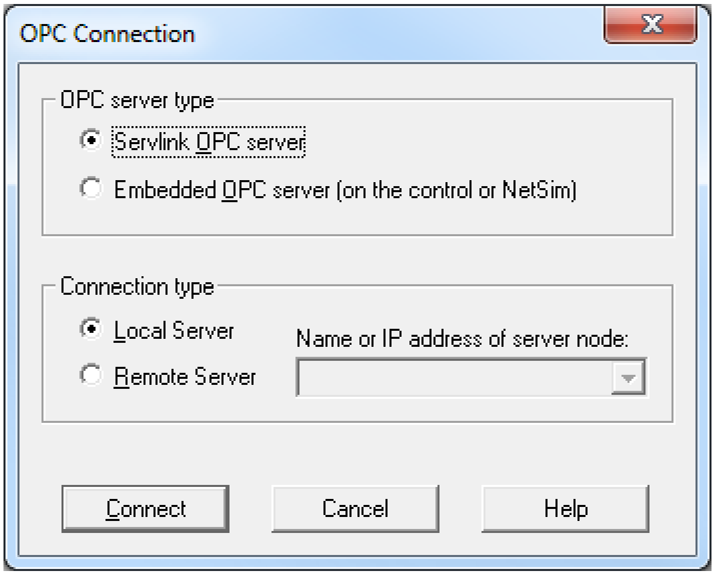


Figure 6-6. Control Assistant WinPanel Launch Icon

This will launch the OPC client dialog mentioned before. Select *Servlink OPC server* and *Local Server*:



OPC Connection

OPC server type

● Servlink OPC server
○ Embedded OPC server (on the control or NetSim)

Connection type

● Local Server
○ Remote Server

Name or IP address of server node:

Figure 6-7. OPC Client Dialog Window

After connecting, WinPanel will be open in Control Assistant. Some menu functions may be disabled (gray) because of the state of the system. If a right mouse click is performed on the target CPU, the following functions are displayed (see Figure 6-8):

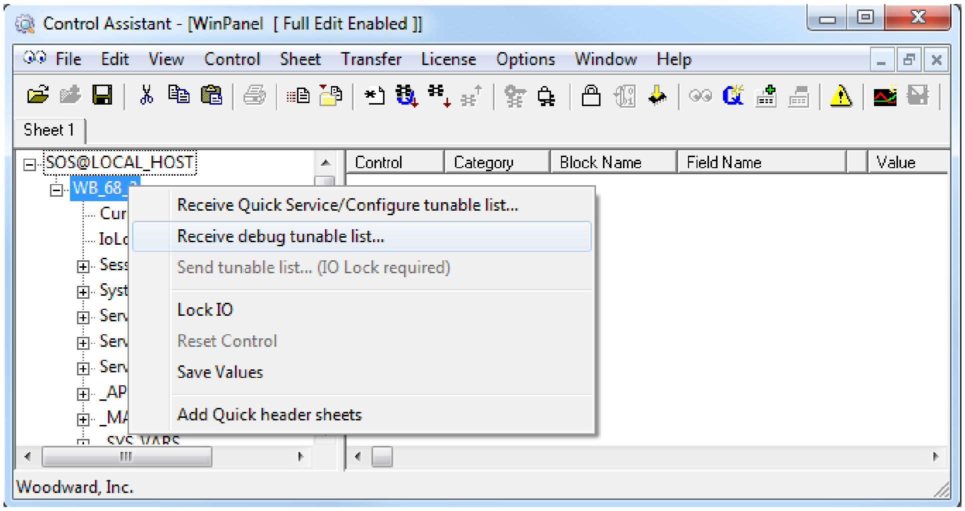
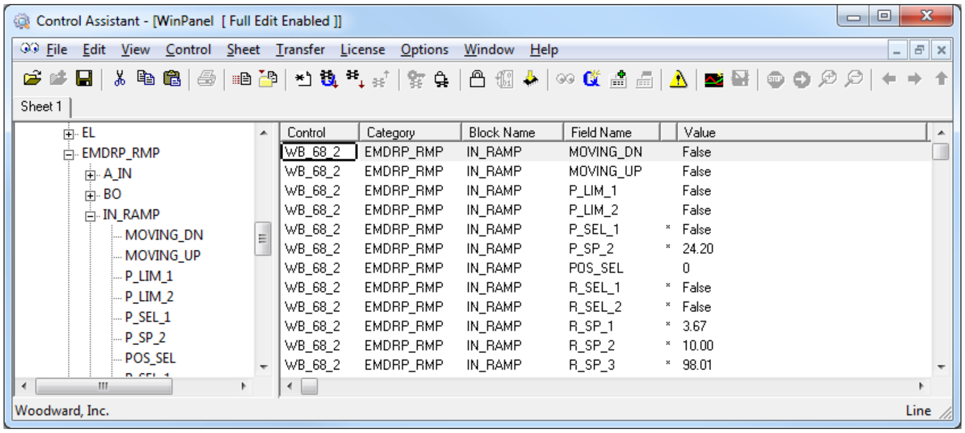


Figure 6-8. WinPanel Screen

To display application values, select the control you want to view and expand nodes in the explorer window tree. You may drag fields, blocks, or entire categories to the value display window on the right side.



Control	Category	Block Name	Field Name		Value
WB_68_2	EMDRP_RMP	IN_RAMP	MOVING_DN		False
WB_68_2	EMDRP_RMP	IN_RAMP	MOVING_UP		False
WB_68_2	EMDRP_RMP	IN_RAMP	P_LIM_1		False
WB_68_2	EMDRP_RMP	IN_RAMP	P_LIM_2		False
WB_68_2	EMDRP_RMP	IN_RAMP	P_SEL_1	*	False
WB_68_2	EMDRP_RMP	IN_RAMP	P_SP_2	*	24.20
WB_68_2	EMDRP_RMP	IN_RAMP	POS_SEL		0
WB_68_2	EMDRP_RMP	IN_RAMP	R_SEL_1	*	False
WB_68_2	EMDRP_RMP	IN_RAMP	R_SEL_2	*	False
WB_68_2	EMDRP_RMP	IN_RAMP	R_SP_1	*	3.67
WB_68_2	EMDRP_RMP	IN_RAMP	R_SP_2	*	10.00
WB_68_2	EMDRP_RMP	IN_RAMP	R_SP_3	*	98.01

Figure 6-9. Viewing Values in WinPanel

WinPanel Functions

“Receive debug tunable list”

- Used to retrieve the current tunable values from the control.

“Send Tunable List” IO Lock Required

- Used to send the open tunable file values to the control. The control must be shut down (IO Lock), and a tunable list window must be open. If more than one tunable list window is open, it may be necessary to select from a list of available tunable lists.

"LockIO"

- Sets the IO LOCK on the VME bus, which disables all output modules.

“Reset Control”

- Used to release the IO LOCK and return the control to operating mode.

“Save Values”

- This saves the GAP application’s “Tunable Values” to the control in its Woodward\Applications\filename.ee file.

Tunables Management

"Tunables" are the application’s variables that are changeable on-line (without the need to modify the GAP application). The application programmer may make certain Boolean, analog, or integer values tunable by adding an asterisk prefix (*) in the GAP application and appending a tunable range.

Tunable values are stored on the control as an .EE file in binary format. This file is not transferred with the .OUT file when AppManager’s [Retrieve App Files] or [Transfer App Files] commands are executed, but may be manually retrieved (for archiving purposes) using AppManager’s [Retrieve App Files] command.

To view and modify individual tunable values while the application is running, use Woodward’s Control Assistant or Monitor GAP tools.

There are several ways to capture and adjust tunable values in GAP applications, and there are two ways to view (in one document) all the tunable values from an application that have been loaded into a control.

IMPORTANT

As part of a best practices commissioning process, Woodward recommends that any saved tunable settings be validated (following any Save operation), by power cycling the control and re-verifying the values.

To capture and adjust tunable values in one document from an application that has been loaded into a control:

No GAP setup is required. Use Control Assistant to retrieve a tunable configuration (".tc") file. This may be done from a menu or toolbar command in the WinPanel window of Control Assistant. Then, use the Control Assistant tool to transfer the ".tc" tunable list for viewing, comparing, sorting, and uploading.

To capture and adjust tunable values in GAP applications:

1. In GAP, select "Tunable List…" from the File menu. This allows exporting to a ".tc" file that can be opened in a text editor. It will show the name, current value and the High Limit and Low Limit. You can change values, save the file, and use Control Assistant to transfer it to the control running this application.
2. Import tunables to GAP from a ".tc" file. If the control tunable values have been adjusted and now you want to get those changes into the source GAP application file, select "Import Tunables…" from the GAP File menu.

IMPORTANT

As part of a best practices commissioning process, Woodward recommends that any saved tunable settings be validated (following any save operation), by power cycling the control and re-verifying the values.

IMPORTANT

For more information on WinPanel and Control Assistant, consult the help document in Control Assistant.

Chapter 7.
Automatic Datalog File Collection

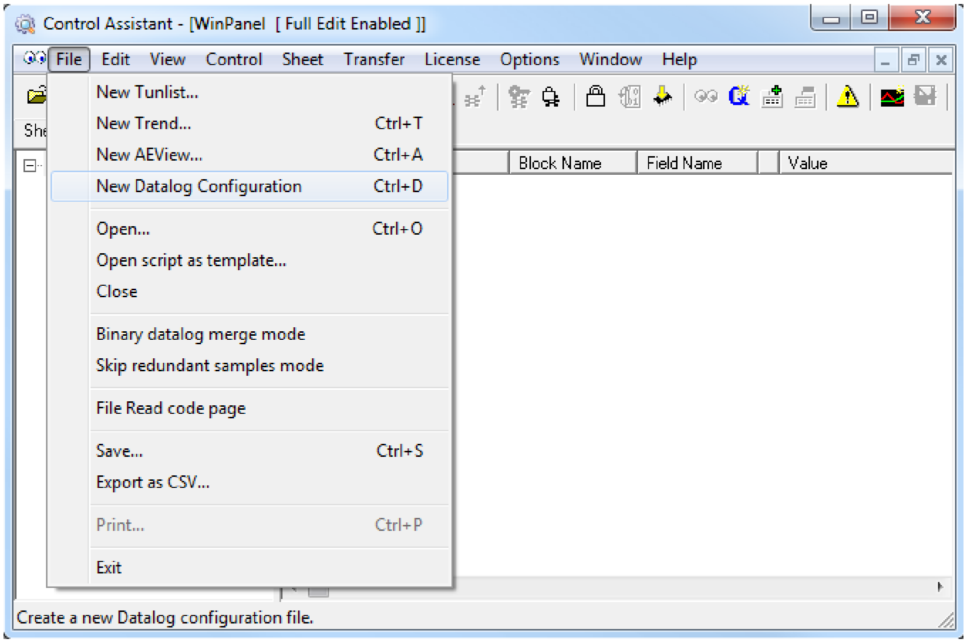
Overview

Datalog files are files that preserve a history of values for chosen variables in the GAP application. A GAP application may be configured to produce these files based on event triggers or to produce them continuously. For information about how to configure a GAP application to produce Datalog files, consult the GAP Block Help for the DATA_LOG and DATA_LOG_M blocks.

Modifying the collected variables for the DATA_LOG_M block

The set of variables collected by the DATA_LOG block is defined statically in the GAP application. The set of variables collected by the DATA_LOG_M may also be defined in the GAP application, but the set may be extended while the application is running. To extend the set of values for a DATA_LOG_M block, create a Datalog extension file, reference that file in the DATA_LOG_M block (“FILE_NAME” field), and load that file to the Applications folder of the control. This file is essentially a list of fully qualified GAP name / tagname value pairs and has the extension “.logConfig”.

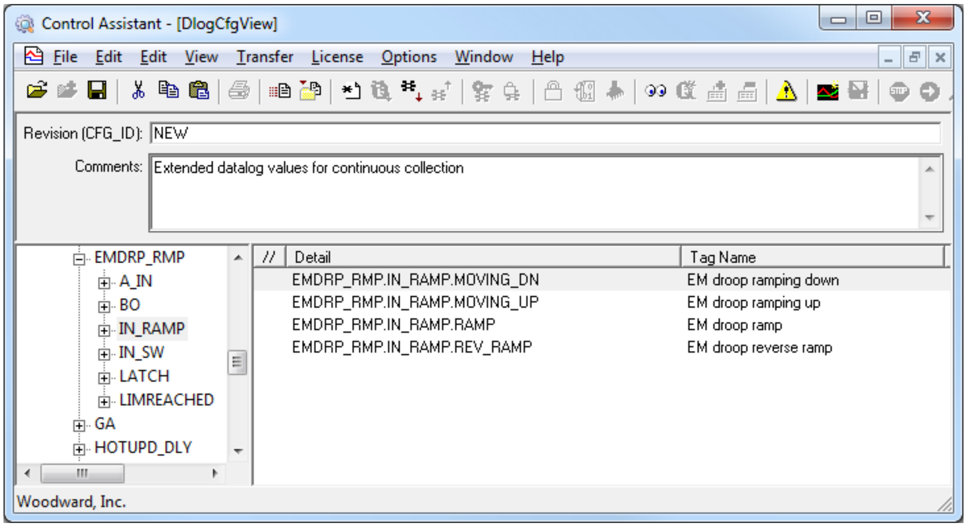
Control Assistant has a utility for building these files (File menu / New Datalog Configuration):



Create a new Datalog configuration file.

Figure 7-1. File Menu – New Datalog Configuration

With this tool connected to SOS, values may be dragged from the browse tree to the configuration. The “Detail” name should match a fully qualified variable name in the GAP application, and the “TagName” may be set to an implementation-friendly name.



Revision (CFG_ID): NEW

Comments: Extended datalog values for continuous collection

//	Detail	Tag Name
	EMDRP_RMP.IN_RAMP.MOVING_DN	EM droop ramping down
	EMDRP_RMP.IN_RAMP.MOVING_UP	EM droop ramping up
	EMDRP_RMP.IN_RAMP.RAMP	EM droop ramp
	EMDRP_RMP.IN_RAMP.REV_RAMP	EM droop reverse ramp

Figure 7-2. New Datalog Configuration Tool

The files may also be modified with a text editor if the syntax is understood.

AppManager may be used to transfer the “.logConfig” file to the Applications folder of the control (using the same command as for transferring application files to the control). If the “.logConfig” file is updated while the DATA_LOG_M block is already collecting, DATA_LOG_M collection must be stopped and restarted to enlist the new values.

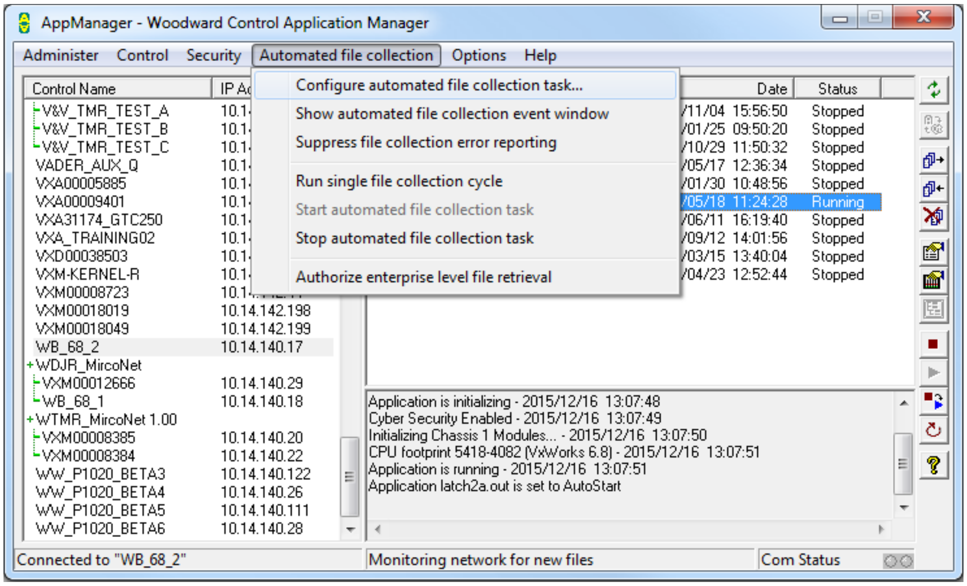
Using AppManager to Collect Datalog files

If the GAP application is continuously producing Datalog files or if there is a risk that event-driven, Datalog files will overwrite existing files. If desired the Datalog files may be automatically archived. AppManager can automatically retrieve the files to a PC where they are stored and may be analyzed.

When AppManager retrieves Datalog files, it automatically renames the files to include a date-time string. This permits multiple instances of files with the same original name to be stored side by side. By default, AppManager stores the files in a subfolder of the Windows ProgramData folder, e.g.:
“C:\ProgramData\Woodward\AppManager\Datalogs\<control name>\”
This location may be overridden in the Automatic File Retrieval Configuration dialog of AppManager.

Automatic File Retrieval Configuration

Open the Scheduled File Retrieval configuration dialog with the menu item shown:


AppManager - Woodward Control Application Manager
Administer
Control
Security
Automated file collection
Options
Help
Configure automated file collection task...
Show automated file collection event window
Suppress file collection error reporting
Run single file collection cycle
Start automated file collection task
Stop automated file collection task
Authorize enterprise level file retrieval

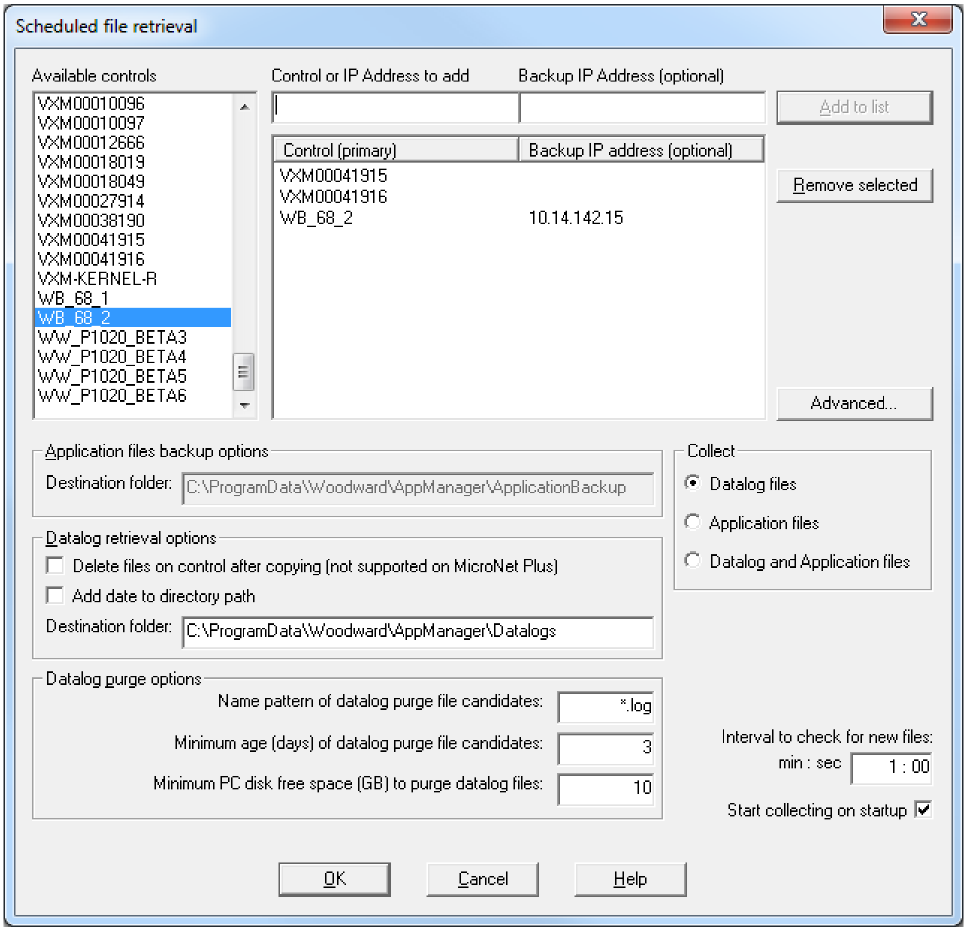
Control Name	IP Ac	Date	Status
V&V_TMR_TEST_A	10.1	/11/04 15:56:50	Stopped
V&V_TMR_TEST_B	10.1	/01/25 09:50:20	Stopped
V&V_TMR_TEST_C	10.1	/10/29 11:50:32	Stopped
VADER_AUX_Q	10.1	/05/17 12:36:34	Stopped
VXA00005885	10.1	/01/30 10:48:56	Stopped
VXA00009401	10.1	/05/18 11:24:28	Running
VXA31174_GTC250	10.1	/06/11 16:19:40	Stopped
VXA_TRAINING02	10.1	/09/12 14:01:56	Stopped
VXD00038503	10.1	/03/15 13:40:04	Stopped
VXM-KERNEL-R	10.1	/04/23 12:52:44	Stopped
VXM00008723	10.1		
VXM00018019	10.14.142.198		
VXM00018049	10.14.142.199		
WB_68_2	10.14.140.17		
+WDJR_MircoNet			
VXM00012666	10.14.140.29		
WB_68_1	10.14.140.18		
+WTMR_MircoNet 1.00			
VXM00008385	10.14.140.20		
VXM00008384	10.14.140.22		
WW_P1020_BETA3	10.14.140.122		
WW_P1020_BETA4	10.14.140.26		
WW_P1020_BETA5	10.14.140.111		
WW_P1020_BETA6	10.14.140.28		

```
Application is initializing - 2015/12/16  13:07:48
Cyber Security Enabled - 2015/12/16  13:07:49
Initializing Chassis 1 Modules... - 2015/12/16  13:07:50
CPU footprint 5418-4082 (VxWorks 6.8) - 2015/12/16  13:07:51
Application is running - 2015/12/16  13:07:51
Application latch2a.out is set to AutoStart
```

Connected to "WB_68_2" | Monitoring network for new files | Com Status

Figure 7-3. Automated File Collection Menu Configure Automatic File

This will open a window like the following:



Scheduled file retrieval

Available controls

VXM00010096
VXM00010097
VXM00012666
VXM00018019
VXM00018049
VXM00027914
VXM00038190
VXM00041915
VXM00041916
VXM-KERNEL-R
WB_68_1
WB_68_2
WW_P1020_BETA3
WW_P1020_BETA4
WW_P1020_BETA5
WW_P1020_BETA6

Control or IP Address to add:

Backup IP Address (optional):

Control (primary)	Backup IP address (optional)
VXM00041915	
VXM00041916	
WB_68_2	10.14.142.15

Application files backup options

Destination folder: C:\ProgramData\Woodward\AppManager\ApplicationBackup

Datalog retrieval options

□ Delete files on control after copying (not supported on MicroNet Plus)

□ Add date to directory path

Destination folder: C:\ProgramData\Woodward\AppManager\Datalogs

Datalog purge options

Name pattern of datalog purge file candidates: *.log

Minimum age (days) of datalog purge file candidates: 3

Minimum PC disk free space (GB) to purge datalog files: 10

Collect

● Datalog files

○ Application files

○ Datalog and Application files

Interval to check for new files:
min : sec 1 : 00

Start collecting on startup ☑

Figure 7-4. Scheduled File Retrieval Dialog Window

Controls to be collected from are specified in the “Control (primary)” list. If the control has a redundant network, it may be used in case of a failure of the primary network (enter the backup IP Address in the second column).

To add to these lists, type values into the “Control or IP Address to add” and “Backup IP Address (optional)” edit windows and then press the “Add to list” button. The “Available controls” list at the left may be used to populate the “Control or IP Address to add” edit window.

It is also possible to configure AppManager to automatically collect application files by selecting “Application files” or “Datalog and Application files” in the “Collect” group-box.

The base destination folders for Datalog and/or Application Files may be specified in the “Destination folder” edit windows.

The schedule for collecting files may be specified in the lower right corner of the dialog. The collection interval should be fast enough to collect files before they are overwritten, but not so fast that collection tasks collide with each other.

Datalog Purge Options

Because continuous Datalog file collection may eventually exhaust PC storage capacity, AppManager provides a strategy for purging Datalog files from the PC. In the box at the lower left of the Scheduled file retrieval dialog, a pattern for purging old files may be specified. While free space on the PC is below the specified minimum PC disk free space value, AppManager will periodically delete Datalog files that match the specified file name pattern and exceed the minimum age specified.

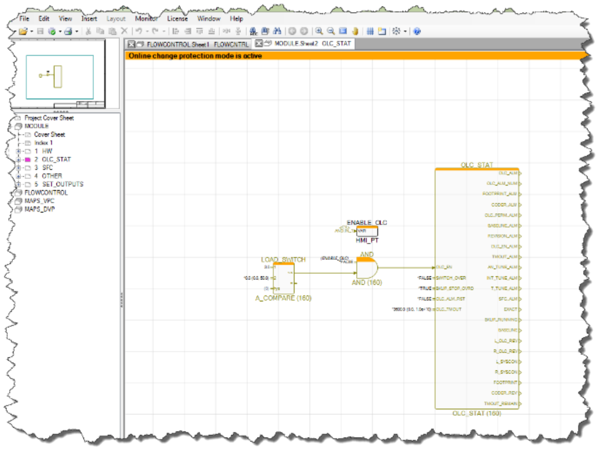
More Information

More information about automatic Datalog file collection is available in the AppManager Help document. Information about configuring an application to produce Datalog files is available in the GAP Block Help.

Chapter 8.
On-line Changes (MicroNet Plus only)

Overview

On-**l**ine programming **C**hanges (**OLC**) are supported in the MicroNet Plus system when using dual CPU's. GAP application updates for online changes are made using a special editor mode that enforces rules during application programming. This is important as it prevents a user from making certain modifications which would create an incompatible application, rather than finding a change is incompatible after loading it on the CPU. Helpful tool tips guide the user to other ways a modification may be possible.



Online change protection mode is active

Once the required application updates are programmed and validated (using NetSim, or other simulation tools), the program is loaded onto the backup (non-controlling) CPU. This gives the user the ability to monitor the new application functionality while it is not yet in control. When ready, the user enables the control switchover to the new application. If necessary, control may be switched back immediately to the previous application now running on the backup CPU.

Control switchover ensures the application stays in control of the unit making for a continuous transfer of control.

System Requirements

Table 8-1. System Requirements

Platform:	MicroNet Plus System with dual CPU's
CPU:	M5200, 5466-1145, 5466-1141, 5466-1245 P1020, 5466-1510, 5466-1520
CPU Footprint:	M5200, 5418-6771 revision C or newer; P1020, 5418-7033 revision D or newer
GAP Editor/Monitor:	GAP 4.00 or newer
Coder:	MicroNet 1.01 or newer

Detailed Information

Detailed information about making On-line programming Changes is available as part of the GAP/Coder environment in helpful user guides and tool tips. Contact Woodward for On-Line programming Change training.

Chapter 9.
Ethernet Networking

Overview

Network settings are likely to require adjustment, so it is important to understand some networking principals. Consult with your Network System Administrator and read this chapter. In addition, networking information can be found on your local Windows PC in, Start\Help – Contents\Networking.

Table 9-1. Internet Vocabulary

IP	Internet Protocol—Designed to link networks together.
IP Address	32-bit number made up of four 3-bit segments (“octets”) separated by periods (The protocol for this type of addressing is named “IPv4”).
TCP	Transmission Control Protocol—Designed to link networks together.
UDP	User Datagram Protocol—Connectionless/ Host-to-Host protocol in the Transport Layer of IP.
DHCP	Dynamic Host Configuration Protocol—Automates IP address assignment.
Gateway	A device or computer that forwards data to a destination on another domain.
Subnet Mask	The binary 1’s mark which bits of the IP address are used for the network. The 0’s mark which bits are for your station’s ID#.
Octet	The 32-bit IP address is grouped 8 bits at a time, each group of 8 bits is an **octet**. Each of the four **octets** are separated by a dot and represented in decimal format, this is known as dotted decimal notation. Each bit in an **octet** has a binary weight (128, 64, 32, 16, 8, 4, 2, and 1).
Port	A logical number that increases the number of devices that can talk without increasing IP addresses.
MAC	Media Access Control—A unique 48-bit number burned into the hardware of the device. Uniquely identifies the device.
Address Mapping	When a host broadcasts to all MACs and associates each responding MAC address with its IP Address.

Internet Protocol

The Internet Protocol (“IP”) is a network layer Internet protocol. IP facilitates communication from the two Transport Layer Protocols, TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). They run on top of the IP layer and are identified by Port Numbers.

IP Addresses

Woodward uses IPv4 IP addresses. The IPv4 address is a 32-bit number made up of four 3-bit segments separated by periods. The Subnet Mask controls which bits are the network identifier and which bits are the station identifier. (The binary 1’s mark, which bits of the IP address represent the network identifier. The binary 0’s indicate which bits of the IP address is your device ID#—for example, a Subnet Mask of 255.255.0.0 = 11111111.11111111.00000000.00000000.) The first 16 bits of the IP address identify the network, and the last 16 bits identify the device.

There are three classes (sizes) of IP networks: A, B, and C. Classes are determined by how many unique devices and sub networks are possible based on how many of the IP address bits are used for designating the network number and how many bits identify the device number. A network identifier between 192—223 is class C size, because the first three bits of the IP addresses are used to identify the network.

IMPORTANT **Some IP address ranges are reserved. Consult your Network Administrator if you want a "fixed/static" IP address for a control.**

The Gateway is a device or computer that forwards data to a destination on another domain. The Port number is a logical number that increases the number of devices that can talk without increasing IP addresses. Port Numbers 1-1024 are reserved for protocols such as HTTP, POP, FTP, etc. Port numbers 1025 to 65000 are available for the typical PC, MicroNet Plus, MicroNet, 505, Flex500 and Atlas-II sessions.

File Transfer Protocol

For non-Cyber Secure CPUs:
The VxWorks operating system has an active FTP Server running on the control. Applications such as AppManager use FTP to transfer files between the control and the local computer.

The recommended mechanism for transferring files between the control and the local computer is with AppManager.

The FTP Server follows the FTP standard, so other standard FTP client programs can be used to transfer files if required.

For Cyber Secure CPUs and CPU_MP1020:
The VxWorks operating system has an active SFTP Server running on the control. Applications such as AppManager use SFTP to transfer files between the control and the local computer.

The recommended mechanism for transferring files between the control and the local computer is with AppManager.

The SFTP Server follows the SFTP standard, so other standard SFTP client programs can be used to transfer files if required.

Pinging the Network

Ping is a DOS command done in the Command Prompt window. It is useful for the following:

- To see if a device with a specific IP address exists on a network. For instance, before connecting a Woodward Ethernet port on your network, do this test to your network to see if the IP address that was fixed (static) in a Woodward control is being used by another device.
- To find a Woodward control with an unknown Computer Name or unknown IP address and confirm you are talking to it by seeing its TX LED blink.
- To see if a TCP/IP Ethernet Port is available to the network.

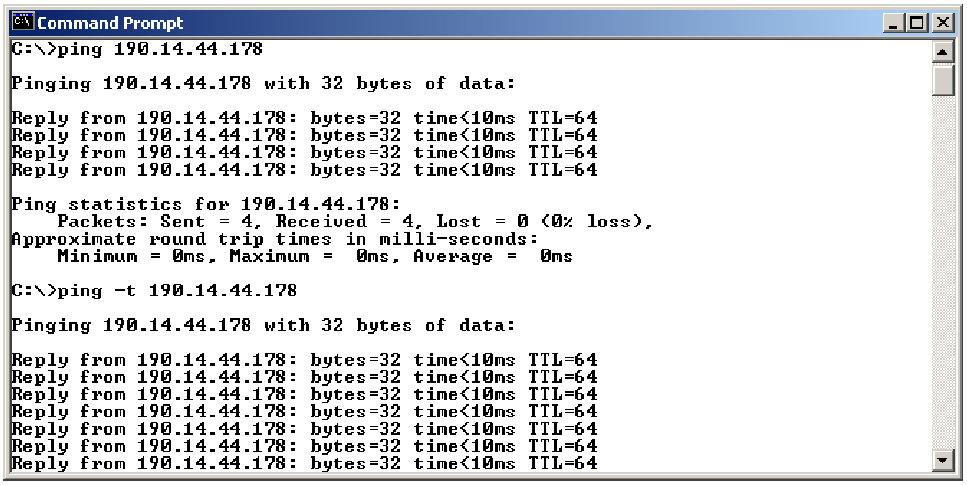
If the control appears to be unresponsive to Ethernet requests, "ping" the control to determine if the control is available. The DOS "ping" command will send a network packet to the control and monitor the Ethernet for a response. If a successful response occurs, it will annunciate the control IP address and the travel time of the communications packet. This indicates that the hardware is working.

Pinging instructions

You can "ping" a control by IP address as follows:

1. Connect the PC to the Control using a shielded Ethernet cable. Verify that you have a green "Link" light, which indicates a good connection.
2. On your PC
   a. select [Start]\Programs and find the Command Prompt shortcut
   b. or type "cmd" into the *Run…* window.
3. Then type in a ping command in the launched window.
4. Example: c:> ping 190.14.98.173. See Figure 9-1.
5. Type in "ping" [Enter] to see ping options. See Figure 9-1.

6. To close the command Prompt Window, type in “exit” [Enter].



```
C:\>ping 190.14.44.178

Pinging 190.14.44.178 with 32 bytes of data:

Reply from 190.14.44.178: bytes=32 time<10ms TTL=64
Reply from 190.14.44.178: bytes=32 time<10ms TTL=64
Reply from 190.14.44.178: bytes=32 time<10ms TTL=64
Reply from 190.14.44.178: bytes=32 time<10ms TTL=64

Ping statistics for 190.14.44.178:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping -t 190.14.44.178

Pinging 190.14.44.178 with 32 bytes of data:

Reply from 190.14.44.178: bytes=32 time<10ms TTL=64
Reply from 190.14.44.178: bytes=32 time<10ms TTL=64
Reply from 190.14.44.178: bytes=32 time<10ms TTL=64
Reply from 190.14.44.178: bytes=32 time<10ms TTL=64
Reply from 190.14.44.178: bytes=32 time<10ms TTL=64
Reply from 190.14.44.178: bytes=32 time<10ms TTL=64
Reply from 190.14.44.178: bytes=32 time<10ms TTL=64
```

Figure 9-1. DOS Ping of IP Address (example)

IMPORTANT **When pinging the control’s Ethernet port, you should see the green LED blink in response to each ping.**

IMPORTANT **TIP—Pinging with a “-t” suffix will continually ping until you press [CTRL]+[C].**

Logging on to a network in DHCP mode

When a device running TCP/IP (e.g. MicroNet Plus, Atlas-II, and/or PC) logs onto a network, it sends out a DHCP Discover message. The DHCP server receives the message and sends out an IP address with the subnet mask and a lease time to the hardware or MAC address of the device. (A typical lease is 30 days.) The device broadcasts a message of acceptance, implements the new identity, and is ready for TCP/IP sessions. The host has Address Mapped the device and associates its MAC address with its IP address.

IMPORTANT **The MicroNet Plus Cyber Secure, 505 and Flex500 CPUs do not support DHCP mode. Only fixed IP addresses are supported.**

Networking with Woodward Controls

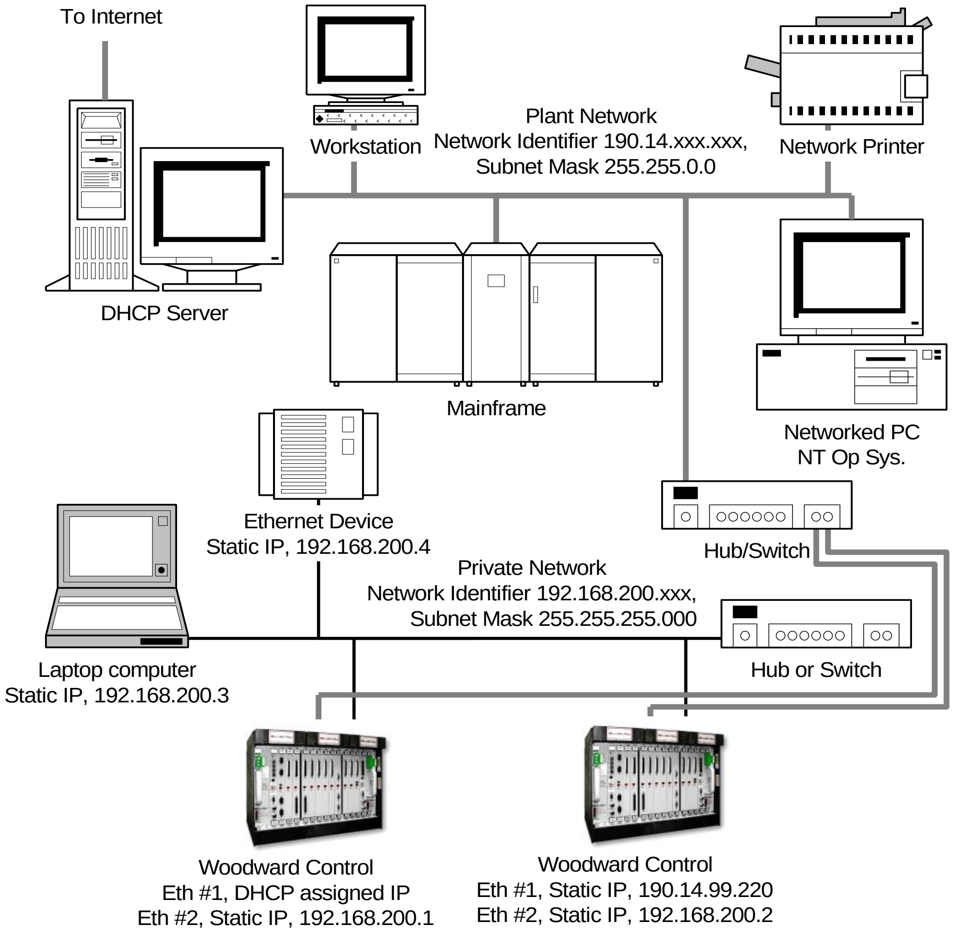


Figure 9-2. Setup Example for Controls with Dual Ethernet

The MicroNet Plus CPU5200 supports two shielded 10/100 Base-TX RJ45 female connectors for TCP/IP sessions; the 505, Flex500 and Atlas-II support four; the MicroNet Plus CPU_MP1020 supports two shielded 10/100/1000 and two shielded 10/100 Base-TX RJ45 female connectors for TCP/IP sessions. These connections are used for network file sharing, application management, and remote control, as well as other control functions like Ethernet Modbus. A client computer using a Windows Operating System is required for networking with the Woodward control.

- A unique Ethernet IP address is required for every device on a particular network in order to avoid IP address conflicts.
- The control's Computer Name is associated with its IP address when using a network DHCP server or AppManager.
- On CPUs with four Ethernet ports, AppManager will only work on Ethernet ports #1 or #2. On CPUs with six Ethernet ports, AppManager works on Ethernet ports #1 through #4.

IMPORTANT

Multiple user Ethernet Ports should not be set to the same Network Identifier because its Operating System may respond out of only one port. You will need to set all ports to a different network to ensure that it will respond. Recommend that initially, one port be set to the same Network as your local PC network so that you can use the software tools described in this manual. See Figure 9-2 for an example of two separate networks.

GAP and Ethernet

Woodward GAP applications typically use UDP blocks to talk Modbus through Ethernet ports. UDP is mainly used for time-sensitive, low-priority data and has no reliability associated with this layer. Transmission is in small, static-size packets. The sender assumes all packets are received and normally does not re-transmit. However, in MicroNet, MicroNet Plus, 505, Flex500 and Atlas-II, the “Modbus“ blocks (C code) tells the master to send data to the slave, and the slave will normally accept the data and respond to the master, so the communications loop will not produce any errors. Should the slave not accept the data (if it receives invalid or no data), the slave will not respond. The master will wait for its time-out period to expire and re-send to the slave. If the master again does not get a response from the slave, the master will generate a Link Error. In addition, the slave is looking for the master to talk to it at static time intervals. If it does not get a transmission, it will generate a Link Error. The UDP header consists of [Source Port, Destination Port, Header Length, and Checksum].

Dual Ethernet GAP Setup

The second Ethernet port is activated when the application uses its IP address. To use the second Ethernet port in Modbus, a UDP_P or TCP_P block must be connected to the Modbus block, and the UDP_P or TCP_P block must be connected to the parent CPU block.

See Figure 9-3.

1. In the CPU parent block, add the second ETHER_2 input by opening the CPU block and clicking on RPT2.
2. At the CPU.ETHER_x inputs, enter the name of the two UDP_P or TCP_P blocks.
3. The UDP_P or TCP_P output from the UDP_P or TCP_P block goes to a MODBUS_M or MODBUS_S PORT_X input.

IMPORTANT **When you have multiple UDP_P blocks, each S_PORT input must be a unique number. See the UDP_P block help.**

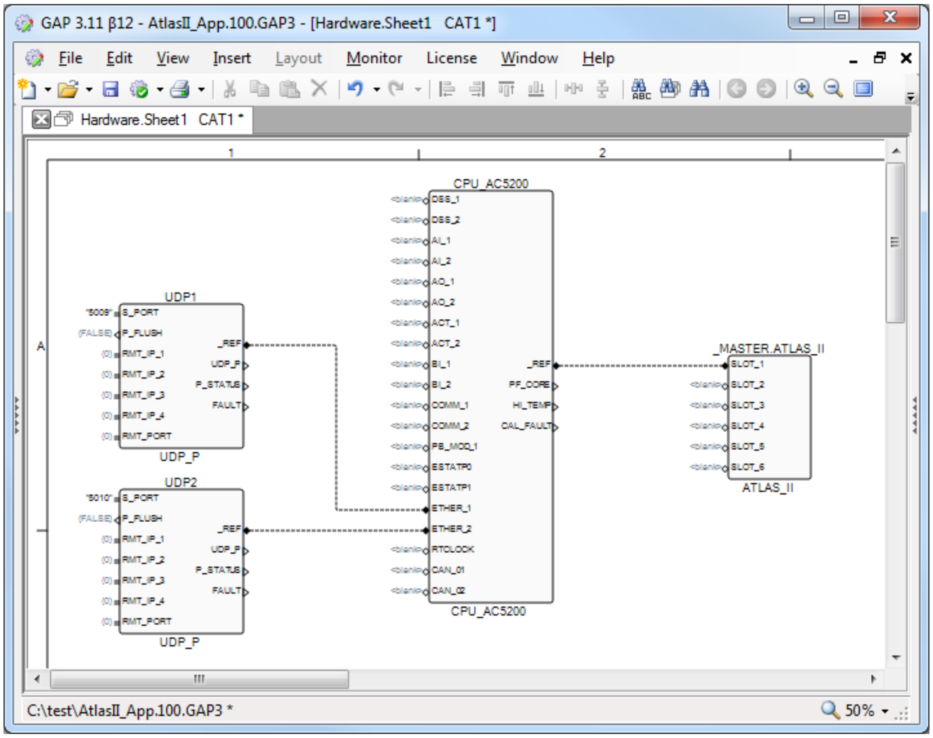


Figure 9-3. Dual Ethernet GAP example for Atlas-II

Ethernet Distributed I/O

For Ethernet Distributed IO, “BootP” is a Woodward tool that is available from the Woodward website (**www.woodward.com/software**). It is an IP/UDP bootstrap protocol, which allows a client machine to discover its own IP address. The protocol operates as a server, continuously listening for a request. When the server gets a request, it looks for an entry in the BootP database that matches the MAC address of the request. If the server finds a match, it sends a response message with the IP address from the entry that matched.

Distributed I/O is covered in considerable detail in volume 2 of the AtlasPC Digital Control Hardware manual (85586V2).

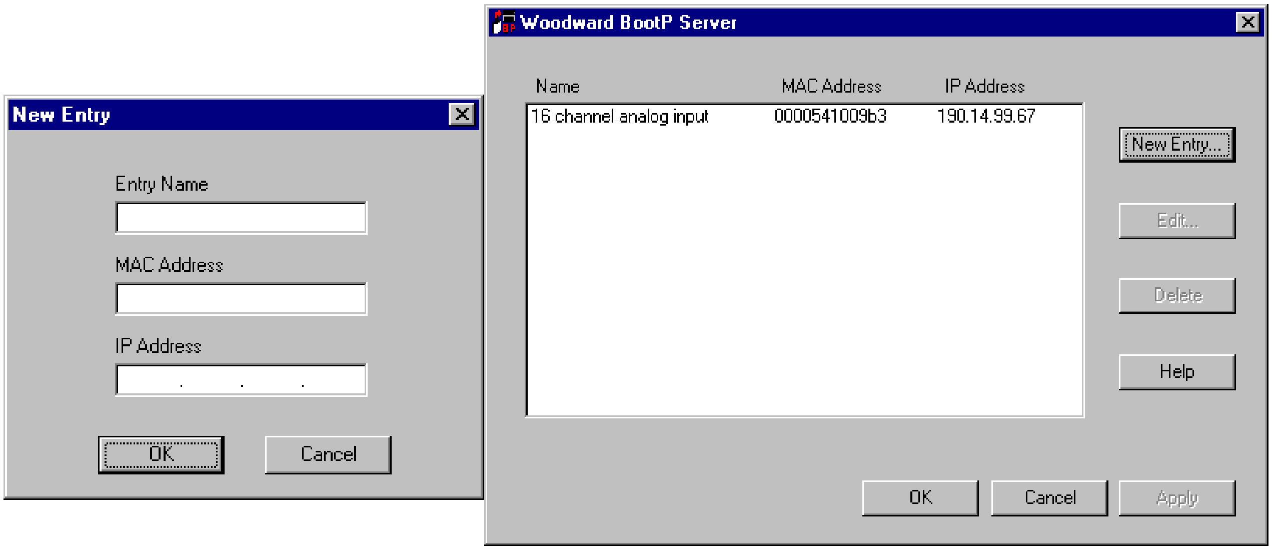
As an example of how to set up a distributed I/O node, a Modicon, analog 16-channel single ended module will be used (170 AAI 140 00).

This module can be configured for ±10 V, ±5 V, or 4–20 mA inputs.

Figure 9-4. 16-Channel Single Ended Module

Giving the module an IP address
Each distributed I/O device has an IP address associated with it. For some devices, a terminal emulator sets this address over an RS-232 line and for other devices; a server called BOOTP sets it automatically. Modicon uses the BootP program.

On each Modicon node there is a MAC address (usually some kind of sticker) which is a unique address given to this node. This address, along with a valid IP Address, can be obtained from the system administrator, as well as an “Entry Name” field or description. Enter as shown, and the module will adopt this new IP Address.



Name	MAC Address	IP Address
16 channel analog input	0000541009b3	190.14.99.67

Figure 9-5. BootP Screenshot

Ethernet Distributed IO and GAP

- In GAP, use FBUS_M to scan Ethernet IO over the network. It will work with any distributed IO that uses the Modbus over TCP/IP standard. It is designed to establish a TCP connection with one device. The block is found in the GAP block tree in the Hardware folder “TCP/IP Fieldbus Blocks”.
- The blocks FBUS_INITA and FBUS_INITB are used to initialize a distributed IO module.
- The FBUS_AI, FBUS_AO, FBUS_BI, FBUS_BO, FBUS_AIO blocks support the Modbus functions.
- Use GAP help for information about writing the GAP interface. Contact Woodward for additional help with Ethernet distributed I/O.
- The Modicon manual will give you information on how to configure inputs for a voltage or current input. It will also give you information about how to scale the raw counts coming from the module into the Woodward control.
- Gap Help about the above-mentioned blocks will instruct the user how to configure the gap blocks to accept the incoming raw counts into a voltage or current signal.

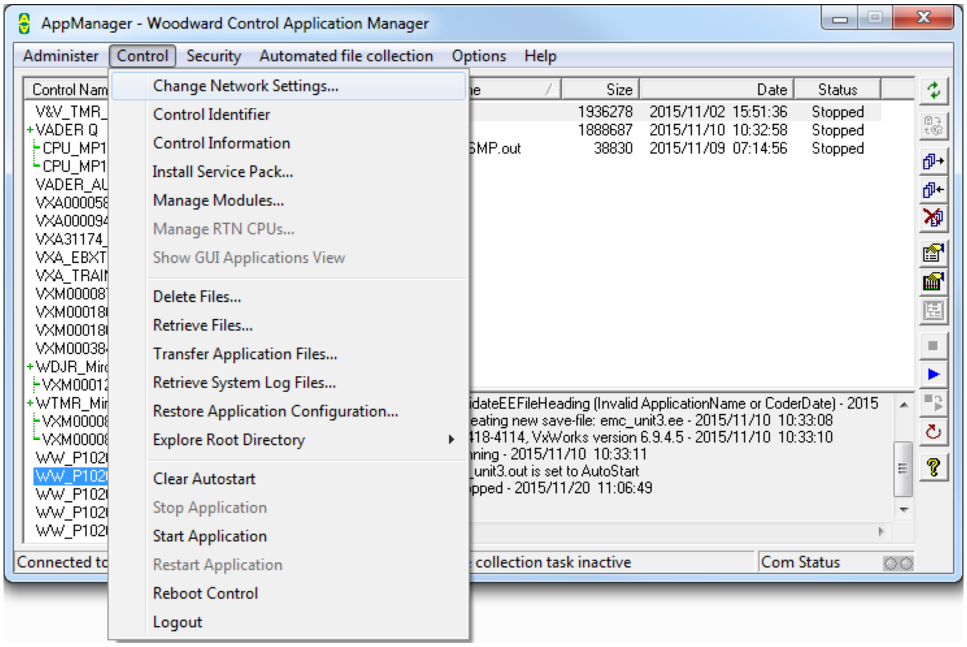
Note: Find more information in Woodward manual 85586V2, *AtlasPC Digital Control Hardware Manual, vol. II (Distributed I/O)*.

Simple Network Time Protocol (SNTP)

The MicroNet Plus, 505, Flex500 or Atlas-II can be configured as an SNTP Client. Using AppManager, the SNTP Server address, and update time can be configured.

The control network settings may be changed in AppManager as follows:

1. On your PC, open AppManager.exe.
2. You should see the control’s Computer Name in the AppManager window. Select the Computer Name of the control. If the control name does not appear on the list, check your connections and verify that the Link lights are on.
3. To change network settings, no application may be running on the control. Verify that the application (if any) is stopped.
4. Click “Control” in the top header of the AppManager window, use the pull down menu, and select “Change Network Settings”.

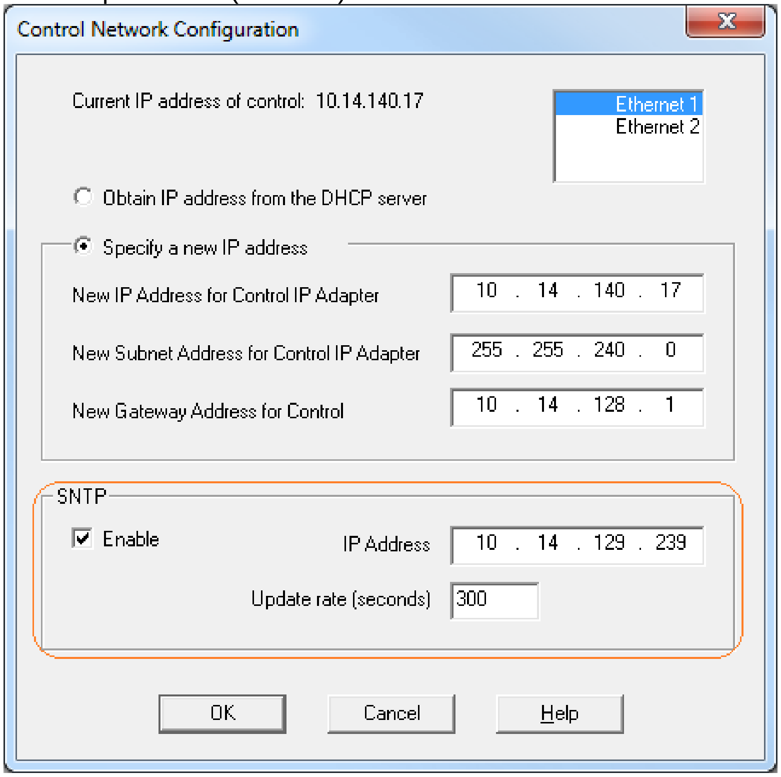


```
e               Size   Date                  Status
             1936278   2015/11/02  15:51:36  Stopped
             1888687   2015/11/10  10:32:58  Stopped
SMP.out        38830   2015/11/09  07:14:56  Stopped
```

```
idateEEFileHeading (Invalid ApplicationName or CoderDate) - 2015
eating new save-file: emc_unit3.ee - 2015/11/10  10:33:08
418-4114, VxWorks version 6.9.4.5 - 2015/11/10  10:33:10
nning - 2015/11/10  10:33:11
_unit3.out is set to AutoStart
pped - 2015/11/20  11:06:49
```

Figure 9-6. Control Menu – Change Network Settings

5. In the SNTP group-box, check the Enable box, enter the IP address for the SNTP Server on the network, and enter the update rate (seconds).



Control Network Configuration

Current IP address of control: 10.14.140.17

Ethernet 1
Ethernet 2

○ Obtain IP address from the DHCP server

● Specify a new IP address

New IP Address for Control IP Adapter: 10 . 14 . 140 . 17

New Subnet Address for Control IP Adapter: 255 . 255 . 240 . 0

New Gateway Address for Control: 10 . 14 . 128 . 1

SNTP

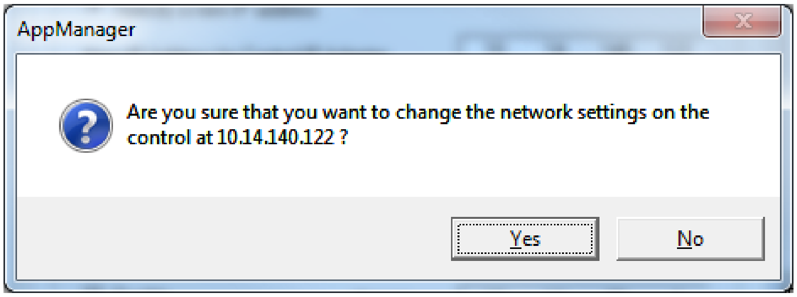
☑ Enable

IP Address: 10 . 14 . 129 . 239

Update rate (seconds): 300

Figure 9-7. Control Network Configuration Window

6. Select “Yes” to change the settings.

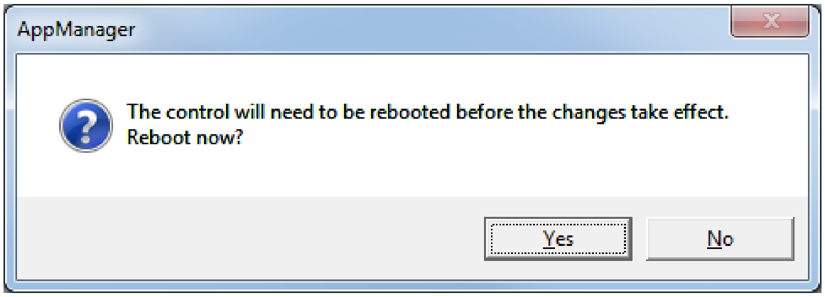


AppManager

Are you sure that you want to change the network settings on the control at 10.14.140.122 ?

Figure 9-8. Network Settings Confirmation Window

7. A message will appear stating that the control settings have been changed and prompt to reboot the control.



AppManager

The control will need to be rebooted before the changes take effect. Reboot now?

Figure 9-9. Control Reboot Prompt

Chapter 10.
Troubleshooting the Control

Overview

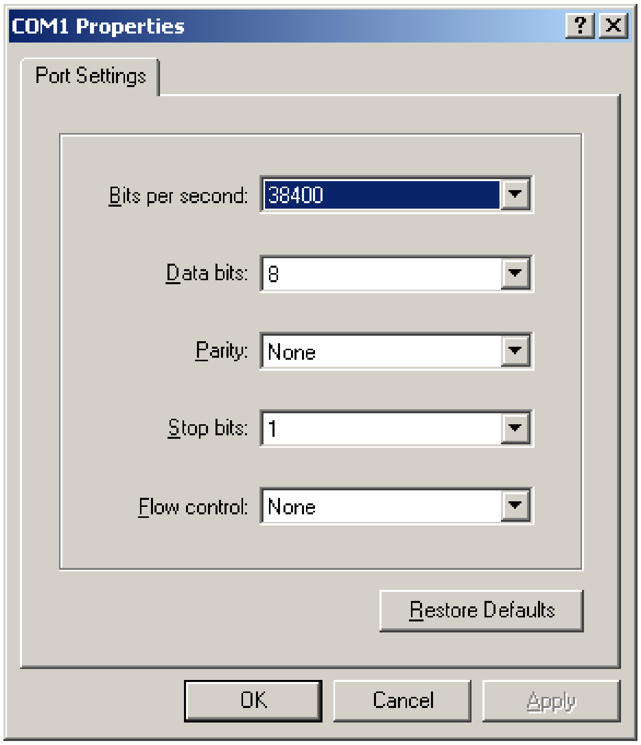
If the control is not functioning properly, it may be possible to investigate and solve what is wrong by applying the tools mentioned in this chapter.

Using the Debug Port (DBUG)

Setup

For debug use, a null-modem cable and 5450-1065 Serial Adapter cable (PS2M to DB9F) is required to attach this port to a PC. This port is to be used by trained Field Service personnel only!

1. Connect a standard null-modem serial cable from your local PC to the Woodward control's debug port using the serial adapter cable.
2. Run a terminal emulation program such as *HyperTerminal* or *TeraTerm* on your PC. Configure a serial port with the parameters shown in Figure 10-1:



Bits per second: 38400

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Figure 10-1. Serial Port Configuration

Using the Service Port

Applicable only on MicroNet CPUs with part numbers 5466-1510 and 5466-1520.

IMPORTANT

The MicroNet CPU Service Port only supports serial communications over USB. Mass Storage (flash drives), keyboards, computer mice and other peripherals are not supported. The USB-Serial converter hardware in the MicroNet CPU is manufactured by FTDI, who has stated that their USB-Serial converter does not contain firmware.

Setup

For troubleshooting use, a USB 2.0 A Male to Micro USB Male cable is required. This port is to be used by trained Field Service personnel only!

1. Connect the Micro USB end of the cable to the MicroNet CPU port labeled “Service” and connect the USB 2.0 A Male connector to the USB port on the PC.
2. Allow Windows to detect the MicroNet connection and wait for driver installation to complete. The driver installation process may take several minutes. Note the Window message that indicates the Com port number that was assigned.
3. Run a terminal emulation program like *HyperTerminal* or *TeraTerm* on your local PC
4. Select “connect using COM#” using the COM port number that Windows assigned.
5. Configure the port settings with the following.
    a. Bits per second: 115,200
    b. Data bits: 8
    c. Parity: None
    d. Stop bits: 1
    e. Flow control: None.

6. All other settings stay at default.

Boot information in debug or service port console

About 15 to 45 seconds after the control is powered on, messages are displayed in the terminal emulation program window that identifies the VxWorks operating system and its version numbers. This message is displayed:

```
    Press any key to stop auto-boot…
        7-6-5-4-3-2-1-0
```

If you press any key, the auto boot is halted and the operating system is in a system boot mode:

“[VxWorks boot]:”

From this prompt you can perform the following commands:

1. “**help**” (this describes all the commands available)
2. “**p**” (this command lists the boot parameters including the IP address and the Control name.)

```
[VxWorks Boot]: p
    boot device          : tffs=0,0
    unit number          : 0
    processor number     : 0
    host name            : mars
    file name            : /OS/System/VxWorks
    inet on Ethernet (e) : 10.14.140.114:ffff0000    (current static IP address)
    host inet (h)        : 10.14.36.132
    user (u)             : mpc5200
    ftp password (pw)    : mpc5200
    flags (f)            : 0x80
    target name (tn)     : VXM12345                  (current Control name)
    other (o)            : bcm0
```

For MicroNet CPU part numbers 5466-1510 and 5466-1520 the following is displayed:

```
[VxWorks Boot]: p

boot device         : fs0
unit number         : 1
processor number    : 2
host name           : host
file name           : /tffs0:1/System/vxWorks
inet on Ethernet (e) : 10.14.138.97:fffff000(current static IP address)
host inet (h)       : 10.14.128.226
gateway inet (g)    : 10.14.128.1
user (u)            : vxworks
ftp password (pw)   : vxworks
flags (f)           : 0x80
target name (tn)    : CPU_MP1020_BD337
other (o)           : motetsec1
```

3. "**c**" (this command allows you to change the values of the IP address or the control name).
   - When you type the "**c**" command, the first line will be displayed with the current data value. To change the value, type in the new value and hit enter. To move on to the next line without changing the current line, just hit enter.
   - To save the new settings, continue hitting enter until you get past the last line. At this time, the control will save the values and give you back the debug prompt.
   - To start running the operating system, either type in "@" followed by enter or reboot the control.
4. When you allow the CPU to boot without pausing in the service or debug mode, there will be many more messages. At the end of all the messages, you will be able to login and get a "->" prompt. You can see the available commands from this menu by typing "**help**" and then pressing Enter.

Network debugging

In the following commands, bcm0 represents user network1, bcm1 represents user network2, bcm2 represents RTN Port 1 for MicroNet Plus and user network3 for 505, Flex500 and Atlas-II, and bcm3 represents RTN Port 2 for MicroNet Plus and user network4 for 505, Flex500 and Atlas-II.

WGNetworkShow—Displays the IP Address settings for the two user Ethernet ports and the two RTN ports in MicroNet Plus or four user ports for the 505, Flex500 or Atlas-II.

```
-> WGNetworkShow
Current Ethernet Configuration
bcm0 -
    IPAddress - 10.14.140.114
    Subnet Mask - 255.255.0.0
bcm1 -
    IPAddress - 192.168.128.20
    Subnet Mask - 255.255.255.0
bcm2 -
    IPAddress - 172.20.22.11
    Subnet Mask - 255.255.255.0
bcm3 -
    IPAddress - 172.20.23.11
    Subnet Mask - 255.255.255.0
```

Ethernet Address - 00128c0001f5
Default Gateway -
For MicroNet CPU part numbers 5466-1510 and 5466-1520, in the following commands, Ethernet0,1,2,3,4, 5 correspond to GbE1, GbE2, ENET1, ENET2, RTN1 and RTN2.

IMPORTANT **MicroNet CPU part numbers 5466-1510 and 5466-1520 do not support the “WGNetworkConfig” command. Changes should be made through AppManager.**

WGNetworkShow—Displays the IP Address settings for the four user Ethernet ports and the two RTN ports.

```
-> WGNetworkShow
Current Ethernet Configuration
Ethernet0 -
        IPAddress - 10.14.138.97
        Subnet Mask - 255.255.240.0
        Default Gateway - 10.14.128.1
        Ethernet Address - 004444000224
Ethernet1 -
        IPAddress - 192.168.128.20
        Subnet Mask - 255.255.255.0
        Default Gateway - Not Set
        Ethernet Address - 004444000225
Ethernet2 -
        IPAddress - 192.168.129.20
        Subnet Mask - 255.255.255.0
        Default Gateway - Not Set
        Ethernet Address - 004444000226
Ethernet3 -
        IPAddress - 192.168.130.20
        Subnet Mask - 255.255.255.0
        Default Gateway - Not Set
        Ethernet Address - 004444000227
Ethernet4 -
        IPAddress - 172.20.22.10
        Subnet Mask - 255.255.255.0
        Default Gateway - Not Set
        Ethernet Address - 004444000228
Ethernet5 -
        IPAddress - 172.20.23.10
        Subnet Mask - 255.255.255.0
        Default Gateway - Not Set
        Ethernet Address - 004444000229
Ethernet Address - 00128c0001f5
Default Gateway -
```

Ping—Tests to see if an external IP Address is accessible from the control. The command “ping” is followed by the external IP Address “190.14.99.110”, and then followed by the number of attempts.

```
        -> ping "10.14.140.110",3
        PING 10.14.140.110: 56 data bytes
        64 bytes from 10.14.140.110: icmp_seq=0. time=5. ms
        64 bytes from 10.14.140.110: icmp_seq=1. time=5. ms
        64 bytes from 10.14.140.110: icmp_seq=2. time=0. ms
        ----10.14.140.110 PING Statistics----
        3 packets transmitted, 3 packets received, 0% packet loss
        round-trip (ms) min/avg/max = 0/3/5
```

Hard Drive Recovery

IMPORTANT **The hard drive recovery steps should only be executed as a last resort. All Application files and Ethernet port settings (except GbE1 or ENET1 and RTN1/2) will be erased.**

The CPU M5200 flash file system is divided into two drives – OS and HD1Flash. The OS drive holds all of the operating system files needed for the control to start. The HD1Flash drive contains all the application related files, VxWorks log, registry files, DATALOG and DATALOG_M application output log files.

The CPU_MP1020 CPU flash file system is divided into four drives, OS, HD1FX, Data, and Backup. The OS drive holds all of the operating system files needed for the control to start. The HD1FX drive contains all the application related files, VxWorks log and registry files. The Data drive contains the application's DATALOG and DATALOG_M output log files. The Backup drive is available as a place to contain PC tools, manuals, applications backup files, and other general items as desired.

The application related files include - NV logs, EE files, etc. **Recommend always keep a backup of the applications files being used on the control.** These backup files are needed to recover from a hard drive corruption.

Recovery for M5200 CPUs

In the unlikely event that a hard drive corruption occurs, the debug port will display a message that says –
"Formatted Flash Drive HD1Flash not found".
The OS drive contains a copy of the needed HD1Flash files. Recovery commands are provided to allow the user to format the HD1Flash drive.

Disk Recovery Procedure
1) Enter the command - WGEraseHD1Flash48, this command will take a couple of minutes to complete as it erases all of the flash sectors.

2) Enter the command - sysTffsHD1Format, this command will take a couple of minutes as it formats the drive.

3) Restart the control by entering – WGReboot.

4a) (**Cyber CPU only**) Enter the command – dosFsVolFormat("/HD1Flash",2,0).

4b) Enter the command – WGRestoreHD1Flash, this command will copy the registry and log files needed by VxWorks.

5) Restart the control by entering – WGReboot.

After completing these steps, the network will need to be reconfigured (see First Time Setup Instructions) and the application files need to be restored (see Downloading and Running the Application). **For Cyber Secure CPUs**, the Accounts will need to be reconfigured.

Recovery for MP1020 CPUs

In the unlikely event that a hard drive corruption occurs, the service port console will display a message that reports "Formatted Flash Drive XXX not found" where XXX may refer to "OS", "HD1FX", "Backup" or "Data" drives.

The OS drive contains a copy of the original factory loaded files. Recovery commands are provided to allow the user to recover from all but an OS drive failure.

These procedures will result in the loss of the customer's application, data logs and other files so ensure backup files are available.

Disk Recovery Procedure
1) Enter the command – WGRestoreFlash "HD1FX" or "Backup" or "Data" as appropriate, this command will take a couple of minutes to complete as it erases all of the flash sectors and restores the file system.

After completing these steps, the network will need to be reconfigured (see First Time Setup Instructions) and the application files need to be restored (see Downloading and Running the Application). The User Accounts will also need to be reconfigured.

Chapter 11.
Product Support and Service Options

NOTICE

CPUs sent into Woodward for repair will be reconfigured to the default settings. This includes Accounts, Passwords, and Network configurations. Secured Application CPUs Authorization Encryption Files ("AEF" files) and related information will be erased and replaced with newly generated information.

Product Support Options

If you are experiencing problems with the installation, or unsatisfactory performance of a Woodward product, the following options are available:

- Consult the troubleshooting guide in the manual.
- Contact the manufacturer or packager of your system.
- Contact the Woodward Full Service Distributor serving your area.
- Contact Woodward technical assistance (see "How to Contact Woodward" later in this chapter) and discuss your problem. In many cases, your problem can be resolved over the phone. If not, you can select which course of action to pursue based on the available services listed in this chapter.

OEM or Packager Support: Many Woodward controls and control devices are installed into the equipment system and programmed by an Original Equipment Manufacturer (OEM) or Equipment Packager at their factory. In some cases, the programming is password-protected by the OEM or packager, and they are the best source for product service and support. Warranty service for Woodward products shipped with an equipment system should also be handled through the OEM or Packager. Please review your equipment system documentation for details.

Woodward Business Partner Support: Woodward works with and supports a global network of independent business partners whose mission is to serve the users of Woodward controls, as described here:

- A **Full Service Distributor** has the primary responsibility for sales, service, system integration solutions, technical desk support, and aftermarket marketing of standard Woodward products within a specific geographic area and market segment.
- An **Authorized Independent Service Facility (AISF)** provides authorized service that includes repairs, repair parts, and warranty service on Woodward's behalf. Service (not new unit sales) is an AISF's primary mission.
- A **Recognized Turbine Retrofitter (RTR)** is an independent company that does both steam and gas turbine control retrofits and upgrades globally, and can provide the full line of Woodward systems and components for the retrofits and overhauls, long term service contracts, emergency repairs, etc.

A current list of Woodward Business Partners is available at www.woodward.com/directory.

Product Service Options

The following factory options for servicing Woodward products are available through your local Full-Service Distributor or the OEM or Packager of the equipment system, based on the standard Woodward Product and Service Warranty (5-01-1205) that is in effect at the time the product is originally shipped from Woodward or a service is performed:

- Replacement/Exchange (24-hour service)
- Flat Rate Repair
- Flat Rate Remanufacture

Replacement/Exchange: Replacement/Exchange is a premium program designed for the user who is in need of immediate service. It allows you to request and receive a like-new replacement unit in minimum time (usually within 24 hours of the request), providing a suitable unit is available at the time of the request, thereby minimizing costly downtime. This is a flat-rate program and includes the full standard Woodward product warranty (Woodward Product and Service Warranty 5-01-1205).

This option allows you to call your Full-Service Distributor in the event of an unexpected outage, or in advance of a scheduled outage, to request a replacement control unit. If the unit is available at the time of the call, it can usually be shipped out within 24 hours. You replace your field control unit with the like-new replacement and return the field unit to the Full-Service Distributor.

Charges for the Replacement/Exchange service are based on a flat rate plus shipping expenses. You are invoiced the flat rate replacement/exchange charge plus a core charge at the time the replacement unit is shipped. If the core (field unit) is returned within 60 days, a credit for the core charge will be issued.

Flat Rate Repair: Flat Rate Repair is available for the majority of standard products in the field. This program offers you repair service for your products with the advantage of knowing in advance what the cost will be. All repair work carries the standard Woodward service warranty (Woodward Product and Service Warranty 5-01-1205) on replaced parts and labor.

Flat Rate Remanufacture: Flat Rate Remanufacture is very similar to the Flat Rate Repair option with the exception that the unit will be returned to you in “like-new” condition and carry with it the full standard Woodward product warranty (Woodward Product and Service Warranty 5-01-1205). This option is applicable to mechanical products only.

Returning Equipment for Repair

If a control (or any part of an electronic control) is to be returned for repair, please contact your Full-Service Distributor in advance to obtain Return Authorization and shipping instructions.

When shipping the item(s), attach a tag with the following information:

- Return authorization number
- Name and location where the control is installed
- Name and phone number of contact person
- Complete Woodward part number(s) and serial number(s)
- Description of the problem
- Instructions describing the desired type of repair

Packing a Control

Use the following materials when returning a complete control:

- Protective caps on any connectors
- Antistatic protective bags on all electronic modules
- Packing materials that will not damage the surface of the unit
- At least 100 mm (4 inches) of tightly packed, industry-approved packing material
- A packing carton with double walls
- A strong tape around the outside of the carton for increased strength

NOTICE	**To prevent damage to electronic components caused by improper handling, read and observe the precautions in Woodward manual 82715, *Guide for Handling and Protection of Electronic Controls, Printed Circuit Boards, and Modules*.**

Replacement Parts

When ordering replacement parts for controls, include the following information:

- The part number(s) (XXXX-XXXX) that is on the enclosure nameplate
- The unit serial number, which is also on the nameplate

Engineering Services

Woodward offers various Engineering Services for our products. For these services, you can contact us by telephone, by email, or through the Woodward website.

- Technical Support
- Product Training
- Field Service

Technical Support is available from your equipment system supplier, your local Full-Service Distributor, or from many of Woodward's worldwide locations, depending upon the product and application. This service can assist you with technical questions or problem solving during the normal business hours of the Woodward location you contact. Emergency assistance is also available during non-business hours by phoning Woodward and stating the urgency of your problem.

Product Training is available as standard classes at many of our worldwide locations. We also offer customized classes, which can be tailored to your needs and can be held at one of our locations or at your site. This training, conducted by experienced personnel, will assure that you will be able to maintain system reliability and availability.

Field Service engineering on-site support is available, depending on the product and location, from many of our worldwide locations or from one of our Full-Service Distributors. The field engineers are experienced both on Woodward products as well as on much of the non-Woodward equipment with which our products interface.

For information on these services, please contact us via telephone, email us, or use our website: **www.woodward.com**.

Contacting Woodward's Support Organization

For the name of your nearest Woodward Full-Service Distributor or service facility, please consult our worldwide directory at **www.woodward.com/directory**, which also contains the most current product support and contact information.

You can also contact the Woodward Customer Service Department at one of the following Woodward facilities to obtain the address and phone number of the nearest facility at which you can obtain information and service.

Products Used in Electrical Power Systems

Facility	Phone Number
Brazil	+55 (19) 3708 4800
China	+86 (512) 6762 6727
Germany:	
Kempen	+49 (0) 21 52 14 51
Stuttgart	+49 (711) 78954-510
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+82 (51) 636-7080
Poland	+48 12 295 13 00
United States	+1 (970) 482-5811

Products Used in Engine Systems

Facility	Phone Number
Brazil	+55 (19) 3708 4800
China	+86 (512) 6762 6727
Germany	+49 (711) 78954-510
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+82 (51) 636-7080
The Netherlands	+31 (23) 5661111
United States	+1 (970) 482-5811

Products Used in Industrial Turbomachinery Systems

Facility	Phone Number
Brazil	+55 (19) 3708 4800
China	+86 (512) 6762 6727
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+82 (51) 636-7080
The Netherlands	+31 (23) 5661111
Poland	+48 12 295 13 00
United States	+1 (970) 482-5811

Technical Assistance

If you need to contact technical assistance, you will need to provide the following information. Please write it down here before contacting the Engine OEM, the Packager, a Woodward Business Partner, or the Woodward factory:

General

Your Name ____________________

Site Location ____________________

Phone Number ____________________

Fax Number ____________________

Prime Mover Information

Manufacturer ____________________

Turbine Model Number ____________________

Type of Fuel (gas, steam, etc.) ____________________

Power Output Rating ____________________

Application (power generation, marine, etc.) ____________________

Control/Governor Information

Control/Governor #1

Woodward Part Number & Rev. Letter ____________________

Control Description or Governor Type ____________________

Serial Number ____________________

Control/Governor #2

Woodward Part Number & Rev. Letter ____________________

Control Description or Governor Type ____________________

Serial Number ____________________

Control/Governor #3

Woodward Part Number & Rev. Letter ____________________

Control Description or Governor Type ____________________

Serial Number ____________________

Symptoms

Description ____________________

____

If you have an electronic or programmable control, please have the adjustment setting positions or the menu settings written down and with you at the time of the call.

Software Setup Record

Woodward Control Part Number ________________

Find via AppManager Control Information screen:

Computer Name VXM / 505_ / FLEX / VXA____________

Footprint Part Number _______________

Footprint Rev _______________

Service Pack Version _______________

Ethernet #1:

Mode Static IP or DHCP

IP Address __________________________

Subnet Mask __________________________

Default Gateway __________________________

Ethernet #2:

IP Address __________________________

Subnet Mask __________________________

Default Gateway __________________________

Ethernet #3:

IP Address __________________________

Subnet Mask __________________________

Default Gateway __________________________

Ethernet #4:

IP Address __________________________

Subnet Mask __________________________

Default Gateway __________________________

Tunable File Name __________________________.tc

Administrator Password __________________________

Third Party Software Licenses

OpenSSL

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually, both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Redistribution and use in source and binary forms, with or without modification, are permitted when the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written to conform to Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such, any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted when the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Revision History

Changes in Revision G—

- Added Chapter 8 On-line Changes (MicroNet Plus Only) including Table 8-1
- Former Chapter 8 Ethernet Networking is now Chapter 9
- Former Chapter 9 Troubleshooting the Control is now Chapter 10
- Former Chapter 10 Product Support is now Chapter 11
- Product names removed from the cover and header
- Added Figure 1-2. Software Tools Connectivity Overview

Changes in Revision F—

- Added Baud Rate for 505, Flex500, and CPU1020 to Chapter 9
- Corrected debug cable part numbers for Flex500, 505 and CPUMP1020
- New icon for Control Assistant replaced previous icon
- Two new paragraphs added to Chapter 1 General Description
- Figures 3-28 through 3-31 plus 3-33, 3-34, and 3-37 replaced with new images.
- Step 10 added to Manage RTN Controllers section in Chapter 3
- Majority of the content in Chapter 5 is updated or new
- New Section addressing SOS Servlink OPC Server w/CPUs added to Chapter 6
- New bulleted list added to pg. 56
- New Notice box added to beginning of Chapter 10
- Third Party Licenses section added

Changes in Revision E—

- Updated Cyber Security licensing to reference Account Management Licensing
- Added descriptions about Cyber Secure vs Account Management
- Added descriptions and instructions for Secured Application CPUs
- Added description of Secured Application Tool
- Added Open Source License for OpenSSL.

Changes in Revision D—

- Updated Cyber Security licensing information

We appreciate your comments about the content of our publications.

Send comments to: icinfo@woodward.com

Please reference publication 26336.

B26336 : G

PO Box 1519, Fort Collins CO 80522-1519, USA
1041 Woodward Way, Fort Collins CO 80524, USA
Phone +1 (970) 482-5811

Email and Website—www.woodward.com

Woodward has company-owned plants, subsidiaries, and branches, as well as authorized distributors and other authorized service and sales facilities throughout the world.

Complete address / phone / fax / email information for all locations is available on our website.