WOODWARD

Product Manual 35219 V4
(Revision -, 11/2024)
Original Instructions

MicroNet XT
Security Manual

Manual 35219 consists of four volumes:
(35219 V1, 35219 V2, 35219 V3, & 35219 V4)

Optional Supplementary Information

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. The latest version of most publications is available on the Woodward website.

http://www.woodward.com

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. The latest version of most publications is available on the Woodward website.

Woodward Industrial Support: Get Help

Always compare with the original for technical specifications and for proper and safe installation and operation procedures.

If your publication is not on the Woodward website, please contact your customer service representative to get the latest copy.

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

Manual 35219 V4

Contents

This manual is divided into four volumes:

- Volume 1 contains mostly hardware information (manual 35219V1)
- Volume 2 is reserved for future use (manual 35219V2)
- Volume 3 contains information about the MicroNet XT software (manual 35219V3)
- Volume 4 contains cyber security information (manual 35219V4)

CHAPTER 1. GENERAL INFORMATION 5
Purpose 5
Scope 5
References 5
Glossary 5

CHAPTER 2. INDUSTRIAL CYBERSECURITY BASICS 7
Introduction 7

CHAPTER 3. DEFENSE IN DEPTH (DID) 10
Introduction 10
Physical Security 10
Policies and Procedures 11
Zones and Conduits 11
Malware Prevention 12
Access Controls 12
Monitoring and Detection 12
Patching 13
Additional MicroNet XT Security Features 13
Attack Scenarios 14
Security References 15
User Account Management 15
Accounts and Permissions 15
Passwords 17
Password Guidelines 17
Backup and Restore 17
Factory Reset 18
Logging 18
Security Notifications and Patching 18
Recommendations for Decommissioning 19

CHAPTER 4. PRODUCT SUPPORT AND SERVICE OPTIONS 20
Product Support Options 20
Product Service Options 20
Returning Equipment for Repair 21
Replacement Parts 22
Engineering Services 22
Contacting Woodward's Support Organization 22
Technical Assistance 23

APPENDIX A. ANTI-TAMPER SEAL LOCATIONS 24

Illustrations and Tables

Figure 2-1. Purdue Model 8
Figure 2-2. ISA/IEC 62443 Cybersecurity Standard Stack (Source: ISA) 9
Figure 3-1. Defense in Depth....10
Figure 3-2. Potential Attack Vectors 14

Appendix A-1. Recommended Additional CPU Module Anti-tamper Seal Location....24
Appendix A-2. CPU and I/O Module Anti-tamper Seal Location....24
Appendix A-3. Intact Seal....25
Appendix A-4. Seal That Has Been Tampered With 25
Appendix A-5. Intact Seal on Chassis....25
Appendix A-6. Tampered Seal on Chassis 25

Warnings and Notices

Important Definitions

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

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

⚠WARNING

Overspeed / Overtemperature / Overpressure

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

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

⚠WARNING

Personal Protective Equipment

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

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

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

⚠WARNING

Start-up

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

NOTICE

Battery Charging Device

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

Electrostatic Discharge Awareness

NOTICE

Electrostatic Precautions

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

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

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

Follow these precautions when working with or near the control.

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

Chapter 1.
General Information

Purpose

This manual provides a description of the cybersecurity (“security”) context and strategies for the MicroNet XT control system. The manual covers security configurations, user access information, decommissioning, and security alert reporting and notification.

Scope

This manual covers the MicroNet XT control CPU part numbers in Table 1-1.

MicroNet XT

Table 1-1. CPU Information

CPU #	Preferred	Min. Coder	Secure Passwords	Achilles Cert	SSH/Firewall	SecureApp
5466-1300	Yes	1.0.0	Yes	No	Yes	Yes

References

Valid as of date of publication.

Woodward MicroNet XT Software Manual 35219 Volume 3

Woodward MicroNet XT Hardware Manual 35219 Volumes 1 and 2

ISA/IEC 62443 Refer to the ISA/IEC 62443 Series of Standards online.

NERC CIP Standards: Reliability Standards (nerc.com)

Glossary

AMService AppManager service running on the control
AppManager Woodward tool used to interface with the control
CIP Critical Infrastructure Protection
CISA Cybersecurity and Infrastructure Security Agency
DDoS Distributed Denial of Service
DiD Defense in Depth
DoS Denial of Service
IACS Industrial Automation Control Systems
IT Information Technology
NERC North American Electrical Reliability Corporation
OT Operational Technology
SOS Servlink OPC Server
SSH Secure Shell

Secure by Design

The Cybersecurity and Infrastructure Security Agency (CISA), defines Secure by Design as:
“Secure by Design products are those where the security of the customers is a core business requirement, not just a technical feature. Secure by Design principles should be implemented during the design phase of a product’s development lifecycle to dramatically reduce the number of exploitable flaws before they are introduced to the market for broad use or consumption.”
The CISA web page can be found at www.cisa.gov.

Woodward controls are designed and developed using an ISA/IEC 62443-based process, the Secure Development Lifecycle that ensures that cybersecurity is built into the product from the beginning. The applicable standards—national, international, and customer driven—are analyzed and pushed into the design documentation. The product design team then ensures that these security requirements are “baked into” the product, not added as an afterthought. All processes associated with product development also include the 62443-based secure development requirements.

Other major national security requirements incorporated into Woodward products include the North American Electrical Reliability Corporation (NERC) CIP standards and, for future product versions, the NIST cybersecurity framework. Refer to these organization’s web sites for more information.

Chapter 2.
Industrial Cybersecurity Basics

Introduction

You hear it in the news all the time lately. Electricity suppliers experiencing disruptions, petroleum companies shutting down, ransomware running rampant. These can all be traced back to attackers making their way into company IT and OT systems and causing these systems to malfunction or become unstable, even shutting down and having critical control systems disabled or destroyed. OT systems are particularly vulnerable to cybersecurity attacks due to complexity. Large systems are difficult to harden against attack. Personnel entrusted with handling cybersecurity tasks are overloaded or nonexistent. The system components that need to be updated or replaced may be very difficult to locate and access by maintenance staff.

Woodward cybersecure products such as the MicroNet XT are hardened during design and development to help aid a system owner in developing a cybersecure system. Features such as user access, logging, limited external/remote access paths, and separation of duties are primary features of MicroNet XT cybersecurity hardening.

What is Cybersecurity?

Cybersecurity is a discipline devoted to minimizing or eliminating any disruption to a system caused by events ranging from accidental user error to state (nation) level attacks intended to cause severe disruption or loss of data. Examples include (but are not limited to):

- Someone tripping over a cable and unplugging something critical.
- Entering a stolen password and gaining control of the system.
- Tampering with logs to hide attack activity.
- Flooding the Ethernet connection with data to disrupt communications with the operator.
- Invalid sensor data that could cause unstable operation of the system.

The MicroNet XT is designed to help prevent cyber attackers from disrupting a control system, thereby disrupting operations. Following the guidelines in this manual and configuring the MicroNet XT appropriately will go a long way towards establishing a stable and secure control system.

Where Does the MicroNet XT Live in the OT Network?

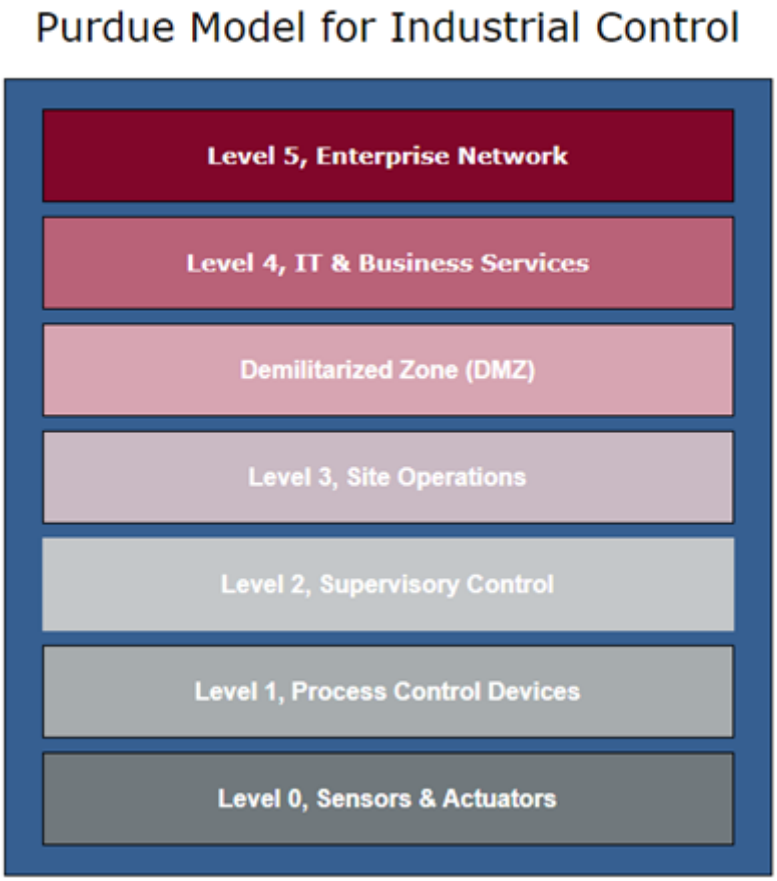


Figure 2-1. Purdue Model

The Purdue Model illustrated above represents a typical OT network architecture. Level 5 represents the enterprise IT network with level 4 representing services provided by IT.

The Industrial Demilitarized Zone, or DMZ, prevents unintended data exchange between IT and OT systems. General user tasks such as email, instant messaging, non-critical file sharing, and entertainment applications must never be allowed to access the OT network.

Level 3 represents site operations. This layer represents manufacturing operations systems including historians, data storage, secure remote access functions, and secure functions to exchange data between the OT and IT networks.

Level 2, the supervisory layer, contains automation operators, engineering workstations, and HMI's.

Level 1 contains basic control equipment. These consist of complex controllers, PLC's, monitoring equipment, and other equipment required to maintain control of the process.

Level 0 consists of sensors and outputs interfacing with the process. Sensors could be pressure, temperature, speed, and so on. Outputs can include motors, relays, valves, and other hardware to perform some function on the process.

The MicroNet XT lives at level 1 of the Purdue model illustrated in Figure 2-1. It is a network endpoint meaning that it does not pass information through to other elements of the network (for example as a network router would). Operators at level 2 can communicate with the control. Devices at level 0 are accessed by the control as inputs and outputs.

ISA/IEC 62443

The ISA/IEC 62443 set of standards provide international standardization of four cybersecurity areas:

- Terminology, metrics, use cases.
- Policies and procedures for manufacturing and integrators.
- System guidance for functions such as development, testing, supply chain, and security level definition.
- Component design and development including secure development lifecycle, development and testing environments.

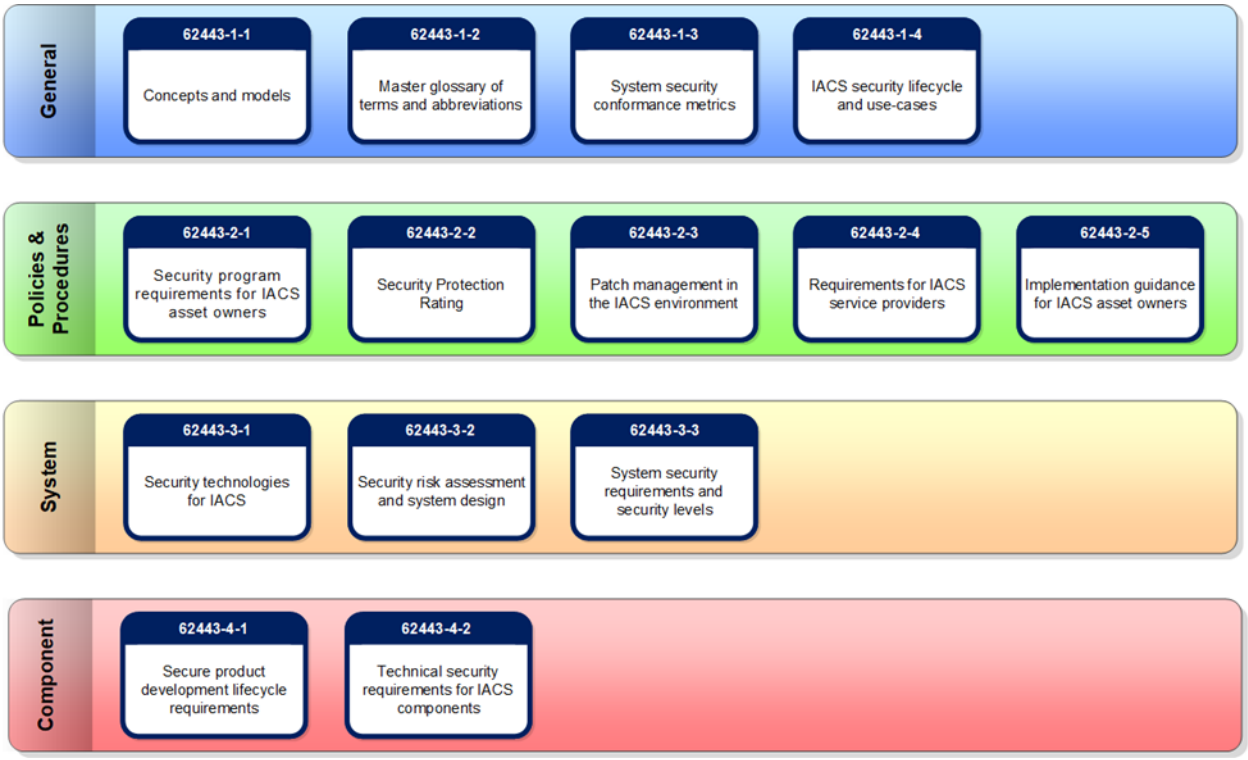


Figure 2-2. ISA/IEC 62443 Cybersecurity Standard Stack (Source: ISA)

Woodward cybersecure products follow a Secure Development Lifecycle (SDLC) based heavily on the ISA/IEC 62443 set of standards. These standards help ensure that not only is the product designed to be secure, but business processes such as development environment, verification and validation, and supply chain are performed to international cybersecure standards.

Woodward cybersecure products are designed to 62443-4-1 and 62443-4-2 in general. This layer deals specifically with component design and development. Standards 62443-3-1, -3-2, and -3-3 are implemented to help ensure business processes are performed such that cybersecurity is built into the final product.

Woodward products are designed in accordance with the guidelines of IEC 62443 via the secure development lifecycle, while also enabling customers to implement their preferred regional or application-specific cyber security standards.

NOTE: Unless otherwise stated elsewhere in this manual, this information does **NOT** imply that any given MicroNet XT part number has ISA/IEC 62443 certification. This section only describes the SDLC process used during product development.

Chapter 3.
Defense in Depth (DiD)

Introduction

This chapter introduces the concept of Defense-in-Depth (DiD).

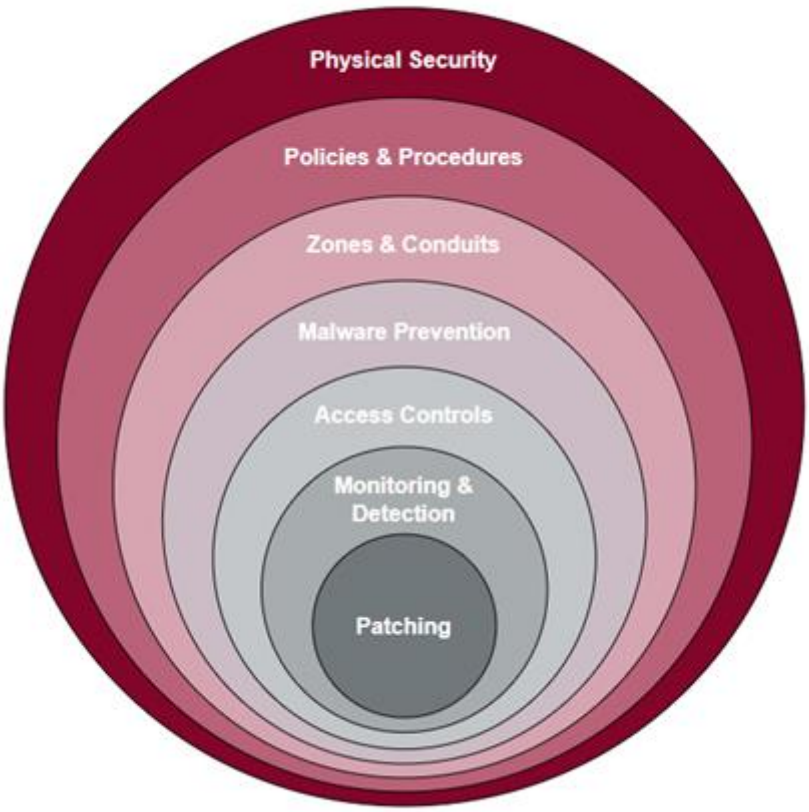


Figure 3-1. Defense in Depth

Defense in Depth is a strategy that leverages multiple security measures to protect an organization's assets. The concept is that if one layer of defense is compromised, additional layers exist to help ensure that threats are stopped before the MicroNet XT is compromised.

Physical Security

Physical security must be tailored to the environment the MicroNet XT is used in. The following are a few guidelines.

The best way to keep the MicroNet XT secure is to limit who has physical access to it. Physical security can include fences, closed-circuit cameras, security personnel, signage, and motion sensors, etc. The idea is to detect and deter attackers before they can access the control system. Ensure that physical security devices notify the appropriate personnel in a timely manner so action can be taken if needed. The earlier the warning occurs the better.
The next layer of physical security is to ensure that the MicroNet XT is installed in a secure, weatherproof, lockable enclosure including conduit to protect cabling to and from the control. Ensure that only approved personnel have access to the enclosure. Provide some method to alert operators that the enclosure has been accessed.

Just as important as physically protecting the MicroNet is protecting the cabling attached to the control. Physical damage to the cabling can cause instability of the equipment controlled by the MicroNet XT and damage to the MicroNet XT itself. Damage to cabling does not need to be severe to be a significant threat. Sensor feedback to the control can cause significant damage and instability. Driver signals to the equipment being controlled can be lost or shorted to each other or ground, causing damage or instability.

Another concern for cabling is the ability of an attacker to tap into the cabling. An attacker could capture proprietary information such as configuration and user data. Capturing data could allow an attacker to create false or inaccurate information by delaying messages or injecting false information causing damage or instability.

Physical security for new components, i.e., cards, includes ensuring that anti-tamper labels applied to all MicroNet XT CPU and I/O cards remain intact. If a label must be removed for service, ensure that a new label is applied. Anti-tamper labels are also used on shipping packaging used for the MicroNet XT. Reject cards that have had the anti-tamper seals damaged or removed. MicroNet XT cards that are not ready to be used, i.e., spares or not ready for installation, must be protected physically by storage in a secure container or cabinet. Refer to Appendix A of this document for images of anti-tamper seals.

All service-related activities should be documented and acknowledged by the system owner. Ensure that all personnel performing service or maintenance are qualified to do the work.

Policies and Procedures

The control owner should have policies and procedures in-place to raise awareness of security practices for control systems and IACS in general. Having a security-aware staff greatly eases the process of implementing security practices. When the team understands the need for security, they are more likely to help ensure security is in place.

Zones and Conduits

This refers to the risk analysis method of separating a system diagram into security zones and the conduits, or data flow, between them. The resulting analysis breaks down the system into manageable sections that can be analyzed individually.

The control should not be directly accessible from any public network including the Internet. Networks are a very common attack path for electronic controls that can be operated remotely. Isolating the MicroNet XT to the secure plant control network should be high priority.

If complete isolation from a public or insecure network is not possible, protect and secure the network in which the MicroNet XT resides from attacks originating from the insecure network. Firewalls, routers, IDS, and IPS equipment can help ensure cybersecurity for the control.

Ports

Disable logical ports that will not be used. The fewer open ports on a device, the fewer access points an attacker will have to get into the device. Often, a system operator may not be aware of open ports. This could be due to maintenance and troubleshooting activities, or through using software that opens ports by default for its own use. Regularly scan the device with a network scanning program or appliance to check for open ports that should not be open and act as necessary. Refer to the MicroNet XT software manual for details of default open ports used by the control.

The MicroNet XT implements a stateful firewall internally to help with communications security. This firewall is configurable to support system operator needs. Refer to the MicroNet software manual for firewall details.

Woodward recommends and can supply external firewall products that implement IDS and IPS. Refer to your sales contact or Woodward customer service for details.

Default Open Ports

22 SSH port for HMI interfaces.

Note on AMService beacon:
The AMService beacon (a multicast UDP message to port 5134) is used by AppManager to automatically discover controls on the network. This presents a potential security risk in that an attacker could detect this signal and use that knowledge to perform a spoofing attack on the control system.

Woodward recommends disabling this signal to enhance the cybersecurity of the MicroNet XT. The signal can be disabled using instructions in AppManager. In “Help” from the main screen, search for “‘beacon”. If the beacon is disabled, the control can still be found by AppManager, but it becomes a manual operation. Full details can be found in AppManager Help.

Denial of Service (DoS) Protection

Denial of Service attacks are ones where a deluge of information is sent to the MicroNet XT’s communications ports causing the ports to slow down substantially or possibly even crash. This information can consist of a combination of valid requests at such a high rate that the port handler cannot keep up, or malformed messages that the port cannot resolve in a timely manner.

The MicroNet XT is designed such that a DoS attack will not interrupt the critical process control. External communications are executed on a separate processor from the mission critical control program. The communication processor can be reset without affecting the process control. Refer to the MicroNet XT hardware manual for the communication processor reset procedure.

Default Communication Protocols

The MicroNet XT provides two default protocols for operator communications. These are:

SSH - Enabled by default on the Ethernet interface for user interaction. It is started by the real time operating system on startup.
SFTP - Available for transferring files by some service tools. Refer to the MicroNet XT software manual.

Malware Prevention

Every effort must be made to ensure that any software or firmware loaded to the MicroNet XT is authentic Woodward software. Woodward firmware is signed to ensure authenticity. Integrity is checked during installation to ensure the software is identical to when it was developed.

Access Controls

User Interface

Control access should be through hardened PC’s or HMI’s. PC’s running Windows provide a widely known attack path. Ensure that all patches and updates are applied and that security tools are installed and kept up to date. Any user interface connected to the MicroNet XT should be hardened and have all security updates applied.

Use encrypted communications whenever possible. The MicroNet XT automatically starts SSH for operator communications. OPC-UA, which can be encrypted, travels via SSL. Modbus is not encrypted.

Service Tools

Woodward provides an array of software tools that can provide functions from monitoring to full MicroNet XT operation and configuration. Ensure that only Woodward supplied tools are used to interact with the MicroNet XT. Refer to the MicroNet XT software manual, your installer or sales contact, or Woodward customer support for details.

Monitoring and Detection

From a cybersecurity perspective, monitoring and detection during system operation will help in detecting unusual operation that may be caused by interference of the physical control system or an attacker intruding into the system. Woodward provides software tools that will help an operator to monitor the system and raise alarms in case of aberrant behavior. Refer to manual B35219V3, Application Programming Tools Real Time Operating System (RTOS) Control Interface (Service) Tools, for details.

Patching

Woodward occasionally releases new software for controls that update the control with new or updated functions. These patches may also contain security updates required to keep the control secure. It is critical that the system owner/operator installs these updates as soon as practicable when they are released.

Additional MicroNet XT Security Features

The MicroNet XT itself implements several security features intended to help the system owner/operator achieve their desired security level. These include:

- Configurable user accounts and passwords.
- Configurable session control for network communications.
- Logging of security and system events.
- Alerts for operational and security events.
- Secure user communications using SSH (Ethernet) and SSL (OPC).
- Secure file transfers when performed using SFTP.

Alerts

The MicroNet XT will generate alerts for these security events:

- Failed access attempts
- Failed login attempts

Factory Reset

NOTE: Pressing the reset button will permanently erase all information listed below. THIS CANNOT BE UNDONE. Ensure all important information is backed up before performing a factory reset. See the section on Backup and Restore later in this document.

The MicroNet XT provides a reset button on the CPU module to return the CPU to factory condition. Use this feature with extreme caution as all user and configuration data will be lost. Refer to the Backup and Restore section for further details to restore a reset control.

To perform a factory reset, the CPU module must be powered down. Refer to manual 35219V3 for instructions on how to perform this procedure.

A factory reset will perform the following changes:

- All GAP applications will be erased.
- All GAP application logs, tunables, and other related files will be erased.
- All local accounts, including passwords, will be reset to the factory default settings.
- All logs will be erased.
- All customer data stored in non-volatile memory will be erased.
- All network configurations will be reset to factory defaults.

Retained Information:

- The latest (last) version of installed firmware will be retained.
- Non-confidential information which may help in troubleshooting will be retained (for example: temperature histograms, run-time hours).
- Unique device attributes programmed during production, such as security keys required for secure GAP apps will be retained.

Tamper Detection

Woodward recommends that tamper evidence, such as anti-tamper tape, be placed over the reset switch to help determine if a user has reset the control. The control does not have anti-tamper tape in place at the time of shipment.

Note that the CPU module does have anti-tamper tape in place near to the reset button. Tampering with this tape will void the product warranty. Make sure you are locating your anti-tamper evidence such that the warranty seal is not affected.

Attack Scenarios

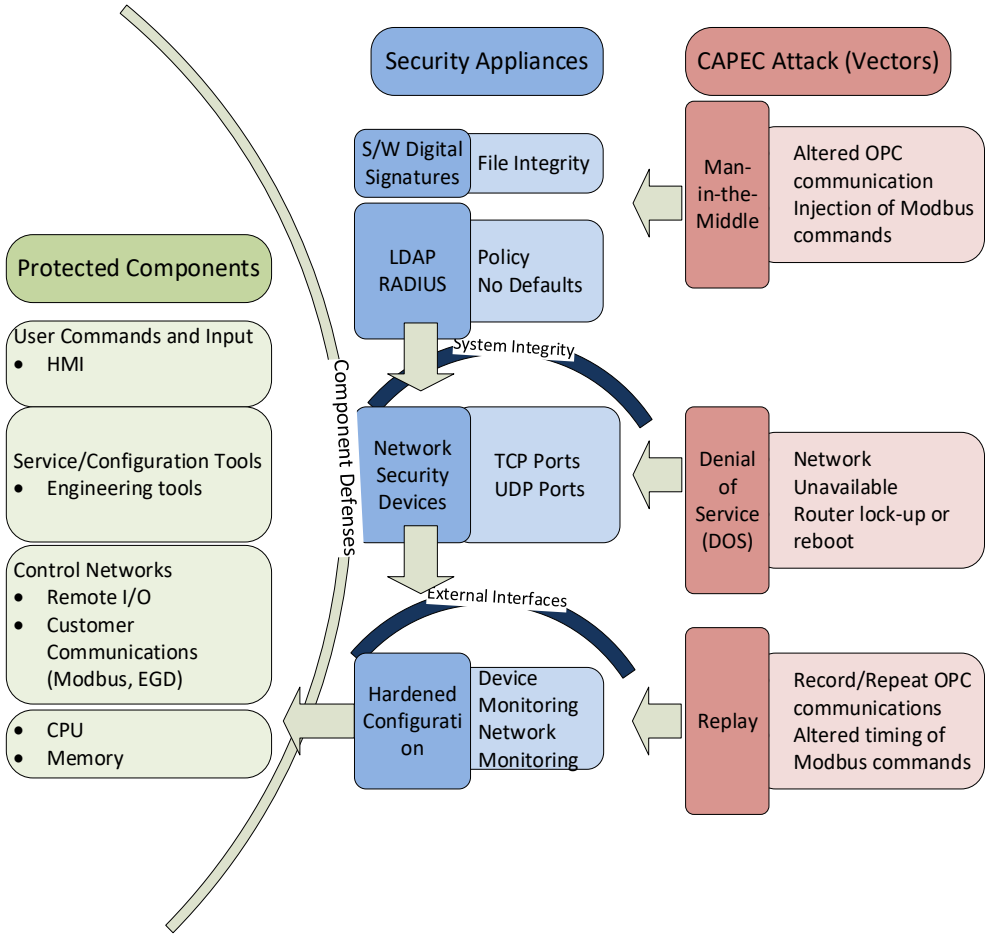


Figure 3-2. Potential Attack Vectors

The attack vectors in Figure 3-2 illustrate a few examples of attacks which could impact the availability and integrity of the MicroNet XT. A man-in-the-middle attack could exploit vulnerabilities of insecure Modbus communication networks, for example. One scenario for this type of attack involves an attacker controlling and possibly altering messages/packets/data between two parties. In a man-in-the-middle attack, the integrity of sensor data or output commands could be compromised, leading to unexpected and hazardous control of the attached machinery. A replay attack can have the same impact, but it exploits valid messages/packets/data which are repeated or delayed, fooling the user 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 attacks often exploit network vulnerabilities by overwhelming routers and network adapters with unnecessary traffic.

To help combat DoS attacks, the system should provide network appliances to detect intrusion, provide rate limiting and provide deep packet inspection. The appliances should be within the same security zone as the MicroNet XT. This will help ensure the MicroNet XT remains responsive.

NOTE: A loss of communications via the Ethernet connection will not shut the MicroNet XT down, but it may make operator access to vital functions difficult or impossible. The system must provide hard-wired backup controls as required to handle critical functions such as shut down or reset, or to provide other safety functions in the event of communications loss.

Security References

Security references, such as those from IEC/ISA 62443, NIST, and NERC, are guidelines to help ensure that the product is designed and developed in such a way that it can guard against attacks and actions that would compromise performance. Examples of these actions range from simple human error, up to and including malicious attacks resulting in damage to the MicroNet XT and damage to equipment connected to the MicroNet XT.

The MicroNet XT control references NERC CIP's 2.5 through 14, as applicable. NERC CIPs are not requirements, rather they guide a system owner to implement a secure system. The MicroNet XT uses the NERC CIPs to aid a system owner to meet their security needs. See Appendix B of this document for details.

The MicroNet XT platform is designed and developed using a cybersecurity development lifecycle based on IEC/ISA 62443 parts 3-2, 4-1, and 4-2. It is recommended that the user implement a cybersecurity management program based on the ISA/IEC 62443-2-1 standard in addition to user designated cybersecurity standards and frameworks.

Incorporating these cybersecurity guidelines and standards helps ensure that the MicroNet XT will integrate well with cybersecure industrial automation control systems (IACS) that implement NERC guidance.

User Account Management

User account management is a crucial step in securing the MicroNet XT. Unauthorized users can cause untold damage to the control system and connected equipment through unauthorized actions, altering operational state, altering configurations, tampering with, or stealing logs, etc.

Repudiation, when a user denies that they accessed and/or altered the control state when in fact they did, makes it very difficult for the system operator to investigate a control tampering problem or other security breach. User account management helps preclude repudiation by rigorously tracking in the system logs who accesses the MicroNet XT and when, and what actions they performed.

Account management falls into three categories:

- Accounts for user access
- Passwords for account access
- Session control

Accounts and Permissions

A primary tenet of account management is that users should only be given the lowest possible permissions that allows them to perform their duties. This is called the least privilege principle.

Accounts should be role-based. It is much easier to manage users by role than by name. Roles can be assigned passwords and permission levels specific to roles used by the MicroNet XT. Users can be moved into different roles or removed from all roles. If permissions and passwords are administered by the user, it is easy to forget to change permissions for a user and difficult to enforce password policies.

Accounts can be configured by the system administrator. Guidelines for account names, permissions, and passwords can be found in the MicroNet XT software manual.

Account Guidelines

Historically, ICS appliances have been delivered with common (identical) accounts and passwords. This has created a situation in which any attacker could readily find the login credentials needed to take control of the system. In order to prevent this situation and provide an extra level of security for

the MicroNet XT owner/user, the MicroNet XT will be supplied with unique initial passwords that are unique to each CPU module. This unique password will use common prefixes followed by the serial number of the CPU module. The following information describes these unique passwords.

The format of the new passwords is <account name>@<serial number> with the serial number being the serial number of the CPU module itself. This format makes it somewhat easier for administrators to remember the unique passwords for each account.

Up to 200 unique user accounts can be created.

As with all passwords, these initial passwords can be changed to any text that complies with the password rules described elsewhere in this manual. Passwords can be changed using Woodward service tools. It is strongly recommended that initial passwords be changed on first login.

Accounts can be assigned security levels ranging from 1 to 15, with 15 being the most privileged. The Administrator account resides at Level 15. This level is reserved for the Administrator account, and new accounts cannot be created for it. The MicroNet XT comes with four different default accounts:

1. Administrator (may **not** be renamed or deleted)
   - A. Initial Password: Admin@<CPU serial number>
   - B. Level: 15 (may not be changed)
   - C. Duration: No Expiration (should be changed to enable security)
   - D. Fixed Password: No (may be changed)
   - E. Role: Master account for managing other accounts

2. ServiceUser (may be renamed or deleted)
   - A. Initial Password: Serv@<CPU serial number>
   - B. Level: 11 (may be changed)
   - C. Duration: No expiration (should be changed to enable security)
   - D. Fixed Password: No (must be changed by administrator)
   - 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. Operator (may be renamed or deleted)
   - A. Initial Password: Oper@<CPU serial number>
   - B. Level: 7 (may be changed)
   - C. Expiration: No expiration
   - D. Fixed Password: No (must be changed by administrator)
   - E. Role: Shared account for HMI operation

4. Datalog (may be renamed or deleted)
   - A. Initial Password: Data@<CPU serial number>
   - B. Level: 1 (may be changed)
   - C. Duration: No expiration
   - D. Fixed Password: No (must be changed by administrator) Role: Shared account for minimal access (e.g., reading files)
   - E. The Datalog account is recommended for use by the WoodwardFileCollector service to collect Datalog files.

NOTE: Fixed passwords must be changed by an administrator. Members of a role cannot change the account password.

User-created Account Names

- The Account Name must be unique.
- The first character must be an ASCII letter (a - z, A - Z), digit (0 - 9), underscore (_) or dot (.)
- The remaining characters must be ASCII letters, digits, underscores, dots, or hyphens (-).
- The name can use a dollar ($) character at the end.
- The Account Name must be between 4 and 32 characters in length (inclusive).

Passwords

Good password policy is critical to good account security. Passwords should have good length and high complexity. Standard secure password guidance should be followed such as no common words or phrases, mix of characters, and adequate length to make brute-force guessing more difficult.

Password Guidelines

Password Rules

The MicroNet XT enforces the following password rules. These rules were derived from several worst-case (most restrictive) industrial cybersecurity standards.

- The new password must be different from current password.
- The password must be between 8 and 511 characters in length (inclusive).
- The password is case sensitive.
- The password must contain at least four different types of characters: uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric ('special' characters). Supported password characters:
  !"#$%&'()*+.0123456789<=>?`ABCDEFGHIJKLMNOPQRSTUWXYZ[\]^_@abcdefghijklmnopqrstuwxyz{|}~-
  NOTE: The password **cannot** contain the characters backslash, colon, or semicolon (\ ,:, or ;)
- The password should have a defined expiration period. The recommended time limit is 15 months maximum.
- The control will enforce a default limit of 12 consecutive login failures per 15 minutes. Additional attempts can be made within those 15 minutes at approximately 3-minute intervals.

Refer to the MicroNet XT software manual for further password guidance and details.

Sessions

Open sessions are another attack path attackers can use. Sessions that have been abandoned can keep a port open that should have been closed. Abandoned sessions may also be found by an attacker scanning a network. Multiple abandoned or unused sessions could use up all available sessions (a maximum of 10) and prevent an operator from accessing the MicroNet XT by creating a DoS situation. The MicroNet XT offers several solutions for session issues. The user of a session can logout properly, which automatically closes a session. The MicroNet XT will log and alert for session issues. Refer to the MicroNet XT software manual for details.

Backup and Restore

The MicroNet XT provides functionality to backup and restore the control applications and configuration. This functionality is available using the AppManager tool. Refer to the MicroNet XT software manual for details.
Backup and restore works with the following data:

- Network configuration
- NTP settings
- GAP application executable
- Files generated by GAP applications
- The name of the control
- Control information needed to restore
  - Module name
  - Module type
  - Module version
- System log files

The control owner/operator should check the MicroNet XT configuration at least once every 35 days for unintended configuration changes. A baseline configuration should be developed to monitor the following items:

- Operating system including version
- Applications including version
- Network configuration

Factory Reset

NOTE: Pressing the reset button will permanently erase all information listed below. THIS CANNOT BE UNDONE. Ensure all important information is backed up before performing a factory reset.

The MicroNet XT will enter “factory reset” mode when the reset button is pressed and held during a cold startup. This is to prevent triggering a reset while the control is running.
The control will announce that a factory reset is in progress via the LED’s and the serial console.
If a reset is performed using the reset button located on the CPU module, the following information will be erased:

- All GAP applications.
- All GAP application related files (logs, tunables, etc.)
- All local user accounts created since the control was last reset. Default accounts and passwords will be re-enabled.
- All logs potentially containing customer confidential information.
- All customer data stored in non-volatile memory.
- All network configurations will be returned to the default values.
- The latest version of installed firmware will be retained.
- Non-confidential information which may be used for troubleshooting the control will be retained.

Logging

The MicroNet XT captures several types of logs to help the user to better understand the status of the control. These include access logs, control system events, security logs, and so on. Refer to the MicroNet XT software manual for details.

Types of Logs Captured

- Access control
  - Successful logins
  - Failed logins
  - Temporarily locked accounts which have reached the limit of the consecutive failed login attempts.
  - Failed logins due to exceeding the total system limit of concurrent connections.
- Request errors
- Control system events
  - System boot
  - Reset/reboot reason
  - GAP events
- Software installation events
  - Information about backup creation and restore actions
  - Errors related to unpacking and installing software/firmware
  - Errors related to authentication of software/firmware
- Configuration changes.
  - Change in network settings
  - Footprint (system software) update steps and errors
- Audit log events
  - Issues with log partition on memory or SYSLOG functions

The MicroNet XT will log changes to the baseline configuration. It is recommended that the user check this log at least once every 35 calendar days for possible configuration changes that may cause unintended control operation.

Security Notifications and Patching

Security Notifications

The Woodward Product Security Incident Response Team (PSIRT) is notified of security incidents related to Woodward secure products. The PSIRT analyzes the incident report and decides how best to deal with the issue. Depending on the severity of the issue, the PSIRT may:

- Notify customers of the incident and possibly offer quick fixes to help minimize risk in the short term.
- Place security event notices on the Woodward product support web site.
- Immediately update product software to fix flaws and release the software on the Woodward product support website.
- Schedule low priority fixes in the product patching schedule to provide security updates in the next service pack release.

Customers can report security problems through Woodward customer service or the Woodward cybersecurity reporting email address: cybersecurityhelpdesk@woodward.com.

Firmware Upgrade

Woodward occasionally releases service packs after product release to fix functional and security issues. It is vital that service packs be installed as soon as practical to keep the MicroNet XT secure. Service packs are available on the Woodward product support web site at:

https://www.woodward.com/en/support/industrial/technical-help-desk.

See the MicroNet XT software manual for details of upgrading software.

Recommendations for Decommissioning

During the life of the MicroNet XT, sensitive information may have been stored on the control. It is critical to owner/operator security to prevent sensitive information from escaping into competitors or security attacker’s hands. To prevent this, Woodward recommends resetting the MicroNet XT to factory default settings. Refer to the MicroNet XT software manual for details.

Chapter 4.
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/local-partner**

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 (5-09-0690) that is in effect at the time the product is originally shipped from Woodward or a service is performed:

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

Replacement/Exchange: Replacement/Exchange is a premium program designed for the user who is in need of immediate service. It allows you to request and receive a like-new replacement unit in minimum time (usually within 24 hours of the request), providing a suitable unit is available at the time of the request, thereby minimizing costly downtime. This is a flat-rate program and includes the full standard Woodward product warranty (Woodward Product and Service Warranty 5-09-0690).

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

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

Flat Rate Repair: Flat Rate Repair is available for the majority of standard products in the field. This program offers you repair service for your products with the advantage of knowing in advance what the cost will be. All repair work carries the standard Woodward service warranty (Woodward Product and Service Warranty 5-09-0690) on replaced parts and labor.

Flat Rate Remanufacture: Flat Rate Remanufacture is very similar to the Flat Rate Repair option with the exception that the unit will be returned to you in "like-new" condition and carry with it the full standard Woodward product warranty (Woodward Product and Service Warranty 5-09-0690). This option is applicable to mechanical products only.

Returning Equipment for Repair

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

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

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

Packing a Control

Use the following materials when returning a complete control:

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

NOTICE

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

Replacement Parts

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

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

Engineering Services

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

- Technical Support
- Product Training
- Field Service

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

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

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

For information on these services, please contact one of the Full-Service Distributors listed at: https://www.woodward.com/en/support/industrial/service-and-spare-parts/find-a-local-partner

Contacting Woodward's Support Organization

For the name of your nearest Woodward Full-Service Distributor or service facility, please consult our worldwide directory at **https://www.woodward.com/support**, 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 _____

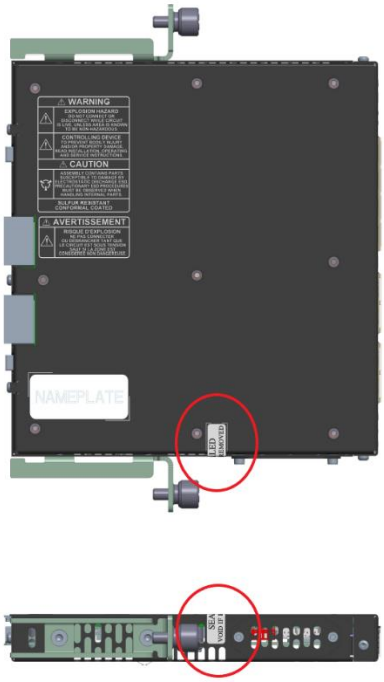
_____

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.

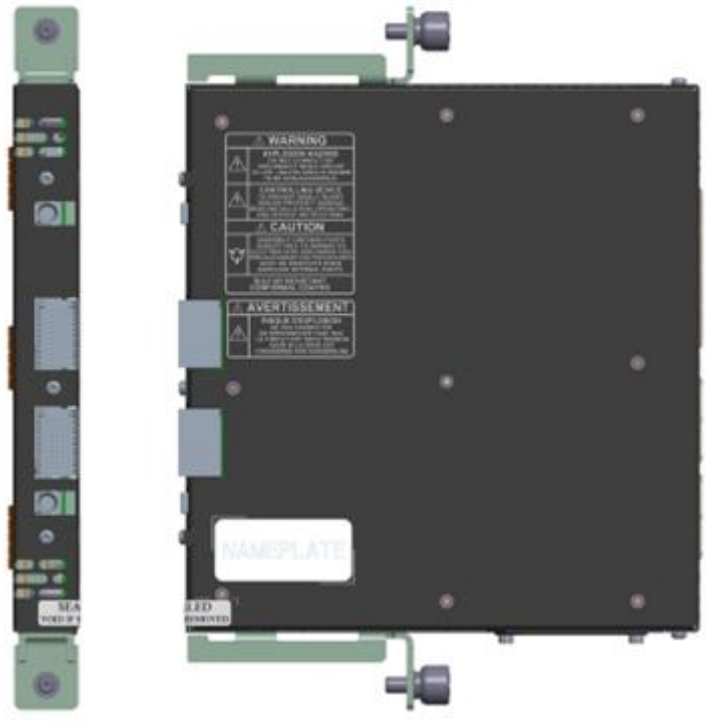
Appendix A.
Anti-tamper Seal Locations

The following images show the locations of the anti-tamper seals on the CPU and I/O cards. There are also images of intact and altered seals.

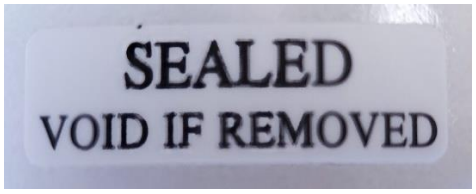
This is the recommended location to place anti-tamper tape on a CPU module. Due to commissioning and configuration activities at the factory and by the installer, the CPU module may or may not have tape applied when the final user receives the module.



Appendix A-1. Recommended Additional CPU Module Anti-tamper Seal Location



Appendix A-2. CPU and I/O Module Anti-tamper Seal Location



Appendix A-3. Intact Seal

Appendix A-4. Seal That Has Been Tampered With

Appendix A-5. Intact Seal on Chassis

Appendix A-6. Tampered Seal on Chassis

Revision History

Revision -

- New manual release

Released

We appreciate your comments about the content of our publications.

Send comments to: industrial.support@woodward.com

Please reference publication 35219V4.

B 3 5 2 1 9 V 4 : -

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.