WOODWARD

Product Manual 35241
(Revision -, 11/2024)
Original Instructions

UG-25+ Governor Security Manual

Security Manual

Released

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.

Woodward Industrial Support: Get Help

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 35241

Contents

WARNINGS AND NOTICES **3**

ELECTROSTATIC DISCHARGE AWARENESS **5**

REGULATORY COMPLIANCE **6**

CHAPTER 1. GENERAL INFORMATION **7**
Purpose 7
Scope 7
References 7
Glossary 7

CHAPTER 2. INDUSTRIAL CYBERSECURITY BASICS **8**
Introduction 8
What is Cybersecurity? 8
Where Does the UG-25+ Live in the OT Network? 8

CHAPTER 3. DEFENSE IN DEPTH (DID) **10**
Physical Security 10
Denial of Service (DoS) Protection 11
Malware Prevention 11
Access Controls 11
Policies and Procedures 12
Zones and Conduits 12
Monitoring and Detection 12

CHAPTER 4. ATTACK SCENARIOS **13**

CHAPTER 5. UG-25+ SECURITY OVERVIEW **14**
UG-25+ Security Overview 14
Security References 14
Security Notifications and Patching 14

CHAPTER 6. PRODUCT SUPPORT AND SERVICE OPTIONS **15**
Product Support Options 15
Product Service Options 15
Returning Equipment for Repair 16
Replacement Parts 17
Engineering Services 17
Contacting Woodward's Support Organization 17
Technical Assistance 18

REVISION HISTORY **19**

Illustrations and Tables

Figure 3-1. Defense in Depth Diagram 10
Figure 4-1. Potential Attack Vectors 13

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

Lockout/Tagout LOTO

Ensure that personnel are fully trained on LOTO procedures prior to attempting to replace or service equipment on a "live" running engine. All safety protective systems (overspeed, over temperature, overpressure, etc.) must be in proper operational condition prior to the start or operation of a running engine. Personnel should be equipped with appropriate personal protective equipment to minimize the potential for injury due to release of hot hydraulic fluids, exposure to hot surfaces and/or moving parts, or any moving parts that may be activated and are located in the area of control of the unit.

⚠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.

⚠WARNING

Automotive Applications

On- and Off-highway Mobile Applications: Unless Woodward's control functions as the supervisory control, customer should install a system totally independent of the prime mover control system that monitors for supervisory control of engine (and takes appropriate action if supervisory control is lost) to protect against loss of engine control with possible personal injury, loss of life, or property damage.

⚠WARNING

IOLOCK

IOLOCK: driving I/O into a known state condition. When a control fails to have all the conditions for normal operation, watchdog logic drives it into an IOLOCK condition where all output circuits and signals will default to their de-energized state as described below. *The system MUST be applied such that IOLOCK and power OFF states will result in a SAFE condition of the controlled device.*

- **Microprocessor failures will send the module into an IOLOCK state.**
- **Discrete outputs / relay drivers will be non-active and de-energized.**
- **Analog and actuator outputs will be non-active and de-energized with zero voltage or zero current.**

Network connections like CAN stay active during IOLOCK. This is up to the application to drive actuators controlled over network into a safe state.

The IOLOCK state is asserted under various conditions, including:

- **Watchdog detected failures**
- **Microprocessor failure**
- **PowerUp and PowerDown conditions**
- **System reset and hardware/software initialization**
- **PC tool initiated**

NOTE—Additional watchdog details and any exceptions to these failure states are specified in the related section of the product manual.

NOTICE

Battery Charging Device

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

Electrostatic Discharge Awareness

NOTICE

Electrostatic Precautions

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

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

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

Follow these precautions when working with or near the control.

1. Avoid the build-up of static electricity on your body by not wearing clothing made of synthetic materials. Wear cotton or cotton-blend materials as much as possible because these do not store static electric charges as much as synthetics.
2. Touch your finger to a grounded surface to discharge any potential before touching the control, smart valve, or valve driver, or installing cabling connectors. Alternatively, ESD mitigation may be used as well: ESD smocks, ankle or wrist straps and discharging to a reference grounds surface like chassis or earth are examples of ESD mitigation.
    - ESD build up can be substantial in some environments: the unit has been designed for immunity deemed to be satisfactory for most environments. ESD levels are extremely variable and, in some situations, may exceed the level of robustness designed into the control. Follow all ESD precautions when handling the unit or any electronics.
        - I/O pins within connectors have had ESD testing to a significant level of immunity to ESD, however do not touch these pins if it can be avoided.
            - Discharge yourself after picking up the cable harness before installing it as a precaution.
        - The unit is capable of not being damaged or improper operation when installed to a level of ESD immunity for most installation as described in the EMC specifications. Mitigation is needed beyond these specification levels.

IMPORTANT

External wiring connections for reverse-acting controls are identical to those for direct-acting controls.

Regulatory Compliance

For all hardware Regulatory Compliance including North America, Europe, International, and Marine compliance refer to manual:

Manual Number	Manual Description
26330	UG-25+ GOVERNOR INTALLATION & OPERATION

Special Condition for Safe Use

The UG-25+ Governor (UG-25+) was developed without a secure development life cycle process prior to the realization of current cybersecurity standards, and as such, shall not be considered a cybersecure product.

Chapter 1.
General Information

Purpose

This manual provides a description of the cybersecurity (“security”) context and strategies for the UG-25+ Governor referred to as the UG-25+ in the rest of this manual. This manual covers security configurations, user access information, decommissioning, and security alert reporting and notification.

Scope

This manual covers the UG-25+ Governor.

References

Woodward Manual 26330, UG-25+ Governor Installation and Operation Manual

Manual B26579, UG-25+ Governor (P3 Version)

Manual B26643, UG-25+ Governor (P3 Version) Turbine Control

SA/IEC 62443 https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Product Change Notification 06905, UG-25+ Control Service Tool Version 2.4

Glossary

CAN	Controller Area Network
DDoS	Distributed Denial of Service
DiD	Defense in Depth
DoS	Denial of Service
HMI	Human Machine Interface
IACS	Industrial Automation Control Systems
ICS	Industrial Control System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
OT	Operational Technology
PLC	Programmable Logic Controller
SCADA	System Control and Data Acquisition
SNTP	Simple Network Time Protocol

Chapter 2.
Industrial Cybersecurity Basics

Introduction

Cybersecurity attacks are often carried out through IT and OT systems causing them to malfunction, become unstable, be disabled, or even be destroyed. OT systems are particularly vulnerable to cybersecurity attacks due to their complexity as large systems, making it difficult to harden against attack. In addition, personnel to handle cybersecurity tasks are often overloaded or nonexistent, and the system components that need to be updated or replaced may be very difficult to locate or be accessed by maintenance staff.

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.
- 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.

Following the guidelines in this manual and configuring the UG-25+ appropriately will aid in establishing a stable and secure environment.

Where Does the UG-25+ Live in the OT Network?

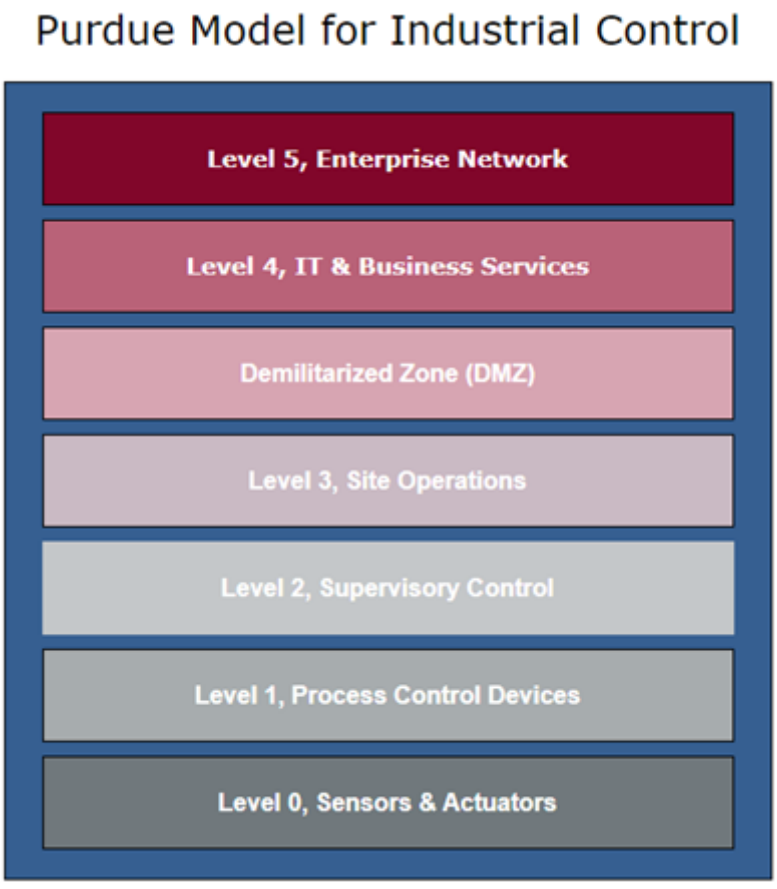

Figure 2-1. Purdue Model

The Purdue reference 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 SCADA (System Control and Data Acquisition) systems, data storage, secure remote access functions, and secure functions to exchange data between the OT and IT networks.

Level 2, the supervisory layer, contains SCADA client functions, 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 UG-25+ has direct physical control of a device so lives at level 0 of the Purdue model illustrated in figure 1.

Chapter 3.
Defense in Depth (DiD)

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

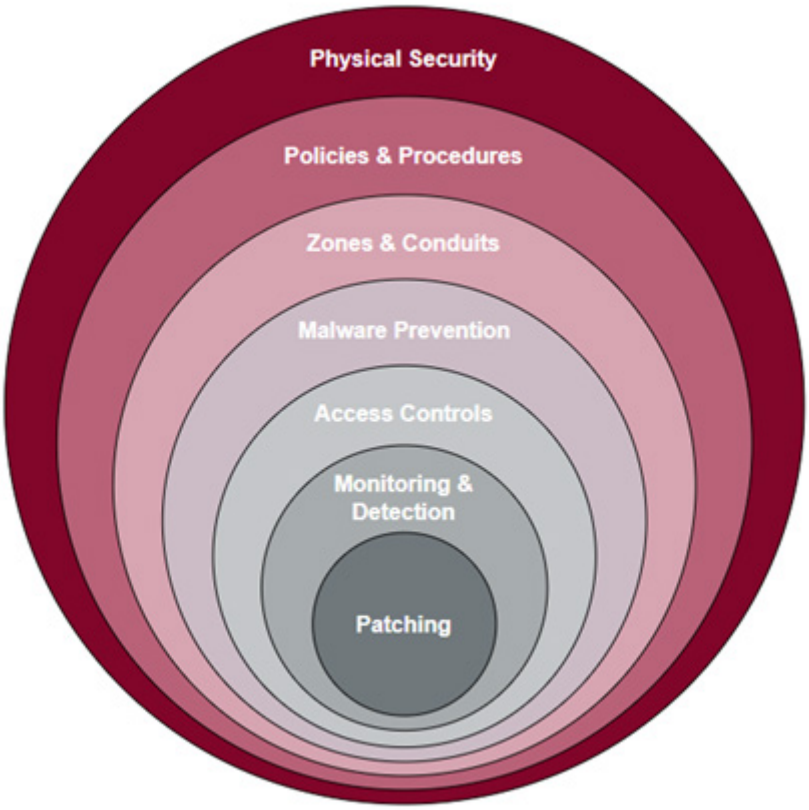

Figure 3-1. Defense in Depth Diagram

Defense in Depth is a strategy that leverages multiple layers of security 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 UG-25+ is compromised.

Physical Security

Physical security must be tailored to the environment the UG-25+ is used in. The following are a few guidelines.

Physical access control is an aspect of a Defense in Depth strategy for securing the UG-25+ in an application. Physical security can include fences, closed-circuit cameras, guards, signage, motion sensors, etc. The objective 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 UG-25+ control is generally mounted near, or on a prime mover. The prime mover and its environment should have secure access to ensure that only approved personnel have access to the control and prime mover. A good practice is to provide a method to alert operators that the control or its environment have been accessed.

Just as important as physically protecting the UG-25+ is protecting the cabling attached to the control. Physical damage to the cabling can cause instability of the equipment controlled by the UG-25+ and

damage to the UG-25+ itself. Damage to cabling does not need to be severe to be a significant threat. Inaccurate or corrupted sensor feedback to the control can cause considerable damage and instability. Driver signals to the equipment being controlled can be corrupted, lost, or shorted to each other or ground, causing damage or instability.

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

Denial of Service (DoS) Protection

The UG-25+ has no external routable network interfaces (i.e. Ethernet) and non-routable system communications (Non-routable Communications include RS-485 Serial and CAN). The UG-25+ service port is not designed for continuous communication and is only for configuration or service of the device.

Malware Prevention

Every effort must be made to ensure that any software or firmware loaded to the UG-25+ is authentic Woodward or application developer software. While the UG-25+ firmware can be field updated, it requires specialized software tools and must be performed by authorized Woodward personnel. If you have any questions about this issue please refer to your installer, sales contact, or Woodward customer support for details.

Access Controls

Service Tools

The UG-25+ has a service tool called the “UG-25+ Governor Service Tool” that can be used to configure, tune, and troubleshoot the device. Using a laptop or PC with the UG-25+ Service Tool installed, users can connect to the device via the service port using a programming/datalink harness. The UG-25+ Service Tool includes optional password protection to provide security against tampering (See Passwords section for more information). Ensure that only Woodward or UG-25+ provider-approved tools are used to interact with the UG-25+. Refer to your installer, sales contact, or Woodward customer support for details

User Interface

The direct user interfaces for the UG-25+ are the panel on the front of the governor and/or a laptop or PC connected to the control with the UG-25+ Service Tool installed. Due to this, the security of the UG-25+ will rely on access controls of the physical system and controlling the input/output sent to the UG-25+. The UG-25+ does not support access control such as roles and passwords by default. Instead, password functionality is included in the UG-25+ Service Tool detailed below.

Passwords

The UG-25+ has no password protection by default, however, several settings of the UG-25+ control can be protected by a password that can be enabled in the UG-25+ Service Tool. To enable this feature, navigate to the Security tab in the UG-25+ Service Tool and check the Read Configuration security box. Once selected, the security password must be set. Only one password is used for all security selections and users will be prompted whenever a secured function is selected. Functions that can be secured with password protection are Configuration Load and Speed Dynamics Edit. Configuration Load protection makes it so that a user must provide the password before a configuration can be loaded into the control. The Speed Dynamics Edit makes it so that a user must provide the password before allowing tuning to the speed PID.

Selecting the Load Configuration File to Control option under the Run screen File in the Service Tool allows loading a configuration file to a control without opening it. Thus, a password protected configuration file can be downloaded without entering the password. However, if downloading a configuration to a control that already contains a configuration with password protection enabled for configuration loads, users will need to use that password.

If the Service Tool password is lost, contact the OEM for retrieval.

For more information on passwords and the UG-25+ Service Tool, refer to the UG-25+ Installation and Operation Manual, 26330, chapter 6.

Patching

The UG-25+ does not support patching. Instead, Woodward occasionally releases full, new firmware updates for controls that add new or updated functions. The UG-25+ firmware is to be installed only by authorized Woodward personnel.

Contact your Woodward sales or support contact for further information.

Policies and Procedures

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

Zones and Conduits

Zones and conduits are not a direct cybersecurity mitigation tool, rather, they are used to analyze and partition the system to develop a defense in depth plan. A zones and conduits analysis can help define trust zones and the elements within those trust zones. Then the system owner can decide what mitigations are needed between zones to create Defense in Depth layers.

Monitoring and Detection

Monitoring and detection tools can help the user catch attackers; however, the UG-25+ does not have this capability built in. Any monitoring or detection should be at the next control level up (i.e. PLC or upper-level control module).

The UG-25+ has no intrinsic networking ports or external routable network interfaces (i.e. Ethernet) and has only non-routable system communications (non-routable communications include RS-485 Serial and CAN).

Chapter 4.
Attack Scenarios

Due to the UG-25+ having no external routable network interfaces and having non-routable system communications, the main attack scenario is through physical access to the control, as noted in the Physical Security section. If an attacker gains access to the prime mover where the UG-25+ is installed, they will have access to the User Interface Panel to directly manipulate the settings for speed, droop, load limit, or stability. The attacker can also plug a PC or laptop into the control using the service port and interfere with the UG-25+'s configuration if there is no Configuration Load password protection in place. This attack would likely involve changing settings in the service tool, re-programming the control, or installing a malicious firmware update using an unsecured PC or laptop to manipulate the control as the attacker sees fit.

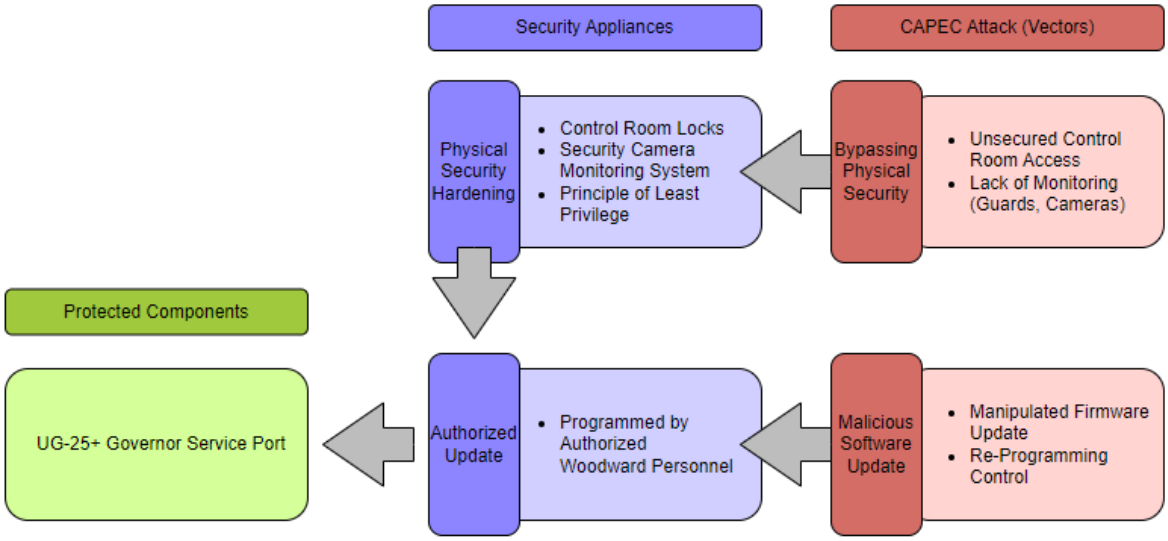

Figure 4-1. Potential Attack Vectors

Chapter 5.
UG-25+ Security Overview

UG-25+ Security Overview

The UG-25+ was not developed within a secure development life cycle process prior to the realization of current cybersecurity standards, and as such shall **not** be considered a cybersecure product. From a networking perspective, since the UG-25+ does not have any networking capabilities, the biggest risk to the product comes from unauthorized physical access to the device using an unsecure PC or laptop. A PC or laptop interacting with the control using the Windows operating system should include device hardening, elimination of unneeded services, malware / anti-virus protection, and user account management. As for physical accessibility, the UG-25+ should be located within a secure environment only accessible to authorized personnel. As such, the room and cabling shall be safeguarded to protect access. Use monitoring and detection techniques to identify unauthorized access to the environment the control resides.

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 of the UG-25+. Examples of these actions range from simple human error up to and including malicious attacks resulting in damage to the UG-25+ and damage to equipment connected to the UG-25+.

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.
- Provide security updates in the next firmware update.

Customers can report security problems through Woodward customer service or by sending an email to cybersecurityhelpdesk@woodward.com.

Firmware Upgrade

Woodward and/or UG-25+ application developers occasionally release firmware updates after product release to fix functional issues. UG-25+ firmware updates may only be installed by authorized Woodward personnel. Firmware update notifications are available on the Woodward product support web site at https://www.woodward.com/support/industrial-support/.

Chapter 6.
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:
https://www.woodward.com/en/support/industrial/service-and-spare-parts/find-a-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 (Woodward North American Terms and Conditions of Sale 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 North American Terms and Conditions of Sale 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 North American Terms and Conditions of Sale 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 North American Terms and Conditions of Sale 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 (51) 636-7080
Poland	+48 (12) 295 13 00
United States	+1 (970) 482-5811

Products Used in Engine Systems

Facility	Phone Number
Brazil	+55 (19) 3708 4800
China	+86 (512) 8818 5515
Germany	+49 (711) 78954-510
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+82 (51) 636-7080
The Netherlands	+31 (23) 5661111
United States	+1 (970) 482-5811

Products Used in Industrial Turbomachinery Systems

Facility	Phone Number
Brazil	+55 (19) 3708 4800
China	+86 (512) 8818 5515
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+ 82 (51) 636-7080
The Netherlands	+31 (23) 5661111
Poland	+48 (12) 295 13 00
United States	+1 (970) 482-5811

Technical Assistance

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

General

Your Name _____

Site Location _____

Phone Number _____

Fax Number _____

Prime Mover Information

Manufacturer _____

Turbine Model Number _____

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

Power Output Rating _____

Application (power generation, marine, etc.) _____

Control/Governor Information

Control/Governor #1

Woodward Part Number & Rev. Letter _____

Control Description or Governor Type _____

Serial Number _____

Control/Governor #2

Woodward Part Number & Rev. Letter _____

Control Description or Governor Type _____

Serial Number _____

Control/Governor #3

Woodward Part Number & Rev. Letter _____

Control Description or Governor Type _____

Serial Number _____

Symptoms

Description _____

_____

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

Revision History

Changes in Revision —

- New manual

Released

We appreciate your comments about the content of our publications.

Send comments to: industrial.support@woodward.com

Please reference publication 35241.

B 3 5 2 4 1 : -

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.