WOODWARD

Product Manual 26479
(Revision C, 9/2022)
Original Instructions

MicroNet™ Plus & MicroNet™ TMR Cyber Security Manual

Installation and Operation 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:

http://www.woodward.com

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 Out-of-date translations are marked with ⚠.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— A bold, black line alongside the text identifies changes in this publication since the last revision.

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 26479

Contents

WARNINGS AND NOTICES 3

CHAPTER 1. PURPOSE 4

CHAPTER 2. DEFENSE-IN-DEPTH (DID) 5

CHAPTER 3. SYSTEM ACCESS 7
3.1 System Access Points 7
3.2 Password Manager Default Settings 9
3.3 Achieving a Secure Environment 10
3.4 Account Levels 11
3.5 History 13
3.6 Protections 13
3.7 Changing User Passwords 14
3.8 Administrator Tools 14

CHAPTER 4. CONTROL FIREWALL 16

CHAPTER 5. APPLICATION ISSUES 17
5.1 Creating GAP Applications 17
5.2 Using Ethernet Ports for Communications 17

CHAPTER 6. CONFIGURING YOUR EXTERNAL PC 18
6.1 Windows Versions 18
6.2 PC Firewall 18
6.3 Remote Desktop 18
6.4 NetMeeting 18
6.5 Unnecessary Services 18
6.6 DCOM and OPC 19
6.7 Woodward Service Tools 20
6.8 HMI 20

CHAPTER 7. CURRENT VERSIONS 21

CHAPTER 8. PATCH AND UPDATE ROLLOUT PLANS 22
8.1 GAP Coder Version Updates 22
8.2 Footprint Changes 22
8.3 Notifications 22
8.4 National Vulnerability Database (NVD) and SCAP 23

CHAPTER 9. NERC-CIP V6 COMPLIANCE 24
CIP-2 BES Cyber System Categorization (v5.1a) 25
CIP-3 Security Management Controls (v7) 27
CIP-4 Personnel and Training (v6) 28
CIP-5 Electronic Security Perimeter (v5) 29
CIP-6 Cyber Security - Physical Security of BES Cyber Systems 33
CIP-7 Systems Security Management (v6) 33
CIP-8 Incident Reporting and Response Planning (v5) 37
CIP-9 Recovery Plans (v6) 38
CIP-10 Configuration Change Management and Vulnerability (v2) 38
CIP-11 Information Protection (v2) 40
CIP-13 Supply Chain Security 41
CIP-14 Physical Security 41

CHAPTER 10 FREQUENTLY ASKED QUESTIONS 42

CHAPTER 11. PRODUCT SUPPORT AND SERVICE OPTIONS 45
Product Support Options 45
Product Service Options 45

Returning Equipment for Repair 46
Packing a Control 46
Replacement Parts 47
Engineering Services 47
Contacting Woodward's Support Organization 48
Technical Assistance 48

GLOSSARY 50

REVISION HISTORY 53

REFERENCES 54

Illustrations and Tables

Figure 2-1. Defense-in-Depth (DiD) 6
Figure 9-1. NERC-CIP Coverage Matrix 24
Figure 9-2. EACMS Architecture 29

Table 1-1. CPU Information 4
Table 1-2. Reference Documents, Manuals, and Information 4
Table 3-1. Access Points and SIEM Log Files 7
Table 3-2. Default Access Control Accounts and Passwords 8
Table 7-1. Baseline Configuration Versions 21
Table 9-1. Functional Responsibilities for Requirement Allocation to Entities 26
Table 9-2. Port Map for Routable Protocols 30
Table 9-3. Security Controls for Detecting Malicious Communications 32

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.

Chapter 1.
Purpose

This manual provides information on cybersecurity strategies for the Woodward MicroNet Plus and MicroNet TMR turbine control systems. Woodward offers CPUs that with a variety of cybersecurity capabilities including user account management with secure passwords, secure applications and encrypted communications. Some versions are Achilles certified.

The minimum CPUs that should be considered for use in security-critical applications are versions with user levels and secure passwords. The 5466-1035 and -1141 CPU on MicroNet Plus and the 5466-1047 and -1247 CPUs for MicroNet TMR do not meet these requirements. If your system has one of these CPUs (or an older Pentium/NT CPU with Ethernet) the system should be upgraded to one of the modern CPUs for security.

Table 1-1. CPU Information

MicroNet Plus

CPU	Preferred	Min. Coder	Secure Passwords	Achilles Cert	SSH/Firewall	SecureApp
5466-1035	No	4.06	No	No	No	No
5466-1045	No	6.00-1	Yes	No	Yes	No
5466-1141	No	6.00-4	No	No	No	Yes
5466-1145	No	6.00-4	Yes	Yes	Yes	No
5466-1245	No	6.00-4	Yes	No	No	No
5466-1511	Yes	Plus 1.02	Yes	Yes	Yes	No
5466-1521	Yes	Plus 1.02	Yes	Yes	Yes	Yes

MicroNet TMR

CPU	Preferred	Min. Coder	Secure Passwords	Achilles Cert	SSH/Firewall	SecureApp
5466-1047	No	4.06	No	No	No	No
5466-1247	No	6.00-1	Yes	No	Yes	No
5466-1347	Yes	TMR 1.01	Yes	Yes	No	No

Table 1-2. Reference Documents, Manuals, and Information

Security Device/Appliance	Artifact / Document
MicroNet Plus	Control Manual (#26166V1, 26166V2, 26166V3) VxWorks RTOS Software Manual (#26336) Achilles Certification report (see Appendix –Achilles Certification Excerpts)
MicroNet TMR	Control Manual (#26167V1, 26167V2, 26167V3) VxWorks RTOS Software Manual (26336) Achilles Certification report (see Appendix –Achilles Certification Excerpts)
SOS	Help file—select Help/Help from the SOS tool
GAP Program	Help file—select Help/Help from the GAP™ Editor tool
AppManager	Help file—select Help/Help from the AppManager tool
Typical System	See Figure 9-2 EACMS Architecture
Project Deliverable	Project specific Network Configuration Document(s)
Moxa EDR-810	Woodward Manual 35095 MOXA EDR-810 Service Manual
Tofino Xenon	Woodward Manual 35097 Belden Tofino Xenon Service Manual
Configuration Management Monitoring Appliance	

Additional supporting citations are listed in the References section.

Chapter 2.
Defense-in-Depth (DiD)

This chapter introduces the concept of Defense-in-Depth (DiD) with respect to industrial control systems.

Woodward DiD recommendation for secure MicroNet installations:

- Use a MicroNet CPU with secure passwords (5466-1511, 5466-1521 or 5466-1347)
- Ensure that the user levels are correctly set and each user assigns and maintains a secure password.
- Maintain physical security. Limit physical access to authorized and trained personnel. Log who enters the control area and why.
- Minimize external Ethernet connections to HMI's, Engineering Workstations and the MicroNet. Secure necessary connections with a deep packet inspection device such as Tofino (described later in this manual).
- Windows-based PCs represent a significant attack vector for an industrial control system. Consider using hardened PC's or thin client servers for these applications.
- Ensure that the OS on any PC connected to the control system are part of a regular patch management program.
- Ensure that any other network element, such as switches, that are used in external Ethernet connections are hardened devices and are properly updated for any known vulnerabilities

The following chapters of this manual discuss the implementation and configuration details of security controls and appliances used to achieve DiD. Figure 2 1 Defense-in-Depth (DiD) summarizes these methods and techniques.

The attack vectors in Figure 2 1 Defense-in-Depth (DiD) illustrate a few examples of attacks which could impact the availability and integrity of industrial control systems. A man-in-the-middle attack could exploit vulnerabilities of OPC or Modbus communication networks. One scenario for this type of attack involves an attacker controlling and possible altering messages/packets/data between two parties. In a man-in-the-middle attack the integrity of sensor date or output commands could be compromised leading to the loss of an asset. A replay attack can have the same impact, but it exploits valid messages/packets/data which are repeated/delayed in order to fool the parties into believing a false context exists. One scenario for this type of attack could be the replay of a valid start permissive which disrupts the intended sequence of operation.

A Denial-of-Service (DoS) or a Distributed-Denial-of-Service (DDoS) are intended to attack a system's availability and prevent normal control functions and operations. Dos/DDoS attacks often exploit network vulnerabilities by overwhelming routers and network adapters with unnecessary traffic. DiD provides multiple layered security controls, from software development practices to real-time monitoring and Deep Packet Inspection (DPI) of network traffic, to help deter attacks and mitigate cyber risks.

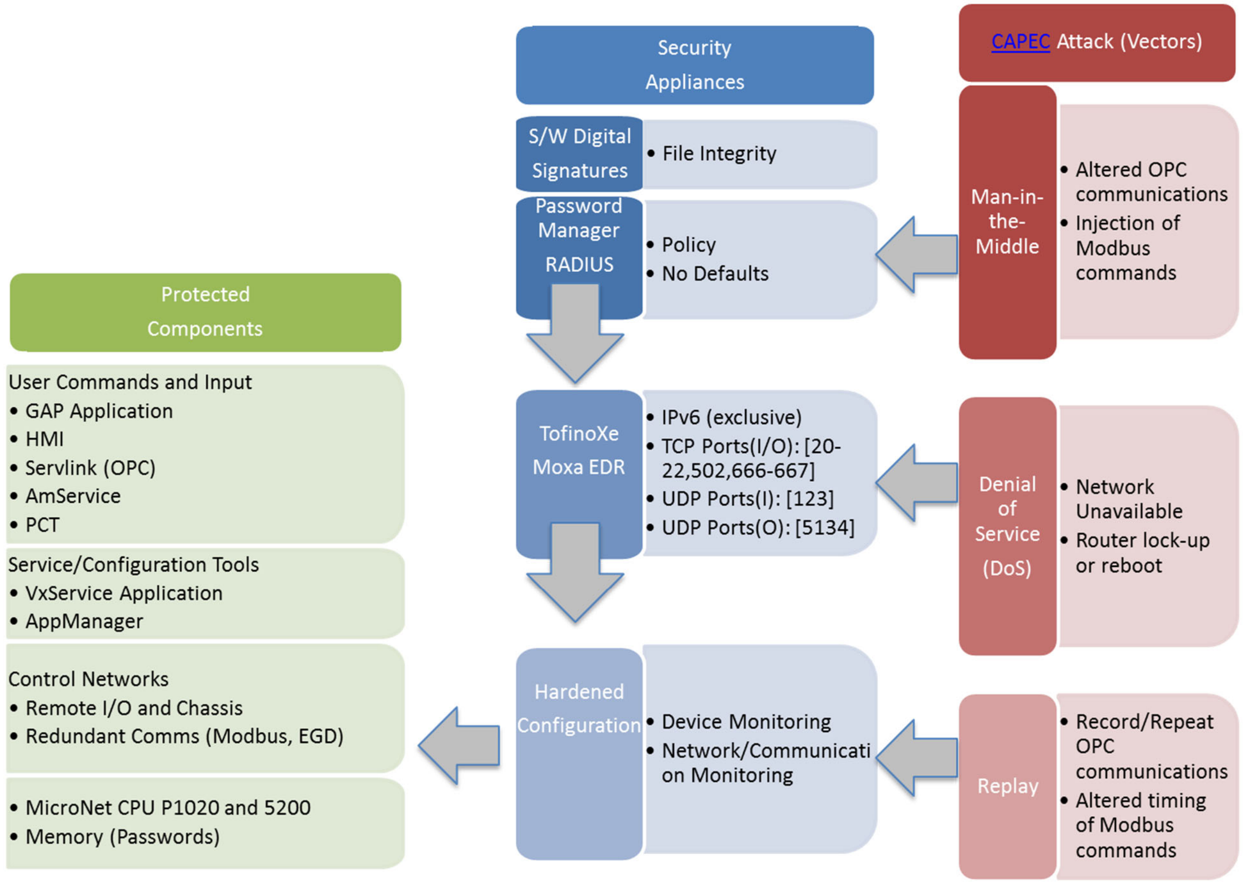


Figure 2-1. Defense-in-Depth (DiD)

Chapter 3.
System Access

3.1 System Access Points

The Woodward VxWorks RTOS Software Tools Manual 26336 identifies the following system software tools with publicly available installers. Some software, however, requires a purchased license before authorization. The default accounts and passwords for these applications have been compile below in Table 3 2 Default Access Control Accounts and Passwords. For system security, it is critical to follow the instructions and consider the recommendations in section 3.4 Achieving a Secure Environment.

Table 3-1. Access Points and SIEM Log Files

Access Point	SIEM Log File(s)	Description
ACA21-USB		Tofino Xenon USB auto-configuration adapter interface (FAT or FAT32 format)
AppManager		GAP software application file management/loader (see *Help*)
Control Assistant		Control Assistant is a utility designed to communicate with Woodward controls over serial or Ethernet connections. Supports: •Live parameter monitoring and tuning •Tunable maintenance (tunable captures, editing, comparing and uploading) •Alarms and Events viewing from SOS servers/controls with AE support •Graphing and trending
GAP Application	Configuration Error Log (.log?) Alarm Log Event Log	System Logs PCT allows exporting
GAP Programmer (Woodard Coder)		
iFix		User Interface (HMI / GUI)
Ladder Logic		
Monitor GAP (and GAP Editor)		
NetSim[1]		The suite of tools used for running simulations of equipment controlled by GAP-based Woodward systems.

[1] License required

Access Point	SIEM Log File(s)	Description
Secured Application Tool (SAT) MicroNet Plus only 5466-1141 and -1521 CPUs		Secured Application Tool (SAT) software is designed to support the creation of a secured application files for use in the Woodward MicroNet® Plus Secured Application product line. SAT also helps manage and store Authorization Encryption File(s) from individual MicroNet® Plus Secured Application CPU(s).
Service Packs		
SFTP		
SOS Servlink	SOS.log	OPC communication events and errors: SOS help (SOS.exe or SOS.chm) – SOS Log file
Tofino Configurator	remote syslog server or eventlogger_<tofino id>.#{1-20}.zip	A Windows-based configuration management tool for the Tofino Xenon which permits a network connection when the *NetConnect LSM* has been loaded on the device. While the Tofino Xenon does not require an IP address to communicate with a remote syslog server, messages will appear to originate from the default IP address 169.254.2.2 unless the Syslog Address settings is configured differently. The USB port is disabled by default (seeCIP-4 R1.3)
Toolkit [2]		ToolKit is used to create and run custom administration tools for many Woodward electronic products. The resulting tools can be used to configure, calibrate, monitor and troubleshoot your device over a serial, CAN, or TCP/IP connection.
MOXA **EDR-810** (Network Interface)		IP Address: 192.168.127.254 (default)
MOXA **EDR-810** (Command Line Interface - **CLI**)		RJ45 RS-232 Serial Console (115200, 8, None, 1, VT100) or Telnet Console

Table 3-2. Default Access Control Accounts and Passwords

Access Point	Default Account	Default Password [3]
ACA21-USB		
AppManager	Datalog [4] (Account Level 1)	Datalog@1
Control Assistant		
GAP Application		
GAP Programmer (Woodward Coder)		
iFix		
Ladder Logic		

[2] Freeware

[3] See CIP-7 R5.3 Default Passwords requires that all default passwords be changed prior to activating and operating a control system.

Access Point	Default Account	Default Password [3]
MicroNet CPU	Administrator [4] (Account Level 15)	Admin@1
MicroNet CPU	Datalog [4] (Account Level 1)	Datalog@1
MicroNet CPU	ServiceUser [4] (Account Level 11)	ServiceUser@1
Monitor GAP		
Monitor GAP (and GAP Editor)		
NetSim		
Secured Application Tool (SAT)		
SFTP		
SOS Servlink	ServiceUser [4] (Account Level 11)	ServiceUser@1
Tofino Configurator		
Toolkit		
MOXA EDR-810 (Network Interface)	admin	moxa
MOXA EDR-810 (Command Line Interface - CLI)	admin user	(null) (null)

3.2 Password Manager Default Settings

The MicroNet™ Plus and TMR controls with user account management and secure passwords come pre-configured with the following security accounts:

1. Administrator (May not be renamed or deleted)
    a. Password: Admin@1 (Should be changed to enable security)
    b. Level: 15 (May not be changed)
    c. Duration: No Expiration (Should be changed to enable security)
    d. Fixed Password: No (May not be changed)
    e. Role: Master account for managing other accounts

2. ServiceUser (May be renamed or deleted)
    a. Password: ServiceUser@1 (Should be changed to enable security)
    b. Level: 11 (May be changed)
    c. Duration: No Expiration (Should be changed to enable security)
    d. Fixed Password: Yes
    e. Role: Shared account for high level access
    f. May be cached (encrypted) in Security Options area of the SOS Servlink OPC Server program to simplify automatic access from SOS to control (not secure)

3. Datalog (May be renamed or deleted)
    a. Password: Datalog@1 (May be changed)
    b. Level: 1 (May be changed)
    c. Duration: No Expiration
    d. Fixed Password: Yes
    e. Role: Shared account for minimal access (e.g. reading files)
    f. The AppManager program uses the credentials of this account, by default, to collect datalog files and to look at controls specified in the Administer Controls List of AppManager. If the account is changed, AppManager may be updated to use a different set of credentials for these functions.

[4].The GAP application permits configuration of the Security Level associated with each user account. More information is available in 3.2 Password Manager Default Settings and 3.4 Account Levels.

3.3 Achieving a Secure Environment

NOTICE

The passwords of all of default accounts should be changed to enable security upon installation and periodically (at least annually) from then on. CIP-7 R5.3 Default Passwords requires that the owner/operator is responsible for changing all default passwords prior to operation.

NOTE on RTN Credentials: If the control system includes a set of expansion chassis in a Real Time Network (RTN), these are also preconfigured with the default accounts. The RTN is on a private control-only network, so it is only accessible after first logging into the main CPU and is thus not vulnerable to unprivileged access. Its credentials may be left at default or changed to match the credentials on the main CPU. Credentials may be changed on an RTN CPU as follows:

1) Login to the main CPU with the AppManager tool
2) Use the Manage RTN CPUs… command from the Control menu of AppManager
3) Right-click on the desired RTN CPU from the window which appears
4) Select Administer Accounts
5) Specify Administrator credentials when prompted to login to the RTN CPU

4. The SOS Servlink OPC program should be configured to enable the OPC security interface. This interface requires client programs to pass in credentials rather than using credentials stored on the SOS Security Options page.

   Note on SOS Credentials: SOS can be configured to communicate with multiple controls. Some OPC clients, like Woodward’s Control Assistant or an HMI tool, can communicate, through SOS, to these different controls simultaneously. If multiple controls are to be serviced at one time with a PC running the SOS program, it is recommended to create the same account configuration on each control. Each client tool can only specify one set of credentials for all controls (this is especially true if the default credentials of SOS are used); if these credentials correspond to different or non-existent security levels, the tool behavior may be confusing.

5. The MicroNet Plus controls with SSH encryption have built-in firewalls (see Chapter 4, Control Firewall) which only allows access to the Secure Shell (SSH) port and any ports which the application exposes.
   a. Ethernet ports like those used by Modbus® * or EGD are not secure. Data in such a network can be viewed and possibly modified. For a secure control, it is recommended to use SOS to achieve HMI communication (through OPC) instead of using unsecure protocols like Modbus or EGD. SOS uses the SSH port and thus all of its communications are protected by login access and encrypted transfer.
   b. Even the SSH port is vulnerable to DNS (“Denial of Service”) attacks such as data-storm attacks. While it is not possible to read or write data to this channel maliciously, it is possible to make the port so busy that desired communication cannot reliably transpire. As such, it is recommended not to put any mission-critical functionality exclusively into remote devices like an HMI PC. Instead, hard-wired operation controls should be established for emergency control in case of communication unavailability.

*—Modbus is a trademark of Schneider Automation Inc.

3.4 Account Levels

Different accounts may be assigned different security levels (0–15). This provides a way to differentiate authority levels of different users. Account levels are created and maintained by an Administrator (see 4.7 Administrator Tools).

1. Security levels protect privileged functionality in AppManager and in SOS.
2. Higher levels contain all of the authority of lower levels.
3. Gaps are left in the level map to allow the application program to create intermediate levels. Application-generated levels apply only to Servlink (SOS) functionality (see item 5 below, Servlink (SOS) Security).
4. AppManager ("Vx-Service") security levels
    a. Level 0
        i. Commands
            - Connect
            - Login
            - Logout
            - Change Password   ii. Level "0" is not a recommended account level. However, when the password expires on an account with a higher level, its level becomes "0" until the account is reset, or the password is changed

        ii. This is the lowest level

    b. Level 1
        i. Commands
            - Read Control Information
            - Read files
            - Explore Module Information
            - Explore RTN Information

        ii. Minimum level for automatic datalog retrieval feature
        iii. This is the level of the default account "Datalog"

    c. Level 11
        i. Commands
            - Write files
            - Delete files
            - Start applications
            - Stop applications
            - Stop automatic application start ("Clear Autostart")
            - Reboot control
            - Execute control service packs
            - Execute module service packs
            - Change network configuration

        ii. This is the level of the default account "ServiceUser"

    d. Level 15
        i. Commands
            - View accounts
            - Add account
            - Delete account
            - Reset account

        ii. This is the level of the Administrator account
        iii. This is the highest level

5. Servlink (SOS) Security – Systems with SSH encryption only
    a. Servlink security levels apply to reading and writing application values. They also apply to Servlink commands executed by SOS, such as Set Control Identifier, Reset and Shutdown.
    b. Applications compiled for MicroNet Plus Cyber Secure controls have a default security configuration, which is recommended. It is possible to override this configuration by modifying parameters in the SYS_INFO block of the application (see SYS_INFO in the GAP Block Help). These parameters are fixed at application build time and can't be modified on-line.
    c. Levels
        i. Default read security ("SYS_INFO.RD_SEC")
            - Default level (if not specified in SYS_INFO block): 4

- Any value in the application without a specified read security level is given this level.
- To override the default read security level for a value, the GAP application may be modified to connect an HMI_PT or HMI_ENUM block to the value (see HMI_PT and HMI_ENUM in the GAP Block Help).

ii. Default write security (“SYS_INFO.WR_SEC”)

- Default level (if not specified in SYS_INFO block): 7
- Any value in the application without a specified write security level is given this level.
- To override the default, write security level for a value, the GAP application may be modified to connect an HMI_PT or HMI_ENUM block to the value (see HMI_PT or HMI_ENUM in the GAP Block Help).

iii. Browse security (“SYS_INFO.BROWSE_SEC”)

- Default level (if not specified in SYS_INFO block): 2
- This is the authorization level required to browse the namespace of a Woodward control. The Control Assistant tool uses browsing to create the value tree shown at the left of the WinPanel. Other OPC client tools also require this functionality to display available control values.
- In some circumstances, it may be desired not to reveal the namespace (a map of all the value names in the application), but still provide access to some values through an HMI tool. The HMI tool can be configured using enough security to browse the namespace (e.g. by a developer with high authority) but can be run with less security (e.g. by an operator with limited authority).

iv. Control read security (“SYS_INFO.CTL_RD_SEC”) • Default level (if not specified in SYS_INFO block): 1

- This is the authorization level required to read control information strings like the configuration ID

v. Control write security (“SYS_INFO.CTL_WR_SEC”) • Default level (if not specified in SYS_INFO block): 7

- This is the authorization level required to write control information strings like the configuration ID. It is also required for saving changed values to non-volatile memory.
- This level is required for uploading a control configuration
- Control start/stop security (“SYS_INFO.CTL_SS_SEC”)
- Default level (if not specified in SYS_INFO block): 11
- This is the authorization level required to perform a shutdown or reset. This level is also required to change the control ID string.
- Since this parameter controls functionality in Servlink (Shutdown, Reset) which is very similar to AppManager functionality in level 11 (Stop, Start), it is recommended to leave this value at “11” in MicroNet Plus Cyber Secure controls. However, this is not required.

3.5 History

1. The following files are stored in the MicroNet Plus and TMR controls
   a. PMLog.txt
      i. Contains all successful and unsuccessful logins and logouts.
      Note: There may be more than one entry per successful login
      ii. Contains password changes
      iii. Contains other account modifications (by Administrator) iv. All entries are marked with the date and the account name of the accessing user
   b. Log.txt
      i. Contains application events
      ii. Identifies and dates privileged access which modify control contents StartApplication
         - StopApplication
         - ClearAutostart
         - ExecuteServicePack
         - Update Module
         - Write file
         - Reboot control
         - Change network configuration
2. These files may be retrieved using the Retrieve System Log Files command from the Control menu of AppManager
3. These files are limited in size to 1 MB. When a log file is about to exceed this size, it is copied to a backup file (“Log.old” or “PMLog.old”) and a new file is started. Thus, the amount of history that can be captured is somewhere between 1 MB and 2 MB of ASCII text. This is likely to represent a long period of use, but there is no easy correlation between the size of the file and the length of the history. It is recommended to periodically retrieve and store these files with a date-based name to avoid losing history (see NERC CIP-007 R6.3 and R6.4).

3.6 Protections

Failed attempt limiter –The MicroNet Plus and TMR control prevents automated guessing of passwords by limiting the number of unsuccessful login attempts in a short period of time. If 12 attempts within a short period of time are made to login to an account using the wrong password, login access to that account is disabled for 15 minutes. The actual strategy follows two rules:

- Increment a counter for every unsuccessful login and to decrement it by three every 15 minutes. While the count exceeds 12, all attempts to login are rejected with a security violation failure.
- Unsuccessful Login attempts from AppManager and SOS count equally. SOS calls the login routine every time an OPC client passes it credentials, even if SOS already has a connection.

3.7 Changing User Passwords

1. The account must be connected using the AppManager tool. For more information, consult the Help document of the AppManager tool
2. Use the Change Password command of the AppManager tool
3. The Account Name may not be changed
4. Password expiration
    a. Some user accounts may be configured by the Administrator to expire after the same password has been in use for a specified duration (see 3.7 Administrator Tools / 1.d).
    b. When the password expires, the level of the account will be set to the minimum authority level, zero, and the user will be prompted to change the password when he/she next attempts to log in through AppManager.
    c. If the password has expired, it is still possible to connect and change the password, starting a new expiration period
5. Password Rules
    a. The new Password must be different from previous password
    b. The Password must be between 6 and 30 characters in length (inclusive)
    c. The Password must contain at least 2 alpha (A-Z, a-z) and 2 non-alpha (0-9,!,@,#,…) characters
    d. The Password is case sensitive

3.8 Administrator Tools

Use the Administer Accounts function of the AppManager tool. For more complete instructions, consult the Help document of the AppManager tool and/or the MicroNet Plus software manual (#26336). The following functions are supported:

1. Creating new accounts
    a. Account Name
        i. The Account Name must be unique
        ii. The Account Name must be between 4 and 30 characters in length (inclusive)
        iii. The Account Name may consist of any combination of alpha (A-Z, a-z) or non-alpha characters (0-9, !,@,#...)
    b. Password
        i. The Administrator may specify an initial password or a fixed password
        ii. The Password must comply with the password requirements (see 3.8 Changing User Passwords)
    c. Level
        i. Any level between 0 and 14 (inclusive) may be specified
        ii. The level 15 is reserved for the Administrator account, of which there may be only one
    d. Duration
        i. The Duration may be set to any number of days after which the password will expire
        ii. A Duration of zero will prevent the password from automatically expiring. If the duration is zero, the string “No Expiration” will be displayed
        iii. NERC CIP requires changing passwords at least annually, so a duration of 365 or fewer days is recommended
    e. Fixed Password
        i. Fixed passwords may be used for shared accounts, so that users are not able to change the password
        ii. Since users may not change the password, it is the Administrator’s responsibility to periodically review and possibly change the password of these accounts
        iii. If an account is given a fixed password and a non-zero expiration, the account may expire and require an Administrator’s intervention to provide a new password before the account is returned to full functionality
2. Temporary Accounts
    a. To achieve a temporary account, a fixed password may be assigned together with the desired Duration value. Once the password has expired, the account will no longer be usable, and the Administrator can delete or modify it at his/her convenience
3. Deleting accounts
    a. Select the account(s) and press the Delete key.

4. Reset existing accounts
    a. Select the account(s) and press the Reset key
    b. This will reset the password and provide edit access to the remaining account configuration fields
5. Changing Administrator Account
    a. The Administrator account may be changed like other accounts through the Administer Accounts command of the AppManager tool, with the following differences:
    b. Account Name is Fixed as “Administrator”
6. Password
    a. May be changed at any time using the same mechanism as changing a user account password (see 4.6 Changing User Passwords). Cannot be changed through the Administer Accounts function
    b. Be careful! If the password is lost, it cannot be recovered
    c. Administrator passwords have the same complexity requirements as user passwords (see 4.6 Changing User Passwords / 5)
    d. Level is Fixed at 15 (the maximum)
    e. Duration of the Administrator account is subject to the same rules and recommendations as user accounts (see 1.d. Duration)
7. Fixed Password
    a. Not allowed for the Administrator account

Chapter 4.
Control Firewall

The MicroNet™ Plus controls with SSH encryption have a firewall which disables access to all but the following ports:

1. The SSH port (22). This port is secure.
    a. This port may be used for communicating with the SOS Servlink OPC

Server program which can serve data to

1. Monitor GAP
2. Control Assistant
3. Another OPC client application (e.g. an HMI program) o This port is used by the AppManager tool
    a. This port is safe from eavesdropping and tampering. However, it may be vulnerable to data-storm type attacks. It is possible, through malicious flooding of data to this port, to prevent desired data from getting through. As such, a secure system requires that all critical control functions (like Start/Stop) be available through a hard-wired control panel. Please consult your Woodward service representative for suggestions about configuring control panels.
    b. Any port which the GAP application enables. These ports are not secure: No encryption is performed on the communication channels, so data could be read and possibly even written to these ports. As such, this functionality is not recommended in a secure system unless the security perimeter includes this network. Examples:
        i. Modbus
        ii. EGD
        iii. PROFIBUS
        iv. Fieldbus

Chapter 5. Application Issues

5.1 Creating GAP Applications

For instructions about how to use the GAP Programmer to create or modify applications in the GAP programming language, please consult your GAP Programmer manuals. Cybersecure GAP applications require the following additional changes:

- The following applies to MicroNet Plus only when equipped with a 5466-1045 or 1145 5200 CPU or any P1020 CPU.
- The CPU block must be an instance of CPU_MC5200 or CPU_P1020
- The SYS_INFO block may be configured to set the levels for Servlink command and value access (see 3.3 Password Manager Configuration / Account Levels / 5). It is suggested to leave these values at their defaults (these are displayed in Password Manager Configuration / Account Levels 5)
- Any readable (outputs) or writable (tunable inputs) application values will inherit the default read and write security levels specified in the SYS_INFO block (as described above). To override these security levels to a lower (more permissive) or higher (more restrictive) value, an HMI_PT, HMI_ENUM or QSERV_HDR block may be tied to the value. The HMI_ blocks also allow specifying descriptive information about the application value for the service interface. For information on adding and configuring HMI_PT, HMI_ENUM or QSERV_HDR blocks, please consult the BlockHelp feature of the GAP Editor program.
    - The LATCH_AE block also has a parameter for overriding the default read security level. This level determines the authority level required to read OPC Alarm and Event (OPC AE) information.
- In previous versions of the GAP Programming language, a block named “PASSWORD” was used to create a security framework. The PASSWORD block is still available on some Woodward controls, but is not allowed in MicroNet Plus Cyber Secure applications. Password functionality is implemented on the MicroNet Plus control and maintained by the AppManager tool (see Chapter 3 Password Manager Configuration).

5.2 Using Ethernet Ports for Communications

As described in Chapter 4 (Control Firewall), all Ethernet ports on the control except for the SSH port are disabled unless they are opened by the GAP application. If the GAP application specifies use of an Ethernet port, it will not be secure. It is recommended to extend the security perimeter to include this network. If not,

- All traffic on this Ethernet port can be spied upon • Data can be tampered with and possibly spoofed
- The port can be attacked with data-storms to prevent valid usage

Examples of GAP Application Ethernet usage:

- Modbus
- EGD
- PROFIBUS
- Fieldbus

Chapter 6.
Configuring Your External PC

6.1 Windows Versions

The AppManager, Control Assistant, GAP™, and SOS tools require the Microsoft .NET Framework version 4.0 or greater to be installed. Windows is a registered trademark of Microsoft Corporation.

6.2 PC Firewall

Woodward recommends the following security measures for computers which connect to a MicroNet™ Plus or TMR control:

- Intrusion Detection & Prevention systems
- Proxy servers
- Web filtering software
- Spam control
- IPSec VPN
- Two-factor authentication for Remote Connectivity
- Anti-virus on e-mail gateway, e-mail servers & internet gateway
- WPA2 encryption for wireless control and Wireless Intrusion Prevention

Woodward offers hardened PCs and thin client servers for use as HMI or Engineering Workstations. Please contact your Woodward representative if you would like a quote on these services.

6.3 Remote Desktop

Remote Desktop functionality may allow a networked user to control the PC. In a secure system, such functionality should be disabled.
To use the computer's local group policy to disable Remote Desktop:

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. In the Group Policy editor, click to expand Computer Configuration, click to expand Administrative Templates, click to expand Windows Components, and then click to expand Terminal Services.
3. Double-click the Allow users to connect remotely using Terminal Services policy.
4. Set the policy to Enabled, and then click OK.

You can also use the following procedure to disable Remote Desktop; however, if you use the preceding procedure, the following configuration is overridden:

1. Right-click My Computer and click Properties.
2. Click the Remote tab.
3. In the Remote Desktop section, click to clear Allow users to connect remotely to this computer, and then click OK.

6.4 NetMeeting

Any PC connected to the MicroNet Plus or TMR control should not run NetMeeting in desktop sharing mode.

6.5 Unnecessary Services

The PC connected to the MicroNet Plus or TMR control should not be running any unnecessary services.

6.6 DCOM and OPC

SOS uses OPC to communicate control data to client tools such as HMI programs, Monitor GAP and Control Assistant. OPC relies on Microsoft COM or DCOM technology to communicate between different processes. COM communicates between different processes within the same computer and DCOM implements COM across different computers on the same network.

SOS can and should be configured to require each client application to provide login credentials (select Enable OPC security interface in the Security tab of the Options window). This setting ensures that only authorized users can gain access to privileged control data and functionality. If this interface is not required by SOS because of ease-of-use considerations or because a client OPC program does not have the required credentials interface (see SOS), DCOM security should be hardened to ensure approved use. As such, Woodward recommends running OPC client applications on the same PC as SOS and disabling DCOM access to SOS. If it is necessary to remotely connect to SOS, DCOM should be configured for maximum security.

6.6.1 Configuring DCOM Security

To view and edit DCOM settings, run the program dcomcnfg from the run menu of Windows

1. Select Start from the taskbar (usually bottom left)
2. Select Run…
3. Type in dcomcnfg and select OK

6.6.2 Disabling DCOM Access to SOS

One way to disable DCOM access to SOS is to disable DCOM for all applications on the PC. This is the most secure choice:

1. Right-click on Component Services / Computers / My Computer
2. Select Properties
3. Select the Default Properties tab
4. Uncheck Enable Distributed COM on this computer

To Disable DCOM access just for SOS:

1. Right-click on DCOM Config / Woodward.ServLinkOpcDa.1
2. Select Properties
3. Select the Location tab and uncheck all of the Run… checkboxes (notably Run application on this computer)

6.6.3 Remote Access Hardening

If remote access to SOS is required, SOS must be configured to require credentials (select Enable OPC security interface in the Security tab of the Options window). DCOM should be configured as securely as possible. For suggestions on hardening DCOM, please consult the following reference information.

6.6.4 Reference Information

For a complete discussion of OPC security considerations, please consult the Tofino™ Security White Paper “Securing Your OPC Classic Control System” at the following link:
www.tofinosecurity.com/professional/securing-your-opc-classic-control-system

More information can be found at the following links (links valid as of 2010):

- www.pacontrol.com/OPC.html
- www.opcconnect.com/dcomcnfg.php
- www.controlglobal.com/articles/2010/OPCSecurity1008.html

6.7 Woodward Service Tools

6.7.1 AppManager

Woodward's AppManager program is the user interface for managing applications and configuring security accounts on the control. AppManager communicates with the control over a secure TCP channel (SSH). For more information about AppManager, consult the AppManager tool's help document and Chapter 3 (Password Manager Configuration) of this document.

6.7.2 SOS

Woodward's SOS Servlink OPC Server is a tool which communicates with a MicroNet Plus control through a secure TCP channel (SSH). It is used to communicate OPC information (OPC DA (Data Access) and OPC A&E (Alarms and Events)) to client tools which know how to use it. Example client tools:
Monitor GAP

- Control Assistant
- Excel spreadsheets
- OPC –Ready HMI applications

6.7.3 Monitor GAP

Woodward's Monitor GAP is a tool within the GAP program for viewing live control values in the context of the application program. Monitor GAP uses OPC to communicate with the SOS tool.

6.7.4 Control Assistant

Woodward's Control Assistant is a tool for service access to a control. It may be used to view and modify control parameters, and graphically view data trends and stored data log files. Control Assistant uses OPC to communicate with the SOS tool.

6.8 HMI

An HMI is a tool for operating and displaying information from a control. HMI tools which support the OPC interface can communicate with Woodward controls through the SOS OPC interface. SOS communicates securely with the control and OPC may be configured to run securely on a PC (see 6.6 Configuring your External PC / DCOM and OPC). For the most secure configuration, SOS requires that the HMI tool presents login credentials (see 6.6 Configuring your external PC / DCOM and OPC). If the HMI tool does not support the IOPCSecurityPrivate interface, it cannot supply credentials to SOS and the Options / Security page of SOS must be modified to not require credentials (this is not a secure configuration). If the credentials interface is not active, it is strongly recommended to limit SOS support of DCOM to the local PC (see 6.6 Configuring your external PC / DCOM and OPC).

Even in a secure configuration, the port used by SOS (the SSH port) can be attacked with data-storms, causing SOS performance to suffer. For a secure system, all critical control functionality implemented through SOS (e.g. through the HMI) must have a backup hard-wired replacement like a control panel. Please consult your Woodward service representative for suggestions about configuring control panels.

For more information about configuring an HMI tool to access SOS values, please consult the Help document of the SOS tool.

Chapter 7.
Current Versions

The following table contains the current versions of system components and can be used to create a baseline configuration for configuration management (CM).

Table 7-1. Baseline Configuration Versions

Component	Type	Part No.	Version
AppManager	Software Application	9927-785	3.#
Configuration Management Monitoring Appliance	Custom Application	NA	NA
Control Assistant	Software Application	9927-1237	4.#
GAP Editor	Software Application	9927-1591	4.##
GAP Programmer	Software Application	9927-2059	6.00-0
MicroNet Plus CPU Module	Hardware	5466-1511 5466-1521	
MicroNet TMR CPU Module	Hardware	5466-1347	
MicroNet Plus CPU Software	Firmware	5418-7799	
MicroNet TMR CPU Software	Firmware	5418-7790	
Moxa EDR-810 Configuration	Configuration	10-004-485	
Moxa EDR-810 Firmware	Firmware	10-004-484	
SOS	Software Application	9927-1223	
Tofino Xenon Configuration	Configuration	10-004-488	
Tofino Xenon Firmware (A customer account and License Activation Key is required)	Firmware	10-004-487	

These versions and part numbers are subject to change. For the latest versions, consult the Woodward website at **www.woodward.com**. The latest software versions are available for download at **www.woodward.com/software/**.

Chapter 8.
Patch and Update Rollout Plans

8.1 GAP Coder Version Updates

New versions of the GAP Coder programmer are typically released several times a year. Newer versions are usually compatible with older applications and control footprints, but it may be necessary to check the version release notes. It is not necessary to use the latest GAP Coder version, but it may be desirable if there are desired features or defect fixes.

8.2 Footprint Changes

The MicroNet control is loaded with an operating system and configuration files. This configuration is called the “Footprint” and provides the environment for running GAP control applications.

8.2.1 Service Packs

Periodically, Woodward modifies the contents of a footprint to address bugs or vulnerabilities or to add functionality. To update the footprint in the field, Woodward provides software patches which may be applied to a control by the AppManager tool. These patch files are named “Service Packs”. Service Packs are labeled with a version and a description of what changes are incorporated.

8.2.2 Installing a Service Pack

Installing a service pack will not change the Password Manager configuration on the control. To install a service pack:

1. Login with enough credentials to the control using the AppManager tool (see 3.3 Password Manager Configuration / Account Levels / 4.c).
2. Ensure that the control application is stopped (the application status is displayed in the right window of the AppManager tool).
3. Select Install Service Pack… from the Control menu of the AppManager tool.
4. AppManager will guide you through the installation process.
5. You will be prompted to reboot to finish implementing the changes.

8.3 Notifications

How are users notified if a security issue has been discovered?
When defects or vulnerabilities in Woodward control software are discovered, a corrective action committee reviews the issue. Typically, the NIST NVD will publish vulnerabilities prior to the availability of a patch or update. In these cases, or if a third-party component supplier is working to resolve the issue, the committee will publish a Woodward Application Note to http://www.woodward.com/searchpublications.aspx. When a patch, update, or mitigation procedure is available and critical to the correct operation of the control system, the committee will create a service bulletin. The service bulletin will explain the problem and a suggested course of action and will be emailed to all Woodward product distributors and customers who have purchased or downloaded the product directly from Woodward.

How can users ask questions about security or report security issues to Woodward?
Woodward has established a help desk for security-related issues. Please email questions or reports to CybersecurityHelpDesk@woodward.com.

How are users notified about new releases?
GAP Coder version update notices are sent to Woodward distributors for dissemination to end customers. The update notices list revisions to the product.
The Woodward website (www.woodward.com/software/) also lists all available software downloads, complete with revision descriptions.

8.4 National Vulnerability Database (NVD) and SCAP

Automated Continuous Diagnostics and Mitigation (CDM) commonly leverages the NIST National Vulnerability Database (NVD) and the Security Content Automation Protocol (SCAP) interface. Many Configuration Management Monitoring Appliances support SCAP interface functionality and are utilized to monitor for new vulnerabilities and record notifications in a log file. See CIP-6 R2.1 Tracking, Evaluating, and Installing for further implementation details.

Chapter 9.
NERC-CIP v6 Compliance

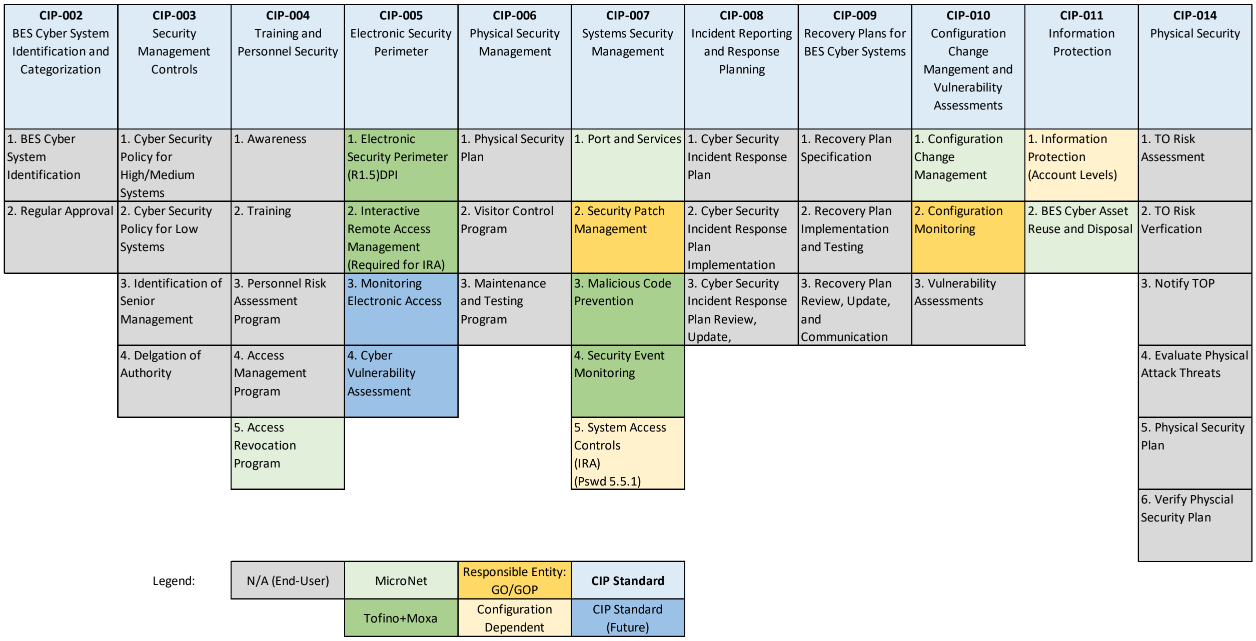
NERC's mission states that it is to "ensure that the bulk power system in North America is reliable." NERC has produced a set of directives for ensuring Critical Infrastructure Protection ("CIP"). A complete specification of NERC CIP requirements can be found by viewing the "Cyber Security" documents at the following URL: **www.nerc.com/pa/Stand/Pages/CIPStandards.aspx**.

This section lists all NERC-CIP v6 requirements standards.v6. Requirements applicable to the MicroNet Plus Cyber Secure solution have been annotated (in brown). The information describes how the Woodward solution contributes to compliance of the NERC CIP requirements.

NOTICE

The Woodward cyber security solution assumes the use of a MicroNet Plus or TMR CPU (part numbers noted above) and GAP application software (coder v6.0 or newer) with the recommended configurations. Older Non-Cyber Secure solutions do not provide sufficient security controls to meet the requirements of the NIST Cybersecurity Framework and NERC-CIP standards.

NIST Special Publication 800-53 (NIST SP 800-53) Security and Privacy Controls provides information for Information Systems and Organizations. Chapter 3 of NIST SP 800-53 catalogs security controls and provides guidance on their application. This reference also defines and classifies common security controls and appliances. Collectively, the typical Woodward solution with the security appliances and the recommended configurations meets the NERC-CIP v6 requirements as illustrated in Figure 9 1 NERC-CIP Coverage Matrix.



CIP-002 BES Cyber System Identification and Categorization	**CIP-003** Security Management Controls	**CIP-004** Training and Personnel Security	**CIP-005** Electronic Security Perimeter	**CIP-006** Physical Security Management	**CIP-007** Systems Security Management	**CIP-008** Incident Reporting and Response Planning	**CIP-009** Recovery Plans for BES Cyber Systems	**CIP-010** Configuration Change Mangement and Vulnerability Assessments	**CIP-011** Information Protection	**CIP-014** Physical Security
1. BES Cyber System Identification	1. Cyber Security Policy for High/Medium Systems	1. Awareness	1. Electronic Security Perimeter (R1.5)DPI	1. Physical Security Plan	1. Port and Services	1. Cyber Security Incident Response Plan	1. Recovery Plan Specification	1. Configuration Change Management	1. Information Protection (Account Levels)	1. TO Risk Assessment
2. Regular Approval	2. Cyber Security Policy for Low Systems	2. Training	2. Interactive Remote Access Management (Required for IRA)	2. Visitor Control Program	2. Security Patch Management	2. Cyber Security Incident Response Plan Implementation	2. Recovery Plan Implementation and Testing	2. Configuration Monitoring	2. BES Cyber Asset Reuse and Disposal	2. TO Risk Verfication
	3. Identification of Senior Management	3. Personnel Risk Assessment Program	3. Monitoring Electronic Access	3. Maintenance and Testing Program	3. Malicious Code Prevention	3. Cyber Security Incident Response Plan Review, Update,	3. Recovery Plan Review, Update, and Communication	3. Vulnerability Assessments		3. Notify TOP
	4. Delgation of Authority	4. Access Management Program	4. Cyber Vulnerability Assessment		4. Security Event Monitoring					4. Evaluate Physical Attack Threats
		5. Access Revocation Program			5. System Access Controls (IRA) (Pswd 5.5.1)					5. Physical Security Plan
										6. Verify Physcial Security Plan

Legend:				
	N/A (End-User)	MicroNet	Responsible Entity: GO/GOP	**CIP Standard**
		Tofino+Moxa	Configuration Dependent	CIP Standard (Future)

Figure 9-1. NERC-CIP Coverage Matrix

Note: The functional obligations of the Generator Owner (GO) and Generator Operator (GOP) entities include providing reliability operating services such as Frequency/Voltage Control, Generation/Load Balancing, and Monitoring/Control of circuit breakers. The standard term for these functions and behaviors is System Operating Limit (SOL). The responsibilities of these entities and the requirements of Control Centers are related to Woodward ITS and the Power Management/Distribution solutions. Requirements of the Transmission Owner and Balancing Authority are not applicable to the MicroNet Plus or TMR control system.

Note: The Woodward cyber security solution assumes that HMI security is addressed by others. For example, iFix Security Feature Configuration (v5.1 or newer is recommended) is outside the scope of this document. Rather, the scope includes the MicroNet Plus control platform (consisting of Woodward hardware and GAP application software, coder v6.0 or newer) and the associated OPC and service tool interfaces.

CIP-2 BES Cyber System Categorization (v5.1a)

Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

CIP-2.1 Critical Cyber Asset Identification and Categorization

Note: The CIP standard defines High/Medium/Low Impact classifications. The Impact Rating depends on both the characteristics of the generation system and the configured functionality of the MicroNet Plus control system. Subsequent NERC-CIP compliance requirements depend on the impact rating, for example, ERC, EAP, LERC, LEAP, and CIP-2 R1 Cyber Security Policy Review and Approval.

Note: The CIP standard defines functional responsibilities and allocates requirements. The following table extends these definitions to include Woodward control systems.

[1] (CIP-002-5.1a Cyber Security - BES Cyber System Categorization, Attachment 1, Impact Rating Criteria 2016)

[1] ((NERC), CIP-002-5.1a Cyber Security - BES Cyber System Categorization, Appendix 1, Section 4 Scope of Applicability 2016)

Table 9-1. Functional Responsibilities for Requirement Allocation to Entities

Woodward MicroNet	Functionality	CIP Reliability Service	CIP Entity
	Generator Protection	Dynamic Response	GOP, GO
	Bus Protection	Dynamic Response	GOP, GO
	Current/Frequency/Speed/Phase Protection	Dynamic Response	GOP, GO
	Spinning Reserve Generation	Dynamic Response	GOP, GO
	Governor/Load Control and Actuation	Dynamic Response	GO
	Under/Over Voltage/Frequency Protection	Dynamic Response	DP
Opt	Automatic Load Shedding	Dynamic Response	DP
	Power System Stabilizers	Dynamic Response	GO
	Non-Spinning Reserve Generation	Load Balancing and Generation	GOP, GO
Import/Export ZPT	AGC	Frequency/Real(kW) Power Control	GOP, GO
AVR	AVR	Voltage/Reactive(kVar) Power Control	GO
	Breaker/Switch Operation	Monitoring and Control	GOP
	Black Start	Restoration of BES	GOP
	Manual Load Shedding	Load Balancing and Generation	BA, DP

CIP-2.1.1 High Impact

The MicroNet Plus and TMR control, as a generation resource, qualify as High Impact critical cyber security assets. Auxiliary devices which communicate with the MicroNet Plus or TMR may or may not be considered critical cyber security assets. If MicroNet real-time functionality depends on inputs from other devices, then these devices should also be considered critical cyber security assets.

The MicroNet is designed as a High Impact Cyber Asset due to its use by the Control Center to manage IROLs and perform the functional obligations of the GO.[5] The customer, as the Reliability Coordinator, may specify the criticality of the MicroNet system as configured for the application.

Note: Remedial Action Schemes (previously Special Protection Systems) are N/A to Woodward automatic generator controls (AGC), AVR, and speed control.[6]

CIP-2.1.2 Medium Impact

If the customer, as the Reliability Coordinate, does not specify the criticality of the MicroNet Plus or TMR system as High Impact, CIP-002-5.1a-Attachment 1 Impact Rating Criteria[7] should be reviewed to determine if the system category is Medium Impact or Low Impact.

CIP-2.1.3 Low Impact

All Woodward components not meeting any of the High Impact or Medium Impact requirements above, are categorized as Low Impact.

2.2 Critical Cyber Asset Identification Management

2.2.1 Review Critical Cyber Assets List

[5] "(CIP-002-5.1a Cyber Security - BES Cyber System Categorization, Attachment 1: High Impact Rating (H) 1.3 (2.8, 2.10), 1.4 (2.6, 2.9), 2016)

[6] (Glossary of Terms Used in NERC Reliability Standards, 2018)

[7] "(CIP-002-5.1a Cyber Security - BES Cyber System Categorization, Attachment 1: High Impact Rating (H) 1.3 (2.8, 2.10), 1.4 (2.6, 2.9), 2016)

2.2.2 Approval of Critical Cyber Assets List

CIP-3 Security Management Controls (v7)

Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Woodward security controls include both proprietary and commercial-off-the-shelf appliances as well as software application development practices. The following information may be referenced for more details on a specific control or appliance. This section, NERC-CIP v6 Compliance, only provides details on controls as they relate to requirements. The artifacts in Table 1 1 Reference Documents, Manuals, and Information provide additional details on individual security controls and appliances, such as configuration and maintenance procedures.

CIP-3 R1 Cyber Security Policy Review and Approval

The MicroNet Plus and TMR controls are a critical cyber security asset and must be included in the Cyber Security Policy. Documentation requirements depend on the Impact Rating of the system controlled by the MicroNet Plus as defined by CIP-002-5.1a R1. The following sub-requirements may be used as a guide during reviews with senior management. The sections of this document provide information for consideration during the review and clarify requirements in terms of Impact.

CIP-3.1.1 High Impact and Medium Impact
CIP-3.1.1.1 Personnel and Training (CIP-004)
CIP-3.1.1.2 Electronic Security Perimeter (ESP) and Interactive Remote Access (CIP-005)
CIP-3.1.1.3 Physical Security (CIP-006)
CIP-3.1.1.4 System Security Management (CIP-007)
CIP-3.1.1.5 Incident Reporting and Response Planning (CIP-008)
CIP-3.1.1.6 Recovery Plans (CIP-009)
CIP-3.1.1.7 Configuration Change Management and Vulnerability Assessments (CIP-010)
CIP-3.1.1.8 Information Protection (CIP-011)
CIP-3.1.1.9 Exceptional Circumstances Declaration and Response
CIP-3.1.2 Low Impact
CIP-3.1.2.1 Cyber Security Awareness
CIP-3.1.2.2 Physical Security Controls
CIP-3.1.2.3 Electronic Access Controls
CIP-3.1.2.4 Cyber Security Incident Response
CIP-3.1.2.5 Malicious Code Risk Mitigation of Transient Cyber Assets and Removable Media
CIP-3.1.2.6 Exceptional Circumstances Declaration and Response

CIP-3.2 Cyber Security Plan for Low Impact Assets

Woodward provides additional reference materials which may be helpful per the required plan sections in CIP-003-7 Attachment 1. However, recommend including Low Impact assets in the High Impact or Medium Impact plans.

CIP-3.3 CIP Senior Manager

CIP-3.4 Delegated Responsibilities

CIP-4 Personnel and Training (v6)

Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

CIP-4 R1 Security Awareness Program

CIP-4 R1.1 Reinforce practices

CIP-4 R2 Cyber Security Training Program

CIP-4 R2.1 Training Content

CIP-4 R2.2 Training Records Prior to Authorization

CIP-4 R2.3 Renew Training

CIP-4 R3 Personnel Risk Assessment Program

CIP-4 R3.1 Identity Confirmation

CIP-4 R3.2 Background/History Record Check

CIP-4 R3.3 Background/History Record Check Criteria

CIP-4 R3.4 Contractor Background/History Record Check

CIP-4 R3.5 Renew Personnel Risk Assessment

CIP-4 R4 Access Management Program

The Administrator account is the only account which may view the list of accounts with access to the secure information of a MicroNet Plus or TMR control. There is only one Administrator account and its name is “Administrator”. The password to this account should be a carefully protected secret.

CIP-4 R4.1 Need-Based Authorization Policy and Process

Refer to the information and references listed in CIP-4 R4.2 Reconcile EACMS and PACS Authorized Accounts

CIP-4 R4.2 Reconcile EACMS and PACS Authorized Accounts

The complete list of authorized accounts of the MicroNet Plus and TMR control may be viewed and modified by an Administrator (Account Level 15) using the “Administer Accounts…” command (see section 3.9 Administrator Tools).

Figure 9 2 EACMS Architecture identifies access points and their associated user roles. A need-based justification for these user roles can be developed based on the functionality and privileges defined in Chapter 3.5 Account Levels. It is recommended that Table 3 2 Default Access Control Accounts and Passwords be updated and maintained to facilitate reconciliation.

CIP-4 R4.3 Review Necessary Authorized Accounts

Refer to the information and references listed in CIP-4 R4.2 Reconcile EACMS and PACS Authorized Accounts

Accounts may be deleted using the AppManager tool and performing “Administer Accounts” in the Control menu. There is no explicit feature for disabling an account.

CIP-4 R4.4 Review Necessary Information/Data Accounts

Refer to the information and references listed in CIP-4 R4.2 Reconcile EACMS and PACS Authorized Accounts

CIP-4 R5 Access Revocation

User Accounts may be managed, reset, or deleted using the Administrator account in the Administer Accounts window (see Chapter 3.8 Changing User Passwords and 3.9 Administrator Tools).

Refer to the information and references listed in CIP-4 R4.2 Reconcile EACMS and PACS Authorized Accounts

User Account changes typically take no longer than 30 seconds to become active for the Tofino Xenon.
Also see the reference information in
Woodward Manual < in CIP-4 Security Management Controls (v7).

CIP-4 R5.1 Process to Remove EACMS and PACS Access Abilities Upon Termination – High Impact and Medium Impact

CIP-4 R5.2 Revoke EACMS and PACS Account(s) Upon Reassignment/Transfer – High Impact and Medium Impact

CIP-4 R5.3Revoke EACMS and PACS Information Account(s) Upon Termination - High Impact and Medium Impact

CIP-4.4.5 Revoke EACMS Non-Shared Account(s) Upon Termination – High Impact

CIP-4.5.5 Change Password(s) for Shared EACMS Accounts Upon Termination/Reassignment/Transfer – High Impact

CIP-5 Electronic Security Perimeter (v5)

Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

A common MicroNet security architecture is illustrated in Figure 9 2 EACMS Architecture. Protected Cyber Assets (PCAs) are shown within the Electronic Security Perimeter (ESP) and Electronic Access Point (EAP) interfaces on the ESP are identified.

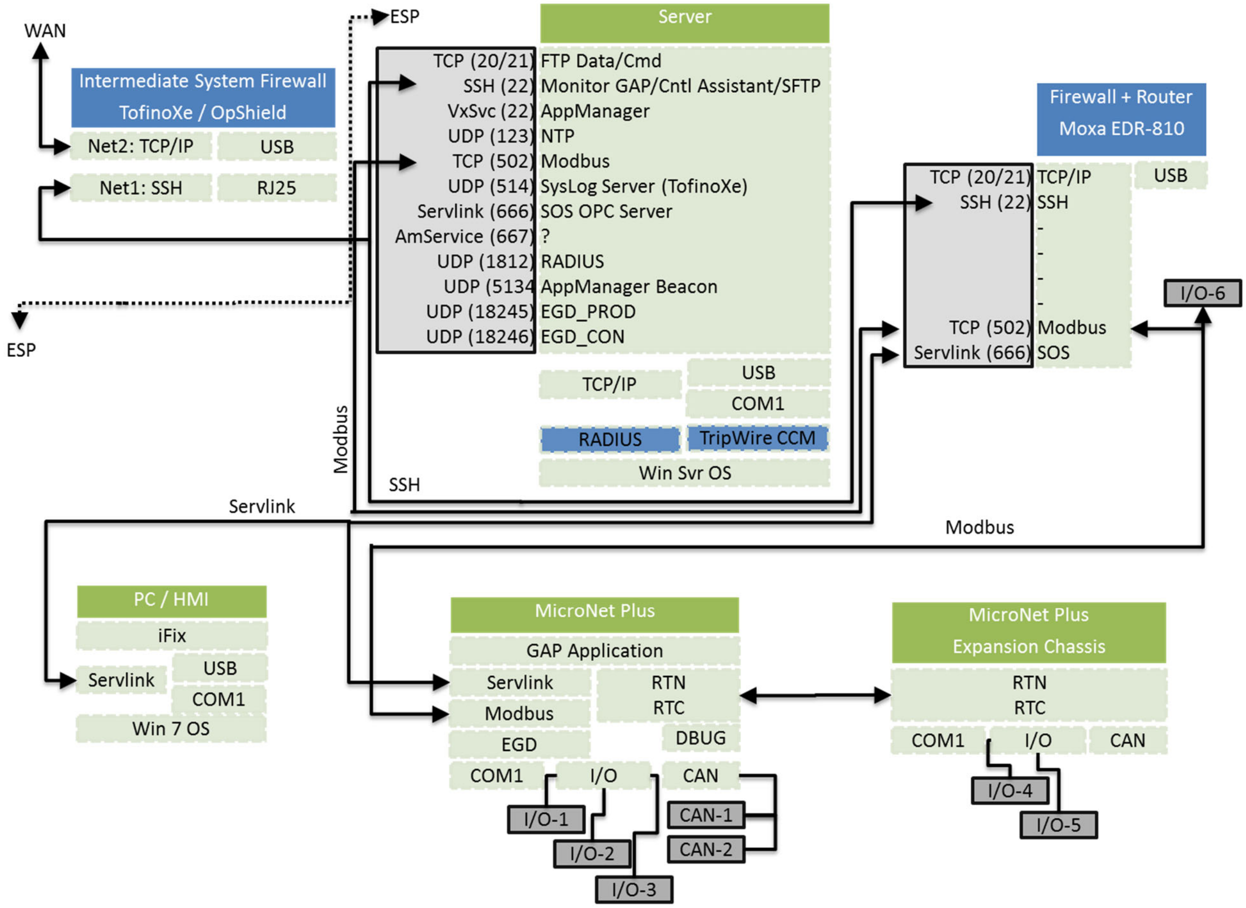


Figure 9-2. EACMS Architecture

Table 9-2. Port Map for Routable Protocols

Port	Protocol	Direction	CIP Class-ification	Associated Application	Associated Device /Appliance	Description
20	TCP	Both				FTP Data Channel
21	TCP	Both				FTP Command
22	SSH	Both		• OPC: SOS ServLink • Monitor GAP • Control Assistant • SFTP	HMI EDR-810 (WAN: 10.0.10.10, LAN: 10.0.100.100)	SSH Secure Shell (Authorized Access)
22	VxSvc	Both		• AppManager Help	MicroNet Plus (10.0.101.1)	SSH Secure Shell (Authorized Access)
123	UDP	In[8]				NTP
502	TCP	Both				Modbus TCP (EGD, Profibus, Fieldbus disabled?)
514	UDP	In		SysLog Server	Tofino Xenon	Event Log communications (configurable)
666	Servlink (TCP)	Both				SOS OPC
667	AmService (TCP)	Both				AmService
1812	UDP	Both		RADIUS	Windows Server (10.0.100.110)	Authentication, Authorization, Accounting (AAA) – Utilized for multi-factor authentication
5134	UDP	Out (multicast)[8]		• AppManager Help (Beacon)		
18245	EGD (UDP)	In				GAP Block Help – EGD_PROD (port configurable)
18246	EGD (UDP)	In				GAP Block Help – EGD_CON (port 18246 f/w cnst)

[8] Only bi-directional connections are classified as ERC per the NERC CIP definition.

CIP-5.1 Implement Electronic Security Perimeter documented processes for the following:

CIP-5.1.1 All networked PCAs connected via a routable protocol shall reside within a ESP – High Impact and Medium Impact

Figure 9 2 EACMS Architecture defines a typical ESP which contains all PCAs and devices of a Woodward control system.

CIP-5.1.2 Electronic Access Points shall be identified for all ERCs - High Impact and Medium Impact

The possible Electronic Access Points to a MicroNet Plus or TMR control platform are identified in Figure 9 2 EACMS Architecture and in Table 3 1 Access Points and SIEM Log Files. The associated network ports are also listed in Table 9 2 Port Map for Routable Protocols in the top-level section of CIP-4 Electronic Security Perimeter (v5).

The primary Access Points to MicroNet control assets include:

- OPC clients
- GAP application configurable network ports and protocols (example: Modbus, EGD)

Details of the functionality, justification, and security of these Access Points is provided in CIP-4 R1.3.

CIP-5.1.3 Justify access for Inbound and Outbound EAPs and deny all others by default – High Impact and Medium Impact

As discussed in CIP-4 R1.2, EAPs are primarily used by legitimate OPC clients and for specific GAP application functionality. A comprehensive list of Electronic Access Points to a MicroNet Plus Cyber Secure control platform are identified in Figure 9 2 EACMS Architecture and in Table 3 1 Access Points and SIEM Log Files. Several security controls are deployed to deny access by default. Boundary Controls and Network Security Controls for these Access Points, such as firewalls and router policies, are discussed in Chapter 4 Control Firewall. Specifically, the policies addressed in CIP-4 R1.3 and CIP-9 R1.1.4 are enforced by these network controls for the ports listed in Table 9 2 Port Map for Routable Protocols of section CIP-4 Electronic Security Perimeter (v5).

Authorized OPC Client connections utilize the SSH port of the MicroNet Plus Cyber Secure control and require submission of appropriate credentials as described in CIP-4 R1.2. No functionality is enabled until the credentials are verified. Data and services are only provided if the credentials match an account configured with a sufficient security level. Security Levels are defined in section 3.5 Account Levels and provide a hierarchy of functionality which can be used as a basis to manage and justify access for individual user accounts. Additionally, the --1511 and -1521 CPUs include a firewall which prevents all other ports from being accessed unless they are configured by the GAP application.

Securing OPC interfaces begins with the configuration of the GAP application as well as the SOS Servlink OPC Server. First, the GAP Programmer Block Help – Security describes how the GAP application configures the authority to access content and services via security levels. Second, the SOS Servlink OPC Server Help – Security Options describes how the recommended Enable OPC Security Interface setting can be used to require credentials for OPC client sessions. Once configured as recommended, tools such as Control Assistant and AppManager will be prompted and required to enter credentials. This is described further in Control Assistant Help – OPC Server Logon Dialog and AppManager Help – Secure Login. Also see Frequently Asked Questions: Why is the security level required for Stopping or Starting an application in AppManager not necessarily the same as the level required to Shutdown or Reset an application through an OPC client tool which uses SOS?

All SSH Secure Shell client connections require authorized credentials and file write access is verified by the MicroNet Password Manager. The primary asset associated with SSH port 22 is the OPC Server. Access to the OPC Server from any client, such as Woodward Control Assistant and Monitor GAP, passes through DCOM. Therefore, secure configurations should be made in both the SOS Servlink OPC program and on any host/personal computers (PC).

First, the credentials of the SOS Servlink OPC program should be configured as recommended in Chapter 3.4 Achieving a Secure Environment. These credentials are passed from the OPC program, through DCOM, and then verified by the MicroNet Plus controller. Second, it is important to configure DCOM remote connection on the host/personal computer and the SOS Servlink settings per the recommendations in Chapter 6 Configuring Your External PC, section 6.6 DCOM and OPC. These settings are independent of the Woodard security system.

It is common for the GAP application to require UDP communications, such as for Modbus and/or EGD protocols. If the application configures and opens such ports, they are not secured. As such, sensitive information and critical functionality should not be implemented through these services (see Chapter 4, Control Firewall). Woodward software application development practices also include a configuration check of the communication ports enabled by the GAP application as described in CIP-6 R1.2.

The controls and techniques described in CIP-6 R1.2 Protect unnecessary and unused ports and services can also be used as an additional layer of protection to deny access and protect EAPs.

CIP-5.1.4 Perform authentication for dial-up connectivity where feasible

The MicroNet Plus and TMR controls do not have a standard dial-up interface.

If using the optional Remote Access kit, please refer to the RemoteAccess manual for ensuring that the Electronic Security Perimeter remains secure.

CIP-5.1.5 Method(s) for detecting malicious communications

The following security control(s) provide mitigation and protection measures for malicious communications. Only Deep Packet Inspection (DPI) and unauthorized asset discovery controls are listed here. General firewall, encryption, and network controls are addressed in CIP-4 R1.3 and CIP-9 R1.1.4.

Table 9-3. Security Controls for Detecting Malicious Communications

Mitigation/Protection Benefit	Security Control
• Denial of Service (DoS) rate limit controls	Tofino Xenon 0200T1T1SDDZ90007-WG-KIT
• Deep Packet Inspection (DPI) – Modbus TCP	Tofino Xenon Enforcer LSM (Modbus)
• Deep Packet Inspection (DPI) – Modbus TCP	Moxa EDR-810

CIP-5.2 Remote Access Management

CIP-5.2.1 Use Intermediate Systems for all Interactive Remote Access - High Impact and Medium Impact

Intermediate Systems manage access control for Interactive Remote Access via routable encrypted protocols and are located outside the ESP. The intended functionality is like jump servers or secure administrative hosts which commonly use firewalls for boundary protection and device management across security zones. Figure 9 2 EACMS Architecture shows three (3) firewalls: The firewalls of the Tofino Xenon, Moxa EDR-810, and Embedded MicroNet. Each of the firewalls can be configured to provide network filtering based on protocol, port, and/or address. The Tofino Xenon is configured to only permit SSH protocol connections and is located outside the ESP, therefore, it functions as an Intermediate System. Additional details on OPC Clients and EAPs, to which Intermediate Systems connect, is provided in CIP-4 R1.2 and CIP-4 R1.3.

CIP-5.2.2 Encrypt Interactive Remote Access between Intermediate Systems and the EAP on the ESP

SSH is an encrypted protocol and is the only standard protocol used between Intermediate Systems and EAPs. The GAP application does permit configuration of communication ports with non-SSH protocols; however, this is not standard or recommended for cyber secure systems (also see CIP-6 R1.2 Protect unnecessary and unused ports and services and CIP-4 R1.3).

CIP-5.2.3 Use multi-factor authentication for all Interactive Remote Access

Enabling RADIUS in the Windows Server 2012R2 OS is available to meet multi-factor authentication requirements when combined with the authentication and access controls described in CIP-4 R1.3.

CIP-5.2.4 Methods for determining active vendor (Interactive) Remote Access sessions

This requirement is part of CIP-005 (v6) which is pending regulatory approval and currently not subject to enforcement. The MicroNet maintains a log file, PMLog.txt, which contains all successful (and unsuccessful) account logins. Additional information for this and the Log.txt file is provided in section 3.6 History.

CIP-5.2.5 Methods for disabling vendor (Interactive) Remote Access sessions

This requirement is part of CIP-005 (v6) which is pending regulatory approval and currently not subject to enforcement.

MicroNet remote access can be disabled either by physically isolating the control system from the network or by configuration of Woodward’s SOS Servlink OPC Server. The procedure for disabling SOS Servlink is provided in Chapter 6 Configuring Your External PC, section 6.6 DCOM and OPC.

Details of the functionality, justification, and security of Remote Access Points is provided in CIP-4 R1.3.

CIP-5.3 Monitoring Electronic Access

CIP-5.4 Cyber Vulnerability Assessment

CIP-6 Cyber Security - Physical Security of BES Cyber Systems

Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

CIP-6.1 Physical Security Plan

CIP-6.2 Visitor Control Program

CIP-6.3 Maintenance and Testing

CIP-7 Systems Security Management (v6)

Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

All authorized and unauthorized access attempts on MicroNet systems with secure passwords are logged to a tamper-proof file on the control. If too many unsuccessful attempts are made to connect to an account, access to that account will be temporarily disabled (see 3.5 Password Manager Configuration / Protections).

R5.1 Retention of electronic access logs
Login and account behavior history are stored in a tamper-proof folder on the MicroNet Plus or TMR CPU. These logs will fill and rollover over time (see 3.4 Password Manager Configuration / History / 3), so they should be copied to a safe location on a different computer.

CIP-7 R1Ports and Services Process Implementation and Documentation

CIP-7 R1.1 Only Enable Necessary physical I/O Ports and Services

Port Locks/Labels are available as an additional layer of physical protection for RJ45 and USB ports. Electronic and configurable protection is discussed in CIP-7 R1.2 Protect unnecessary and unused ports and services

CIP-7 R1.2 Protect unnecessary and unused ports and services

Only the SSH port and any application-defined ports are enabled on CPUs using SSH communications. The authority to access services may be mapped to different sets of credentials (see Chapter 3.5 Account Levels).

Woodward software application development practices include an automated configuration check of GAP applications. The purpose is to enumerate all configurable ports, services, and authorized security level settings. The following are among the tests and scans included.

- Auto-Configuration Analysis which performs a configuration check of the communication ports enabled by the GAP application. User Blocks (such as EGD_CON, EGD_PROD, and SIO_PORT) are identified and their configuration settings are evaluated against Woodward coding standards.

- Auto-Configuration Analysis which performs a configuration check of the security levels enabled by the GAP application. User Blocks are identified, and their configuration settings are evaluated against Woodward coding standards.
  - Also see GAP Programmer Block Help: SYS_INFO, SERVLINK, SIO_PORT, HMI_PT, HMI_ENUM, PASSWORD, QUICKCONF, QUICKSERV, Security, and SOS Servlink OPC Server

  Note: The SOS Servlink OPC Server permits client access to control registers. The authority to read/write and execute commands via OPC is configured and managed by the GAP application. The justification and security configuration of SOS Servlink is discussed in CIP-4 R1.3.

  Note: Configuring iFix security features is not considered within this document.

CIP-7 R2 Security Patch Management Implementation and Documentation

CIP-7 R2.1 Tracking, Evaluating, and Installing

Security patch/update management commonly utilizes Automated Continuous Diagnostics and Mitigation (CDM). The following paragraphs describe the update capabilities and procedures for the Woodward security controls.

The Tofino Xenon Enforcer LSM (Modbus) may require firmware updates. A customer account and License Activation Key is required to search for updates. Login to Tofino-Hirschmann Support and select the Software and Security Profiles to obtain updates.

Additional security appliances may be integrated in order to interface with known vulnerabilities managed by the National Vulnerability Database (NVD). These appliances typically utilize the NIST Security Content Automation Protocol (SCAP) protocol intended to meet NIST-IR-7511 and provide functionality which allows standardization and automation of security information communication between both humans and devices. The vulnerabilities listed in the log files of these additional appliances can be evaluated by the responsible entity to help identify potential patches and updates.

Also see Table 1 1 Reference Documents, Manuals, and Information for additional information on default policies and maintenance procedures for these security controls and devices.

CIP-7 R2.2 Evaluate applicable new security patches

See CIP-7 R2.1 Tracking, Evaluating, and Installing for information on identifying and accessing security updates.

CIP-7 R2.3 Apply Patches or document the mitigation plan

Available patches which are not automatically applied/installed and may be applicable should be considered by the responsible entity or CIP Senior Manager as part of the mitigation plan.

CIP-7 R2.4 Implement mitigation plans

CIP-7 R3 Malicious Code Prevention Implementation and Documentation

CIP-7 R3.1 Deploy security controls to deter, detect, or prevent malicious code

The MicroNet Plus and TMR permits authorized users to add files to the control and it is assumed that the control will not be used to store unnecessary files. Therefore, the risk of malicious files is considered low. The use of additional Configuration Management Monitoring Appliances can provide additional security for the GAP application executable file (.out, .hex, .dll) and the configuration file (.cfg).

The Woodward Secure Development Lifecycle (SDLC) is most closely aligned with Capability maturity Model Integration (CMMI) Level 3. Traceability is maintained between a requirements management and integrated product specification.
Integrated project management, organizational training on GAP development, employee/contractor background checks, and physical/logical security controls provide governance of coding standards and quality/test procedures. These measures are designed to help prevent the introduction of malicious code prior to the delivery.
File Checksums are generated for GAP application files and service tools can be used to verify the software integrity. Cyber Secure CPU systems also follow secure boot procedures and help prevent malicious code or compromised applications from executing after power-cycles.

CIP-7 R3.2 Mitigate malicious code threats

The security controls described in CIP-7 R2.1 generate logs for security events. These events serve as mitigation records. Specific security events are listed in CIP-7 R4 Security Event Monitoring. See Table 3 1 Access Points and SIEM Log Files for a listing of all log files.

CIP-7 R3.3 Updates for Malicious Code Security Controls

The security patch management information in CIP-7 R2 also applied to these updates.

CIP-7 R4 Security Event Monitoring

CIP-7 R4.1 Implement and document the process for monitoring security events

The MicroNet control produces log files of privileged access events. These log files should be downloaded and reviewed periodically to check for suspicious behavior. A complete list of SIEM log files is provided in Table 3 1 Access Points and SIEM Log Files.

The MicroNet control provides historical lists of activity for all accounts. Actions, dates and account names are stored. It is possible to collate these lists in order of individual accounts in order to ascertain individual account history. The events which are stored include (see section 3.6 History)

- Login / Logout
- Add Account, Remove Account, Change Password
- Start Application / Stop Application / Disable Autostart of Application / Reboot control
- Administer Module Service Pack
- Administer Control Service Pack
- Write or Delete file
- Change network configuration

The Tofino Xenon has a configurable cut-off level {0-7} which filters the recorded events by priority. Level 1 records only Emergency and Alert priority events while Level 7 will record all possible events. Level 2 events are considered Critical and indicate possible changes to the firewall operation. Level 2 events are also triggered when new configurations are loaded and can be used for CIP-9 R2 Configuration Monitoring.

CIP-7 R4.2 The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents
The policy rules of the Tofino Xenon are configurable as described in Configure Firewall Security of the Woodward Manual 35097 Belden Tofino Xenon Service Manual. This manual also provides information on the SIEM Log File Configuration and procedures for retrieving them.

Firewall and DPI events considered to be cyber security incidents include detection of unknown network IP addresses and traffic other than the ports, protocols, and directions specified in Table 9 2 Port Map for Routable Protocols. The standard configuration will trigger an alarm/alert on these conditions and record each event in the SIEM log file.

CIP-7 R4.3 Log File Retention
The MicroNet control produces log files of privileged access events.
R6.4 Logs shall be retained for 90 days

CIP-7 R4.4 Review Logged Events
The event logs in CIP-7 R4.1 and the alert logs in CIP-7 R4.2 are available for audits by the responsible entity.

CIP-7 R5 System Access Control
The following requirements are applicable to EACMS, PACS, and PCA

Refer to Table 3 1 Access Points and SIEM Log Files in Chapter 3 System Access for details on all Access Points.

CIP-7 R5.1 Process to Enforce Authentication
See CIP-4 R1.3 Justify access for Inbound and Outbound EAPs and deny all others by default – High Impact and Medium Impact and CIP-4 R2.3 Use multi-factor authentication for all Interactive Remote Access

Default Accounts
All default accounts and passwords are identified in Table 3 2 Default Access Control Accounts and Passwords in Chapter 3 System Access also contains important account management information for meeting the requirements of CIP-4 R4.2 Reconcile EACMS and PACS Authorized Accounts

CIP-7 R5.2 Identify Shared Accounts
Accounts may be shared by a group of users with a Fixed Password. Fixed Passwords are maintained exclusively by the Administrator.
Refer to the information and references listed in CIP-4 R4.2 Reconcile EACMS and PACS Authorized Accounts for a listing of shared accounts.
(Also see Chapter 3.9 Administrator Tools for additional information)

CIP-7 R5.3 Default Passwords

NOTICE

The owner/operator is responsible for changing all default passwords prior to operation. The MicroNet does not ship with unique pseudo-randomly generated passwords, however, all default accounts and passwords are identified in Chapter 3: Table 3-2 Default Access Control Accounts and Passwords in section 3.1 System Access Points. These Access Points are also shown in Figure 9-2 EACMS Architecture and the associated Descriptions and SIEM Log Files are listed in Chapter 3: Table 3-1 Access Points and SIEM Log Files.

The only protection for shared accounts is to keep the password secret from users who do not require it. If the password becomes too widely known, it is recommended that an Administrator change the password. Woodward also recommends changing all default passwords because some accounts may be configured to have a high level of authority and the default passwords are public information.

Refer to the information and references listed in CIP-4 R4.2 Reconcile EACMS and PACS Authorized Accounts

CIP-7 R5.4 Interactive User Access with Password-Only Authentication

- The AppManager tool and the MicroNet control enforce a length restriction for all passwords of between 8 and 30 characters (inclusive).
- The AppManager tool and the MicroNet control enforce a rule that each password contain at least 2 alpha and 2 non-alpha (numeric and/or "special") characters
  (see Chapter 3.3 Password Manager Default Settings and 3.8 Changing User Passwords)

CIP-7 R5.5 Renew Interactive User Access with Password-Only Authentication

The AppManager tool may be used to set the expiration period applied to passwords. (Also see Chapter 3.9 Administrator Tools for additional information)

The Administrator may configure an account password to expire. If this account is given a "Fixed Password", it is the responsibility of the Administrator to change the password when it has expired. If the account does not have a fixed password, the user who logs in with that account will be prompted to enter a new password upon expiration of the old one (see Chapter 3.8 Changing User Passwords).

CIP-7 R5.6 Unsuccessful Authentication Attempts

The AppManager tool may be used to set the limit for unsuccessful login attempts. (Also see Chapter 3.7 Protections for additional information)

CIP-8 Incident Reporting and Response Planning (v5)

Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

CIP-8 R1 Incident Response Plan

CIP-8 R1.1 Identification, Classification, and Response

Woodward suggests resetting all compromised accounts on a MicroNet Plus or TMR control when there is a security event. Reset user accounts are assigned default passwords (see Table 3 2 Default Access Control Accounts and Passwords) which should then be changed to enable security by the Administrator and/or the account holders. Any fixed accounts whose passwords are compromised should manually have their passwords changed.

8.1.2 ES-ISAC Notification Process

8.1.3 Incident Response Roles and Responsibilities

8.1.4 Incident Response Containment, Eradication, Recovery, and Resolution

This document may be consulted for elements of incident response.

CIP-8 R2 Incident Response Implementation and Testing

CIP-8 R2.1 Testing Frequency

CIP-8 R2.2 Document Test Results

CIP-8 R2.3 Reportable Incident Record Retention

The documentation should include a copy of all log files from the MicroNet control. These may be retrieved with the "Retrieve System Log Files" command of the AppManager program (see Chapter 3.6 History).

CIP-8 R3 Incident Response Plan Review and Maintenance

CIP-8 R3.1 Lessons Learned

CIP-8 R3.1.1 Document Lessons Learned

CIP-8 R3.1.2 Update the Response Plan

CIP-8 R3.1.3 Update Notifications

CIP-8 R3.2 Changes to Roles, Responsibilities, or Technology

CIP-8 R3.2.1 Update the Response Plan

CIP-8 R3.2.2 Update Notifications

CIP-9 Recovery Plans (v6)

Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

CIP-9 R1 Recovery Plan Specifications

CIP-9 R1.1 Activation Criteria

CIP-9 R1.2 Roles and Responsibilities

CIP-9 R1.3 Recovery Resources - Backup and Storage

This document may be consulted for elements of disaster recovery Woodward suggests resetting all compromised accounts on a MicroNet control when there is a security event. Reset user accounts are assigned default passwords (see Table 3 2 Default Access Control Accounts and Passwords) which should then be changed to enable security by the Administrator and/or the account holders. Any fixed accounts whose passwords are compromised should manually have their passwords changed.

> **Note:** the process and procedures of CIP-9 R1.5 Preserve Diagnostic Data should be performed prior to resetting all compromised accounts.

CIP-9 R1.4 Backup Verification Process

Woodward does not supply facilities for transferring security configurations to a MicroNet control. As such, the backup and restore facilities will solely be comprised of written instructions. For security purposes, it is not recommended to make this information complete.

CIP-9 R1.5 Preserve Diagnostic Data

See CIP-7 R2.3 Reportable Incident Record Retention

CIP-9 R2 Recovery Implementation and Testing

CIP-9 R2.1 Testing Frequency

CIP-9 R2.2 Recovery Resource Sample Test

CIP-9 R2.3 High-Impact Operational Test

CIP-9 R3 Review Recovery Plan

CIP-9 R3.1 Lessons Learned

CIP-9 R3.1.1 Document Lessons Learned

CIP-9 R3.1.2 Update the Recovery Plan

CIP-9 R3.1.3 Update Notifications

CIP-9 R3.2 Changes to Roles, Responsibilities, or Technology

CIP-9 R3.2.1 Update the Recovery Plan

CIP-9 R3.2.2 Update Notifications

CIP-10 Configuration Change Management and Vulnerability (v2)

Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

CIP-10 R1 Configuration Change Management

CIP-10 R1.1 Baseline Configuration

CIP-10 R1.1.1 OS and Firmware Versions

See Table 7 1 Baseline Configuration Versions for a list of current versions by type.

CIP-10 R1.1.2 Commercial and Open-Source Application Versions

CIP-10 R1.1.3 Custom Application Versions

Note: the GAP application configures the security level associated with user accounts. The defaults are listed in Table 3 2 Default Access Control Accounts and Passwords and described in Chapter 3.5 Account Levels. Application configuration management (CM) is important to ensure appropriate security levels for the configurable user accounts. For example, the Datalog account primarily has the authority to read files, but, if the GAP application is configured with weak security, the Datalog account can be granted a high level of authority in the GAP application. Woodward software application development practices include a configuration check of the security levels enabled by the GAP application as described in CIP-7 R1.2.

See Table 7 1 Baseline Configuration Versions for a list of current versions by type.

CIP-10 R1.1.4 Logical Network Accessible Ports

Standard network ports are listed in Table 9 2 Port Map for Routable Protocols for the typical system illustrated in Figure 9 2 EACMS Architecture.

CIP-10 R1.1.5 Security Patches

See CIP-7 R2 Security Patch Management Implementation and Documentation

CIP-10 R1.2 Authorize and Document Deviations from Baseline

Configuration Change Management is closely related to the event logs in CIP-7 R4.1 and the associated alerts in CIP-7 R4.2. The following SIEM resources are available for configuration audits by the responsible entity:

CIP-10 R1.2.1 Log files listed in Table 3 1 Access Points and SIEM Log Files may also record configuration change events. For example, the MicroNet control records network configuration changes in the Log.txt file.

CIP-10 R1.3 Baseline Updates

CIP-10 R1.4 Baseline Update Procedure

CIP-9 R1.4.1 Prior to Update, Review Impact on CIP-4 Electronic Security Perimeter andCIP-7 Systems Security Management

Note: The addition of new devices, security controls/appliances or any configuration change will likely impact other security components. For new devices or services, consider possible impacts to Figure 9 2 EACMS Architecture and Table 9 2 Port Map for Routable Protocols. It may also be necessary to update policies and configuration management monitoring appliances

For new services and communication ports, consider changes to the Tofino Xenon firewall policies.

The Woodward Tofino manual lists sources for additional information on implementing necessary changes. For changes to user accounts, consider performing the procedures listed in CIP-4 R4.2 Reconcile EACMS and PACS Authorized Accounts.

CIP-10 R1.4.2 Following Update, Verify No Impact

CIP-10 R1.4.3 Document Update Verification Results

CIP-10 R1.5 Testing High-Impact PCA Updates

CIP-10 R1.5.1 Test Environment

N/A for Woodard

CIP-10 R1.5.2 Test Results

N/A for Woodard

CIP-10 R2 Configuration Monitoring

CIP-10 R2.1 Baseline Changes

The MicroNet controller records network configuration changes in the Log.txt file.

Additional Configuration Management Monitoring Appliances are available to continuously monitor for changes of the devices and firmware listed in CIP-10 R1.1 Baseline Configuration. These additional appliances are designed to identify changes and trigger an alert/alarm which is recorded in an event log and/or annunciated.

The event logs in CIP-7 R4.1 and the alert logs in CIP-7 R4.2 are available for audits by the responsible entity.

10.3 Vulnerability Assessment

10.3.1Review Frequency

During vulnerability assessment reviews, the following information is available for audits by the responsible entity:

- Event logs in CIP-7 R4.1
- Alert logs in CIP-7 R4.2
- Information in CIP-7 R2 Security Patch Management Implementation and Documentation may be reviewed and compared to the configuration baseline and software versions listed in CIP-10 R1 Configuration Change Management

10.3.2 Test Frequency

10.3.2.1 Active Test

10.3.2.2 Document Test Environment and Results

10.3.3 New PCA Vulnerability Assessment

10.3.4 Vulnerability Mitigation Plan

10.4 Transient Cyber Assets and Removable Media

The Tofino Xenon configuration disables the USB port by default. (see the “Network Only” Communications settings on the General page as discussed in the Tofino Xenon Configurator User Manual)

> **Note:** With the USB port disabled, the Tofino Xenon log files can only be retrieved via the Tofino Configurator in Table 3 1 Access Points and SIEM Log Files or via a remote syslog server.

CIP-11 Information Protection (v2)

Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

CIP-11 R1 Information Protection

CIP-11 R1.1 Classification Method for BES Cyber System Information

Access to control information through the Woodward AppManager and SOS Servlink tools are governed by security levels. Chapter 3.5 Account Levels defines levels for information access and privileges such as read/write/delete and view/set. Classification methods can be customized using a range of security levels (0-15).

CIP-11 R1.2 Handling Procedures

The security levels described in CIP-10 R1.1 Classification Method for BES Cyber System Information also determine how information is handled through the Woodward AppManager and SOS Servlink tools.

CIP-11 R2 Reuse and Disposal

CIP-11 R2.1 Prevent Unauthorized Retrieval Prior to Reuse

Woodward recommends deleting the accounts of a redeployed MicroNet Plus Cyber Secure control. The security logs cannot be tampered with, so they will continue to show history from the previous deployment. It may be appropriate to record the state of the log files before redeployment, so that the history of the different deployments may be differentiated.

CIP-11 R2.2 Prevent Unauthorized Retrieval Prior to Disposal

Woodward recommends deleting the accounts of a MicroNet Plus or TMR control system prior to disposal. The security logs cannot be tampered with; however, this is a cyber security best practice.

CIP-13 Supply Chain Security

Woodward flows down our security requirements to identified critical suppliers via procedure 03-OF-03777. Please contact your Woodward representative if you have questions regarding supplier flowdown on a specific Woodward product.

CIP-14 Physical Security

Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.

CIP-14 R1 Transmission Owner Risk Assessments

CIP-14 R1.1 Risk Assessment Frequency

CIP-14 R1.2 Identify Primary Control Center

CIP-14 R2 Transmission Owner Risk Assessment Verification

CIP-14.2.1 Select Unaffiliated Entity

CIP-14 R2.2 Perform and Complete Verification

CIP-14 R2.3 Address Recommendations

CIP-14 R2.4 Procedures for Information Protection

CIP-14 R3 Notify Transmission Operator(s)

CIP-14 R4 Evaluate Potential Physical Attack Threats and Vulnerabilities

CIP-14 R4.1 Unique Characteristics

CIP-14 R4.2 Prior History of Attack

CIP-14 R4.3 Intelligence or Threat Warnings

CIP-14 R5 Physical Security Plan

CIP-14 R5.1 Resiliency or Security Control Measures

CIP-14 R5.2 Law Enforcement Coordination Information

CIP-14 R5.3 Execution Timeline

CIP-14 R5.4 Evaluate Evolving Physical Threats

CIP-14 R6 Physical Security Plan Verification

CIP-14 R6.1 Select Unaffiliated Entity

CIP-14 R6.2 Perform and Complete Verification

CIP-14 R6.3 Address Recommendations

CIP-14 R6.4 Procedures for Information Protection

Chapter 10
Frequently Asked Questions

Are there default accounts present?

- At installation, the MicroNet control contains three default accounts (see 3.1 Password Manager Configuration / Using Default Settings). These are:
  - Administrator
  - ServiceUser
  - Datalog

Are individual user accounts supported?

- The MicroNet control allows up to 50 security accounts. These may be either shared or individual. It is up to the Administrator to configure the collection of accounts and to pick appropriate names and account configurations.

Is the MicroNet control capable of strong password complexity requirements?

- The password complexity requirements are fixed:
  - Length between 6 and 30 (inclusive)
  - At least 2 alpha characters (A-Z, a-z)
  - At least 2 non-alpha characters (0-9, !@#...) o These requirements are consistent with the requirements of NERC CIP-007 5.3.

Vendor's current version (firmware, client software, etc)

- Please consult Chapter 7 (Current Versions).

What are the mechanisms (URLs, email lists, or individual names if need be) through which security patches are announced and distributed?

- Woodward maintains a list of customers who have purchased controls or downloaded software. Through the Woodward Service Bulletin distribution procedure, customers are notified of patches and how and why to implement them.

What is the status of vendor support (supported, end of sale, end of life, etc.)?

- Supported

Is the ISA99 standard followed?

- Woodward's MicroNet control was not designed to meet the ISA99 standards for security except to the extent that its requirements are aligned with the requirements of NERC CIP.

Is AV (anti-virus) supported?

- Anti-virus software is not supported on the MicroNet control. Real-time performance of the controller could be compromised by anti-virus activity. However, it is very unlikely that a virus could infect a MicroNet Control, because the only applications which a user runs on a MicroNet system are control applications generated by Woodward software. Furthermore, customers are discouraged from storing any files unrelated to control requirements on the MicroNet Plus or TMR control.

If yes, is Kaspersky supported (or other manufacturer)?

- No. See the "Is AV (anti-virus) supported" question

Which MicroNet CPUs are SSH capable?

- The SSH port is enabled on the 5466-1045, 5466-1145, 5466-1510 and 5466-1520 CPUs. However, all access to privileged functionality (e.g. file writes) is controlled through the Password Manager which runs on the control. An SSH client tool would need to present appropriate credentials for authorization to perform any privileged operations through SSH.

Is the MicroNet control SFTP capable?

- The SFTP port is enabled on the MicroNet control. However, all access to privileged functionality (e.g. file writes) is controlled through the Password Manager which runs on the control. An SFTP client tool would need to present appropriate credentials for authorization to perform any privileged operations through SFTP.

Is the MicroNet Plus or TMR control Telnet capable?

- No. Telnet has been disabled for security reasons.

Is the MicroNet control FTP capable?

- No, FTP has been disabled on the MicroNet Plus Cyber Secure control for security reasons. Instead, the MicroNet supports the Secure FTP protocol (SFTP).

Are other remote management protocols supported?

- No, other remote management protocols have been disabled on the MicroNet control for security reasons.

Can the device be managed locally (via serial port)?

- Yes for 5200 CPUs it is possible to configure use of a serial port in the GAP application. Serial ports may be configured to access SOS Servlink or other HMI-related software. It is also possible to access the control's operating system through the Vx-Works debug port, given enough credentials (as defined in the Password Manager). The P1020 CPUs do not contain serial ports.

Does the MicroNet control support DNS configuration?

- No. MicroNet Plus controls may be assigned a human-friendly name for display in the AppManager and SOS Servlink tools, but generic access to the control must be through the IP Address or through the OPC protocol (which uses the human-friendly name).

Does the MicroNet Plus control support NTP configuration?

- MicroNet controls implement the Simple Network Time Protocol ("SNTP"). If there is an SNTP time server on the network, the MicroNet Plus control can be synchronized to it (look up "SNTP" in the AppManager tool's help document).

Does the MicroNet control support SYSLOG configuration?

- Not currently. The MicroNet Plus control logs follow an ASCII protocol.

Is OPC-UA (Unified Architecture) supported by SOS Servlink?

- No, only OPC-DA (Data Access) and OPC-A&E (Alarms & Events) are supported.

What kind of OPC data is provided by SOS Servlink?

- Woodward supports OPC DA (Data Access) 3.0 and A&E (Alarms and Events) 1.0. The Alarms and Events server only produces simple events without server-specific attributes or server-side event filtering. Woodward's OPC interface has not been certified, but it has been run with many different off-the-shelf client OPC applications.

Why is the security level required for Stopping or Starting an application in AppManager not necessarily the same as the level required to Shutdown or Reset an application through an OPC client tool which uses SOS Servlink?

- The security levels used to control AppManager ("Vx-Service") functionality like Stop and Start are required to be available whether or not an application is running on the control. These values are fixed.
- The application can set the SOS Servlink security levels in the SYS_INFO block (consult "Block Help" in the GAP Editor program). These security levels, as defined in the running application, may be different from the fixed AppManager levels (see Chapter 3.3 Password Manager Default Settings and 3.5 Account Levels).

How do I clear login credentials from an AppManager session when I am done if I want to prevent someone else from using my credentials?

- AppManager caches login credentials for any control for up to 24 hours (configurable in the Options dialog of AppManager –Duration of login cache). This is for convenience. To remove these credentials:
    - Select Logout from the Control menu. This command is only available if a session is active in the control.
    - Select Log Off from the Administer menu. This command clears the login credentials for all controls AppManager has connected toOr close the AppManager tool.

Why does the Datalog Retrieval Tool functionality not work?

- One possibility is that the security credentials configured in the Options dialog of AppManager do not match the security configuration on a control. AppManager only allows one set of credentials to be specified, and it must be usable by all controls which AppManager collects datalog files from.
- Check the datalog events window or the datalog events file of the AppManager tool for more information about what may be wrong (see AppManager help).

How can I use the Datalog Retrieval Tool functionality in AppManager without storing login credentials on the PC?

- This is not possible. Datalog functionality requires credentials to communicate with MicroNet Plus Cyber Secure controls. It is suggested to use an account with low authority for this purpose (e.g. the default “Datalog” account). The account must have an authority level of at least “1” in order to read files. The password is cached in an encrypted form in the registry, so it is not possible to re-use this information to gain access to the control for another purpose.

Why are some of the menu commands in AppManager disabled?

- Menu or toolbar commands in AppManager may be disabled for one of two reasons:
    - The command is not appropriate for the context. For example, many of the commands in the Control menu require that a control be selected and connected in the left window of AppManager.
    - The logged-in user has insufficient credentials for the command. To see the level of the current AppManager session, select Display Account Information… from the Control menu. The level shown by this command may be compared to the security levels required for various commands (see Chapter 3.3 Password Manager Default Settings and 3.5 Account Levels).

Chapter 11.
Product Support and Service Options

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 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 needs 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 5-01-1205 North American Terms and Conditions of Sale (Industrial Business Segment).

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 most 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 5-01-1205 North American Terms and Conditions of Sale (Industrial Business Segment) 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 5-01-1205 North American Terms and Conditions of Sale (Industrial Business Segment). 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.

For instructions about sending your MicroNet control to Woodward for repairs, please consult your product manual. It is suggested that you change the password of the Administrator account to the default value (“Admin@1”) before sending it to Woodward. This will make it possible for Woodward to make appropriate changes to your control without removing your account configuration.

If you do not provide Administrator account credentials to Woodward for performing the work, Woodward will return the Password Manager configuration to the default configuration (see 3.1 Password Manager Configuration / Using Default Settings). It will be your responsibility to reconfigure the accounts to a secure and appropriate configuration. 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, 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) 8818 5515
Germany:	+49 (711) 78954-510
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+82 (32) 422-5551
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) 8818 5515
Germany	+49 (711) 78954-510
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+ 82 (32) 422-5551
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) 8818 5515
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+ 82 (32) 422-5551
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.

Glossary

Acronym/Term	Definition/Description
BES	**Bulk Electric System**
CSC	**Critical Security Controls**
DFARS	**Defense Federal Acquisition Regulation Supplement**
EACMS	**Electronic Access Control or Monitoring System**: firewalls, authentication servers, log monitoring, alerting/alarming systems
EAP	**Electronic Access Point**: a Cyber Asset interface that allows routable communications across the ESP
ERC	**External Routable Connectivity**: remote access to a Cyber Asset from outside the ESP via a bi-directional protocol
ESP	**Electronic Security Perimeter**: The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.
GO	**Generator Owner**
GOP	**Generator Operator**
IRA	**Interactive Remote Access**: User-initiated access via a remote client using a routable protocol and originates from a Cyber Asset outside the ESP
IS	**Intermediate System**: One or more Cyber Assets outside the ESP performing access control for Interactive Remote Access which utilizes data encryption to/from the EAP
PACS	**Physical Access Control System**: applicable to External Routable Connectivity
PCA	**Protected Cyber Asset**: programmable electronic device including hardware, software, and data
PSP	Physical Security Perimeter
SIEM	**Security Information and Event Management**
UFLS	**Under Frequency Load Shedding**
UVLS	**Under Voltage Load Shedding**
VRF	**Violation Risk Factor**
Achilles	GE Digital's **Achilles** Communication Certification (ACC)tests the control for robustness and cyber security for attack vectors utilizing Ethernet communications ports. Specific CPUs have been certified to the Achilles standards as indicated in Chapter 7
Administrator	**Administrator** is the most privileged account on the MicroNet Plus Cyber Secure control. There may be only one Administrator account, and its name is "Administrator". Its password is known and may be managed only by the people given the role of Administrator.
AppManager	Woodward's **AppManager** program is the user interface for managing applications and configuring security accounts on the control.
CIP	The **Critical Infrastructure Protection** program (CIP) coordinates all of NERC's efforts to improve physical and cyber security for the bulk power system of North America as it relates to reliability. These efforts include standards development, compliance enforcement, assessments of risk and preparedness, disseminating critical information via alerts to industry, and raising awareness of key issues. Additionally, the program monitors the bulk power system to provide real-time situation awareness leadership and coordination services to the electric industry.
Control Assistant	Woodward's **Control Assistant** is a tool for service access to a control. It may be used to view and modify control parameters, graphically view data trends and stored data log files.

Acronym/Term	Definition/Description
Cyber Security	**Cyber Security** is the practice of protecting read and write access to privileged control information and functionality by limiting access to authorized users.
DCOM	**Distributed Component Object Module** (DCOM) is a proprietary Microsoft® technology for communication among software components distributed across networked computers. Woodward uses DCOM to implement OPC, which the SOS Servlink OPC Server uses to communicate control values to networked PC applications.
EGD	The **Ethernet Global Data** protocol (EGD) was created by General Electric to exchange data between the GE Fanuc control and one or more consumer devices.
Fieldbus	**Field bus** (Fieldbus) is the name of a family of industrial computer network protocols used for real-time distributed control, now standardized as **IEC 61158**.
GAP	Woodward's **Graphical Application Programmer** is the software program used to build software applications for the MicroNet Plus control.
HMI	A **Human Machine Interface** (HMI) is a software or hardware system that enables the interaction of man and machine.
ISA99	The purpose of **ISA99** is to improve the confidentiality, integrity, and availability of components or systems used for industrial automation and control and provide criteria for procuring and implementing secure control systems. Compliance with ISA99 will improve system electronic security, and will help identify vulnerabilities and address them, thereby reducing the risk of compromising confidential information or causing degradation or failure of the equipment or process under control. For more information concerning ISA99 consult the following web page: **http://isa99.isa.org/default.aspx**.
Modbus	**Modbus** is a communications protocol designed by Modicon Incorporated for use with its PLCs. It is widely supported by many vendors, including Woodward.
Monitor GAP	Woodward's **Monitor GAP** is a tool within the GAP program for viewing live control values in the context of the application program.
NERC	**North American Electric Reliability Corporation**. NERC's major responsibilities include working to develop standards for power system operation, monitoring and enforcing compliance with those standards, assessing resource adequacy, and providing educational and training resources as part of an accreditation program to ensure power system operators remain qualified and proficient.
OPC	**Object linking and embedding for Process Control** (OPC) is a standard that specifies the communication of real-time plant data between control devices from different manufacturers. Woodward's SOS Servlink OPC Server tool uses OPC to communicate control data to PC software tools like HMIs, Monitor GAP and Control Assistant.
OPC A&E	**OPC Alarms & Events:** Standards created by the OPC Foundation for alarm monitoring and acknowledgement.
OPC DA	**OPC Data Access:** Standards created by the OPC Foundation for accessing real time data from data acquisition devices such as the SOS OPC server.
OPC UA	**OPC Unified Architecture:** Standards created by the OPC Foundation for integrating the existing OPC standards. OPC UA does not require Microsoft technology, as OPC DA does, but is not available from Woodward.
PLC	A **Programmable Logic Controller** (PLC) is a dedicated computer used for controlling industrial machinery and processes.

Acronym/Term	Definition/Description
PROFIBUS	**Process Field Bus** (PROFIBUS) is a standard for field bus communication in automation technology and was first promoted (1989) by BMBF (German department of education and research).
RTN	The **Real Time Network** (RTN) is a network of Woodward expansion chassis which communicate and remain time-synchronized with the main CPU. Expansion chassis on the RTN may not be connected to another network but can be managed indirectly through the main CPU by the AppManager tool.
SIL	**Safety Integrity Level** (SIL) is defined as a relative level of risk reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a Safety Instrumented Function (SIF).
SNTP	**Simple Network Time Protocol** is a protocol for synchronizing the clocks of computer systems on the same network.
SSH	**Secure Shell** (SSH) is a network protocol that allows data to be exchanged using a secure channel between two networked devices. SSH uses encryption to provide confidentiality and integrity of data over an unsecured network, such as the Internet.
SOS	The **SOS Servlink OPC Server** (SOS) is a Woodward program that uses OPC to communicate control data to PC software tools which implement the OPC protocol. OPC-based HMI tools and Woodward's Monitor GAP and Control Assistant programs are such tools.

Revision History

Changes in Revision C—

- Added MicroNet™ TMR to the manual
- Added content to the first two paragraphs in Chapter 1
- Added MicroNet™ TMR to Tables 1-1 and 1-2
- Added Woodward DID Recommendations to Chapter 2
- Edited headings in Table 3-2
- Edited heading in paragraph 5 in Section 3.5
- Edited heading in paragraph 1 in Section 3.6
- Edited first paragraph in Section 3.7
- Edited first paragraph in Chapter 4
- Added first bullet and edited second bullet in Section 5.1
- Edited Sections 6.1, 6.2, 6.4, and 6.7
- Multiple edits in Table 7-1
- Edited Section 8.2
- Edited Notice Box in Chapter 9
- Edited Table 9-1 and added TMR references within Chapter 9
- Added CIP-13 Supply Chain Security to Chapter 9

Changes in Revision B —

- Updated NERC CIP Compliance to v6
- Added related documents for new cyber security appliances MOXA EDR-810 and Tofino Xenon
- Moved Chapter 2 Definitions and Abbreviations to the Glossary and appended new entries
- Added Chapter 2 Defense-in-Depth (DiD)
- Expanded Chapter 3 to the broader subject of System Access and added
    - Table 3 1 Access Points and SIEM Log Files
    - Table 3 2 Default Access Control Accounts and Passwords
- Added new security appliances to Chapter 7 Current Versions
- Added NIST NVD to section 8.3 Notifications
- Moved Chapter 8.4 Warranty Repair to new Chapter 11 Product Support and Service Options
- Revised CIP-2 to reflect new NERC CIP categorizations by impact rating
- Added Revision History
- Added References

References

(NERC), N. A. (2016, 12 14). *CIP-002-5.1a Cyber Security - BES Cyber System Categorization, Appendix 1, Section 4 Scope of Applicability.* Retrieved from (CIP) Critical Infrastructure Protection - Subject to Enforcement: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

(NERC), N. A. (2016, 12 14). *CIP-002-5.1a Cyber Security - BES Cyber System Categorization,* Attachment 1, Impact Rating Criteria. Retrieved from (CIP) Critical Infrastructure Protection - Subject to Enforcement: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

(NERC), N. A. (2016, 12 14). *CIP-002-5.1a Cyber Security - BES Cyber System Categorization, Attachment 1: High Impact Rating (H) 1.3 (2.8, 2.10), 1.4 (2.6, 2.9).* Retrieved from (CIP) Critical Infrastructure Protection - Subject to Enforcement: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

(NERC), N. A. (2018, 1 31). *Glossary of Terms Used in NERC Reliability Standards*. Retrieved from NERC Glossary of Terms: http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

This Page Intentionally Left Blank

This Page Intentionally Left Blank

This Page Intentionally Left Blank

We appreciate your comments about the content of our publications.

Send comments to: icinfo@woodward.com

Please reference publication 26479.

B 2 6 4 7 9 : C

WOODWARD™

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.