WOODWARD

Product Manual 35244
(Revision -, 02/2025)
Original Instructions

EasYgen-3000XT Series Genset Control Security Manual

Security Manual

General Precautions

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

Practice all plant and safety instructions and precautions.

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

Revisions

This publication may have been revised or updated since this copy was produced. 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— A bold, black line alongside the text identifies changes in this publication since the last revision.

Manual 35244

Contents

WARNINGS AND NOTICES **3**

ELECTROSTATIC DISCHARGE AWARENESS **5**

REGULATORY COMPLIANCE **6**

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

CHAPTER 2. INDUSTRIAL CYBER SECURITY BASICS **8**
Introduction 8
What is Cybersecurity? 8
Hardening 8
Where does the easYgen-3000XT Series exist in an OT network? 9

CHAPTER 3. DEFENSE-IN-DEPTH (DID) **10**
Physical Security 11
Access Controls 11
User Interface 11
User Accounts 12
User Account Levels 12
Passwords 14
Denial of Service (DoS) Protection 15
External Interfaces 15
Ethernet Interfaces 15
USB Interface 15
CAN Bus Interfaces 15
Malware Prevention 16
Ports 16
Default Open Ethernet Ports 16
Network Security 16
Monitoring and Detection 17
Patching 17
Decommissioning 18

CHAPTER 4. ATTACK SCENARIOS **19**

CHAPTER 5. SECURITY REFERENCES **21**
How are users notified if a security issue has been discovered? 21
How can users ask questions about security or report security issues to Woodward? 21

CHAPTER 6. PRODUCT SUPPORT AND SERVICE OPTIONS **22**
Product Support Options 22
Product Service Options 22
Returning Equipment for Repair 23
Replacement Parts 24
Engineering Services 24
Contacting Woodward's Support Organization 24

TECHNICAL ASSISTANCE **25**

REVISION HISTORY **26**

Illustrations and Tables

Figure 1-1. Purdue Model 9
Figure 2-1. Defense in Depth Diagram 10
Figure 3-1. Potential Attack Vectors 19

Table 1-1. CPU Information 7
Table 1-2. Glossary of Terms and Abbreviations 7
Table 2-1. Code Levels and Permissions 13

Warnings and Notices

Important Definitions

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

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

⚠WARNING

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, European Union, International, and Marine compliance, refer to the Approvals section (section 8.1.8) of Woodward Manuals:

Manual Number	Manual Description
B37574	easYgen-3000XT Technical Manual for easYgen-3100XT/3200XT-P1
B37580	easYgen-3000XT Technical Manual for easYgen-3400XT/3500XT-P1
B37581	easYgen-3000XT Technical Manual for easYgen-3400XT/3500XT-P2

Additional manuals may be available at www.woodward.com. Navigate to Support > Industrial Support > Manuals, Software, and License Keys.

Special Condition for Safe Use

The easYgen-3000XT Series of Genset Controls were 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 easYgen-3000XT Series of Genset Controls. The manual covers security configurations, user access information, decommissioning, and security alert reporting and notification.

Scope

This manual covers the easYgen-3000XT Series of Genset Controls (3100, 3200, 3400, 3500).

CPU Information

Table 1-1. CPU Information

EasYgen-3000XT Series

CPU #	Preferred	Secure Passwords	Achilles Cert	SSH/ Firewall	ToolKit
1681-1846	Yes	Yes	No	No	Yes

References

Refer to the Regulatory Compliance section for a list of relevant manuals.

Glossary

Table 1-2. Glossary of Terms and Abbreviations

CAN	Controller Area Network
DDoS	Distributed Denial of Service
DiD	Defense in Depth
DoS	Denial of Service
Harden	The practice of reducing a systems vulnerability by reducing its attack surface
IACS	Industrial Automation Control Systems
ICS	Industrial Control System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
OT	Operational Technology
SCADA	System Control and Data Acquisition
SNTP	Simple Network Time Protocol
VNC	Virtual Network Computing

Chapter 2.
Industrial Cyber Security 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, making them 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 difficult to locate or be accessed by maintenance staff. Ensuring cybersecurity of an OT system requires knowledge, diligence, and team wide collaboration. Following the guidelines in this manual can help mitigate the risk of a cybersecurity attack happening as well as help mitigate the extent of damage caused.

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):

- Tampering with logs to hide attack activity.
- Flooding the Ethernet connections with data to disrupt communications with the operator.
- Invalid sensor data that could cause unstable operation of the system.
- Someone tripping over a cable and unplugging a critical component.

Hardening

An important aspect of securing a system mentioned in this manual is the concept of “hardening”. Hardening refers to the practice of reducing a system’s vulnerability by reducing its attack surface. One of the goals of this manual is to help control owners harden their system and components that connect to their system to reduce the chance and impact of a cyber-attack. Following the defense-in-depth guidelines in this manual and configuring the easYgen-3000XT Series Genset Control appropriately will aid in establishing a security hardened system and a stable and secure operating environment.

Where does the easYgen-3000XT Series exist in an OT network?

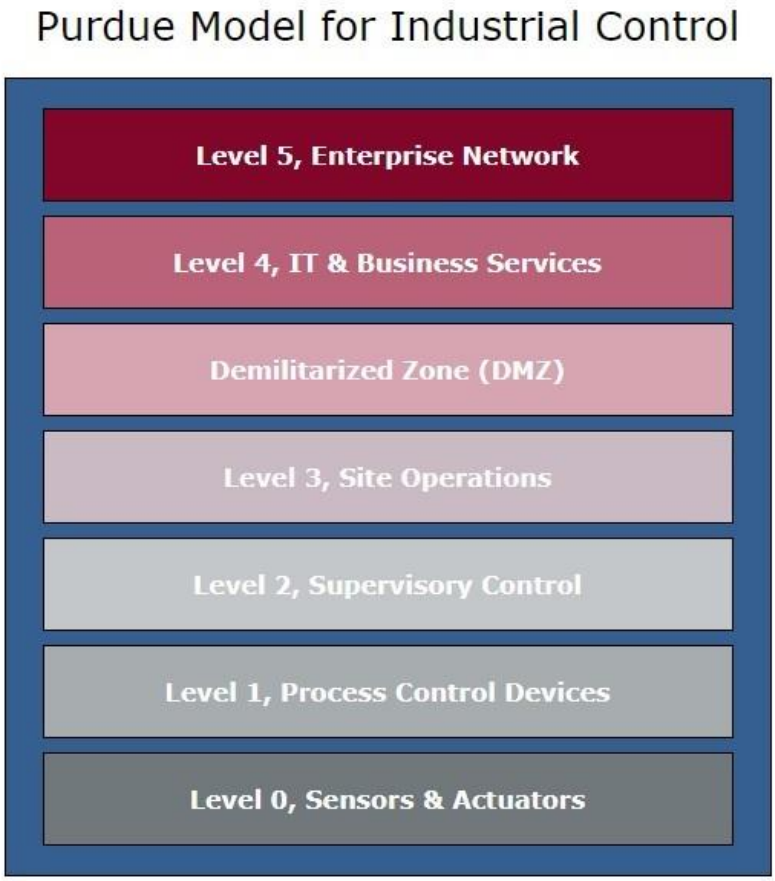

Figure 1-1. Purdue Model

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 includes SCADA 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 that is required to maintain control of the process.

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

The easYgen-3000XT Series of Genset Controls lives at level 1 of the Purdue model illustrated in figure 1. Operators at level 2 can communicate with the control. Devices at level 0 are accessed by the control as inputs and outputs.

Chapter 3.
Defense-in-Depth (DiD)

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

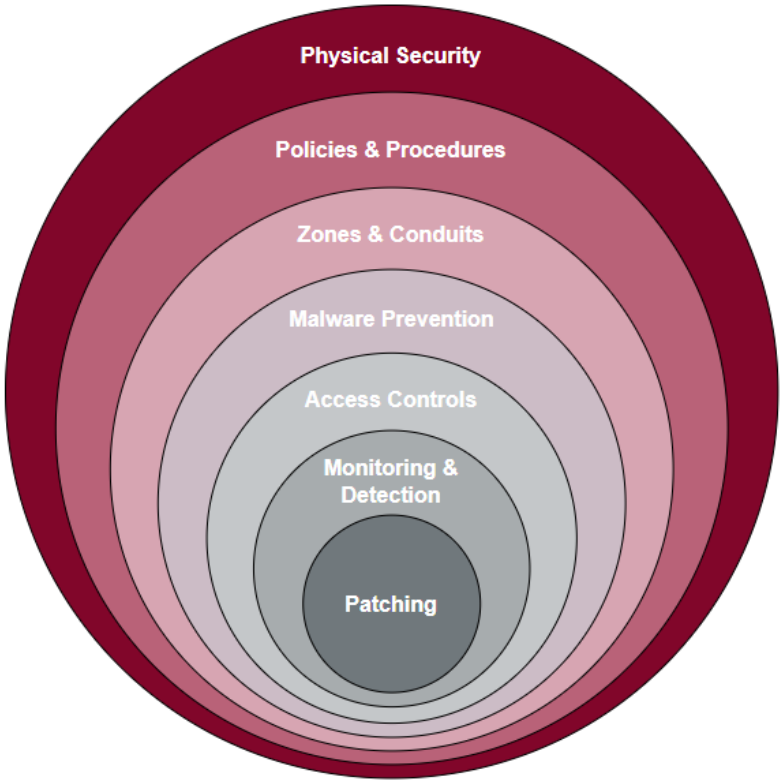

Figure 2-1. Defense in Depth Diagram

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 ensure that threats are stopped before the easYgen-3000XT Control is compromised.

Woodward DiD recommendations for secure easYgen-3000XT installations include:

- Updating default passwords to more secure passwords
- Ensure that users only receive passwords and access to the Code Level (permissions level) they need to carry out their job functions.
- Maintain physical security. Limit physical access to only authorized and trained personnel. Log who enters the control area and why.
- Minimize external Ethernet connections to HMI's, Engineering Workstations and the easYgen.
- Windows-based PCs represent a significant attack vector for an industrial control system. Consider using hardened PC's or thin client servers for these applications (see User Interface section for details on securing PC's).
- Ensure that the OS on any PC connected to the control system is part of a regular patch management program.
- Ensure that any other network element, such as switches and firewalls, that are used in external Ethernet connections are hardened devices and are properly configured and updated for any known vulnerabilities.

The easYgen-3000XT Series 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. However, there are many things that owners can do to create a more secure environment for the easYgen-3000XT Series.

Physical Security

Physical security refers to the physical protection that is put in place to protect the easYgen control. This security can include electronic door locks, authenticated entry, fences, closed-circuit cameras, guards, signage, motion sensors, etc. Physical security devices must notify the appropriate personnel of access in a timely manner so action can be taken if needed. Speed is important when dealing with an attack so the earlier the warning occurs and is reported, the better. Physical security requirements can vary depending on the environment in which the easYgen is being used.

The easYgen-3000XT is a mounted control, usually on a panel inside a cabinet or directly on a cabinet surface. To prevent an attacker from accessing the control, only approved personnel must be allowed access to the area where the cabinet and control are located. Create a method or procedure to alert operators when the cabinet and/or its environment have been accessed.

The cabling attached to the control must also be physically protected. Physical damage to the cabling can cause instability of the equipment controlled by the easYgen and damage to the control 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. Communication between equipment can be corrupted, lost, or shorted to each other or ground, causing damage or instability. Cables can also be tapped into. An attacker could supply false or inaccurate data using an unprotected cable. Sensors and outputs must be similarly protected from access to prevent a false context for engine operation and control.

In some applications, the easYgen has no HMI and is mounted in a locked cabinet. In this configuration control of the easYgen is through remote panels RP-3000XT or easYview which can be located on the outside of the cabinet or mounted further away. The same security procedures should be followed when protecting the cabling, service ports and physical safety of the RP-3000XT and easYview remote panels (see User Interface section for more information).

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.

Access Controls

Service Tools

The easYgen-3000XT Series uses Woodward ToolKit to allow users to change settings on the control using a PC. ToolKit can be used to create and run custom administration tools for many Woodward electronic products. ToolKit can be installed via CD or downloaded on a laptop or PC, then connected to the easYgen to configure, calibrate, monitor, and troubleshoot the device over a serial, CAN, or TCP/IP connection.

Ensure that only Woodward or easYgen provider-approved tools are used to interact with the easYgen. See the User Interface section of this manual for more details on making the connected PC secure.

For the current PC Requirements and more information for configuring ToolKit, refer to Woodward manual B37917, Toolkit Manual for easYgen-3000XT Series

User Interface

Users can interface with an easYgen control in several ways. Users that have access to the environment where the easYgen is installed can manipulate it by physically interacting with the control’s HMI screen or front panel access buttons. Front panel access buttons can be disabled by ToolKit with parameter “Lock keypad.”

There is a “Headless” version of easYgen that has no HMI built onto the control. In this configuration, the easYgen-3000XT is usually locked in a cabinet and changes to the control are made using remote panels connected via cables. Internally, this version has the same software for HMI setup as the non-headless easYgen-3000XT. The only difference is that on the headless easYgen, the HMI is drawn into internal memory and is accessed using VNC rather than a real HMI.

The easYgen-3000XT Series can be remotely controlled by remote panels called the easYview and the RP-3000XT. The RP-3000XT is at End of Life as of June 28, 2024, and has been replaced by the easYview, a drop-in replacement of the RP-3000XT. Configurations using these panels are set up with Ethernet and switches to allow a remote panel to control multiple easYgens or multiple remote panels to control a single easYgen. Physical security best practices such as locking and monitoring the environment where the control or remote panels live can prevent attacks.

EasYgen controls can also be configured by users using a Windows laptop or PC with Woodward ToolKit installed. This PC can be connected to the control using either the USB (preferred) or Ethernet service ports. PC’s running the Windows operating system provide easy attack paths, so any PC that accesses the control must be hardened. To harden the security posture of a PC or laptop, ensure that all the most recent patches and security updates have been installed, all unneeded services are disabled, the PC has been scanned using malware/anti-virus protection, and user accounts with appropriate permissions are in place.

Woodward recommends the following security measures for PC’s and laptops that connect to an easYgen-3000XT control:

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

Some settings can also be changed by the customer via Modbus, Modbus/TCP, and CANopen. These settings are password protected using the code levels in Toolkit. For more information on code levels, refer to the user account levels section.

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

User Accounts

The easYgen-3000XT Series utilizes a password protected multi-level access hierarchy through Code Levels to prevent unauthorized access to parameters, configuration, and calibration items. This allows varying degrees of access to the parameters by assigning unique passwords to each Code Level then giving that password to designated personnel. When assigning passwords to users, limit access rights of each user to the minimum level necessary to perform job functions.

User Account Levels

Users can log in at any of the levels listed in the following table if they provide the basic code entry or user account entry and password. The higher the code level, the more permissions the user has. The already existing usernames cannot be changed and are fixed for the desired code level.

Basic Code Entry is used to access Code Levels using an easYgen HMI, and User Account Entry is used with ToolKit when connecting to the control over USB (preferred) or Ethernet. The following table provides information on the code levels and the permissions each provide.

Table 2-1. Code Levels and Permissions

Code Level	User Account Entry: Username	User Account Entry: Password (Default)	Basic Code Entry: Password (Default)	Permissions
5	CL05	CL0500	500	**The Super Commissioning Level** Access to nearly all parameters of configurations, excluding calibration and super user items. Users own code level, and the levels below can be indicated and configured.
4	AC04	Algorithm Code*	Algorithm Code*	**The Temporary Super Commissioning Level** Has the same rights as Super Commissioner but has the following exceptions: • The password for this level is not visible. • Access is dismissed afterwards.
3	CL03	CL0003	3	**The Commissioning Level** Access to well defined parameters and configurations, which are usually needed on a commissioning level. Users own code level, and the levels below can be indicated and configured.
2	AC02	Algorithm Code*	Algorithm Code*	**The Temporary Commissioning Level** Has the same access rights as Commissioner Level but with the following exceptions: • The password for this level is not visible. • Access is dismissed afterwards.
1	CL01	CL0001	1	**The Basic Level** Access to a limited number of parameters and configurations.

				Users own code level can be indicated and configured.
0	None	None	None	Using HMI: No access rights to change or view information. Using ToolKit: Users at this level may view settings but cannot reconfigure them.

*The algorithm code is an implemented procedure to give temporary access to the device at a certain Code Level without the user being able to see or change the corresponding password.

Users are automatically logged out (moved to Code Level 0) from their current code level after 2 hours or during power supply cycling. Communication between ToolKit and the control will never automatically logout.

Users are forced logged out (moved to Code Level 0) when users input an incorrect password or use the Toolkit logout function.

Passwords

Passwords can be changed for each code level equal to or below the level of the account the user is currently logged into. It is recommended that the owner of the control changes all default passwords of all accounts using ToolKit once the control is installed to prevent unauthorized access or manipulation of the easYgen's settings.

Users with access to Code Level 5 have the ability to issue certain flash updates. As such, changing the password and limiting the users who have access to this account is important.

Parameter	Required Code Level	Description
Basic Level – Change Password	1	Allows user to change password for Code Level 1
Commissioner Level – Change Password	3	Allows user to change password for Code Level 3
Super Commissioner Level – Change Password	5	Allows user to change password for Code Level 5

Default passwords can be restored with the proper code level; however, if the password for the Super Commissioning level (5) is lost or forgotten, the code level to execute the default password reset will need to be provided by a Woodward sales support partner.

Parameter	Required Code Level	Description
Reset Default Password – Basic Level	2	Resets Password to "CL0001"
Reset Default Password – Commissioner Level	4	Resets Password to "CL0003"
Reset Default Password – Super Commissioner Level	11	Resets Password to "CL0005" (Requires Woodward Sales Support Partner)

Refer to section 4.3.4.1 of Woodward Manuals B37574, B37580, and B37581 for more details on the ToolKit password system for easYgen.

Denial of Service (DoS) Protection

Denial of service attacks occurs when a constant flow of data is sent to the easYgen's communication ports. This can cause the control to slow down substantially or even crash. This flow of data can consist of a combination of both valid and malformed requests at such a high rate that the port cannot resolve the requests in a timely manner. DoS attacks can occur on the Ethernet and CAN interfaces of the easYgen-3000XT Series. The easYgen does not have integrated capabilities to deal with these attacks so it is up to the system and/or controller network to implement real-time monitoring and Deep Packet Inspection (DPI) of network traffic to deter this attack and help mitigate cyber risks.

External Interfaces

The easYgen-3000XT Series has several interfaces that should be considered for security. The following is a list of interfaces found on the controls.

- Ethernet Interface (RJ-45) LAN A
- Ethernet Interface (RJ-45) LAN B (easYgen 3400XT and 3500XT only)
- Ethernet Interface (RJ-45) LAN C (easYgen 3400XT and 3500XT only)
- USB Interface (2.0, Read-Only) Service Port
- CAN Bus Interface CAN #1
- CAN Bus Interface CAN #2
- CAN Bus Interface CAN #3 (easYgen 3400XT and 3500XT only)
- RS-485 Interface #1

Ethernet Interfaces

Ethernet interfaces on the easYgen should only be used to provide fast communication to other devices like other easYgens, remote panels, PLCs, or SCADA systems. Do not use the Ethernet ports to connect the easYgen directly to the Internet (see Remote Gateway section for information on connecting to and securing remote communication gateways). Do not use the ethernet ports to connect to a laptop or PC that is connected to the Internet. Ethernet interfaces are susceptible to DoS attacks, so monitoring and detecting traffic of these ports is recommended. If available, use RJ-45 caps to protect ports that are not in use.

USB Interface

The USB interface on the easYgen-3000XT Series is a service port used to connect the control to ToolKit. For all other connections besides ToolKit, the USB interface is read-only. Physically protecting the area that the control is installed in can protect the USB port. Preventing unauthorized access to the control and using monitoring and detection strategies can reduce the chance of someone attempting to use the USB port as an attack vector. If available, use USB port caps to protect ports that are not in use.

CAN Bus Interfaces

Each of the CAN Bus Interfaces on the easYgen-3000XT operates with a different level of the control. CAN Interface 1 (Guidance Level) is a freely configurable CANopen interface. CAN Interface 2 (Engine Level) supports connection of a wide range of ECUs and J1939 analog input extension modules. The easYgen-3100XT and easYgen-3200XT Series only supports CAN interface 1 and 2. EasYgen-3400XT and 3500XT also have CAN Interface 3 (System Level), which is used for load sharing and communication with CAN devices like the LS-5 or LS-6XT circuit breaker control units. As with the other external interface ports on the easYgen, utilizing physical security best practices along with monitoring the room the control is installed in and detecting unauthorized user access can prevent manipulation of CAN bus interfaces.

Malware Prevention

Every effort must be made to ensure that any software or firmware loaded to the easYgen is authentic Woodward or application developer software. Utilize methods such as hashing and signatures to help ensure authenticity of software. A likely source of malware is the Window's PC or laptop that can connect to the easYgen to adjust settings using the ToolKit service tool. Consider the security of this PC and harden it to prevent malware from being introduced to the control. See the User Interface section for more information on PC hardening.

Ports

Disable communication ports that will not be used. Leaving unused ports open creates more access points for an attacker. Regularly scan the device to check for open ports that do not have a documented, reviewed, and approved business case, and reconfigure any that are found to make them unavailable.

Default Open Ethernet Ports

Below is a list of commonly used Ethernet ports on the easYgen-3000XT Series and applications interfacing with external devices. Not all ports listed may be in use for a particular application.

Port Number	Service
20, 21	FTP
123	SNTP
502	Modbus
666	Servlink
667	AppManager
1010	Inter-Control Communications
1024	Inter-Control Communications
1805	Interconnect Mapper
5901	VNC-Server
17185	System Viewer

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

Network Security

The easYgen-3000XT Series contains routable protocols through its ports so network security must be considered. The easYgen should not be directly accessible from any public network, including the Internet. Networks are a common attack path for electronic controls that can be operated remotely. If the easYgen needs to reside in a network, make sure that the network is isolated, with no connection to the greater Internet. If the easYgen cannot be isolated from a public or insecure network, make sure that protection in the form of firewalls, secure remote gateways, and IDS and IPS equipment are in place to provide layers of security. These appliances are external to the easYgen but should be within the same security zone. Whenever the easYgen is connected to and exposed to an already existing Ethernet network, a network responsible person must arrange and allocate the IP addresses.

Remote Gateways

Some control owners may choose to hook up an easYgen-3000XT to a remote communication gateway to adjust functionality of the control remotely using a cloud-based service. When installing remote gateways, the owner and users should be aware of the security risks that are associated with placing the

components of an ICS on a network connected to the internet. Although many remote gateways detail a strong security posture, additional security considerations should be made.

Firewall rules need to be in place for any remote gateway that connects to a local network. Users must ensure that any remote communication gateway connected to an ICS has the latest software and firmware versions available from the manufacturer. Remote gateway traffic should be monitored with a plan in place to respond to attacks when they are detected. Some remote communication gateway companies supply monitoring and detection features. Limiting the number of computers that have remote access to the gateway and limiting access of these computers to only authorized personnel using group policy is recommended. Physically protecting the area in which a remote communication gateway resides is also important to prevent unauthorized manipulation of the gateway's settings.

SNTP Feature

The easYgen-3000XT Series can be usable as a SNTP (Simple Network Time Protocol) server within the local area network by its own IP address. This feature is set to internal clock by default, which disables SNTP functionality. EasYgen can also be set to Load Share mode where clock information is generated within the easYgen system. The final setting is for External SNTP-Server. It is not advised to enable External SNTP-Server unless the server and control are located within the same secure, segmented network with no outside access to the internet. Connecting the control to the internet introduces the risk of broadcast clients in the ICS getting disrupted by hostile external SNTP servers.

Monitoring and Detection

Monitoring and detection tools can help catch attackers. Ethernet-based communications should be passed through a firewall, IDS, and/or IPS to mitigate security risks. Communications sent through the CAN interfaces on the easYgen control must also be protected from DoS and adversary-in-the-middle attacks. Using redundant command strategies, such as CAN and analog demand together can help ensure that invalid commands are not sent to the control.

Alarm and Event Monitoring

The easYgen-3000XT Series supports the security practice of repudiation in the form of Alarm List and Event History. These logs allow Administrators to verify what specific actions were applied to the control and when those actions took place. The Alarm List will display a list of alarm messages which have not been acknowledged or cleared yet. Repeated alarms about a certain activity on the control may be due to an attack and should be responded to and investigated quickly. Event History displays a list of system events along with a timestamp of when the action occurred and if the condition was activated or de-activated. During or after an attack, Event History can help pinpoint the time an attack happened and the components or settings an attacker manipulated. Event History can hold up to 1000 events before the oldest messages start to be overwritten by new messages. Event History can be reset by users with the appropriate Code Level.

See section 9.5.4.1 and 9.5.4.2 of Woodward Manuals B37574 and B37581 for complete lists of Event Messages and Alarm Messages.

Patching

Woodward occasionally releases new software for controls that contain new or updated functions. These updates may also contain security updates required to keep the control secure. Users can flash update an easYgen-3000XT by connecting a security hardened PC with ToolKit and the appropriate configuration files installed to the control using Ethernet (preferred for updates). See User Interface section for PC security hardening recommendations. The system owner/operator should install released patches as soon as possible to prevent vulnerabilities from being exploited.

Patches can be released for boot-level firmware and/or application firmware. Application firmware patches may be supplied by Woodward or the application developer.

Note: When applying a software update to easYgen, the warning LED will blink rapidly to signal that the update is being applied to the control. If the device is shut down before the light has stopped flashing, the update will not be implemented, and the device will boot with the old software version. This can also result in damage to the control.

See Woodward manual 37630 for more information on the easYgen-3000XT update procedure or contact your Woodward sales or support contact for further information.

Decommissioning

When an easYgen-3000XT has reached end-of-life and is ready to be decommissioned, removing data from the control is recommended. This includes removing any potentially sensitive information from the control such as configuration information or personally identifiable information and restoring the control to factory default settings. Restoring the factory default settings will reset all parameters excluding customer defined passwords to their factory default values.

See section 4.3.5 System Management in manuals B37574, B37580, and B37581 for more information on restoring the easYgen to factory default settings.

Chapter 4.
Attack Scenarios

Figure 3-1 illustrates attacks vectors that could impact the availability and integrity of the easYgen-3000XT Series.

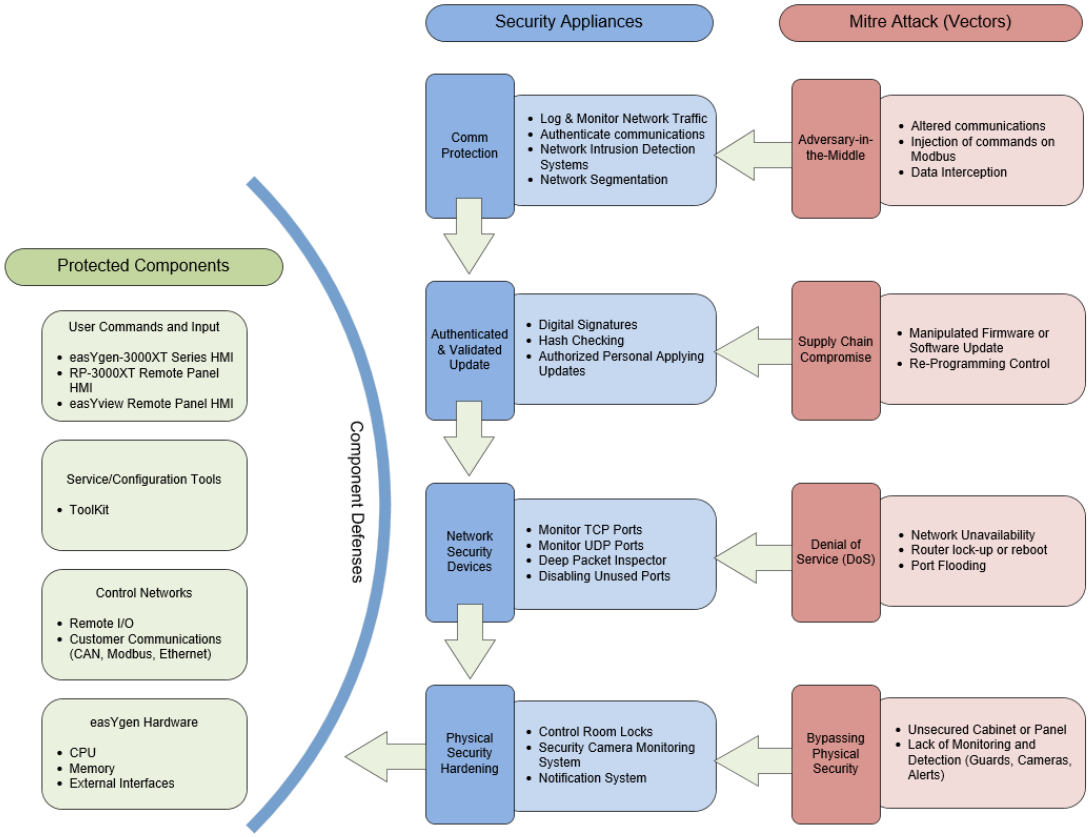

Figure 3-1. Potential Attack Vectors

An Adversary-in-the-Middle Attack (AiTM) can be achieved when an attacker intercepts communications that are sent to and from the control and allows them to block, log, modify, or inject traffic into the communication stream. This can lead to several problems. The attacker can capture and log information about the control system then use that information to inject new rules for the control causing unavailability and/or damage to the system. Modbus communications are particularly vulnerable to this type of attack due to the protocol being natively insecure. Data gateways, Field I/O, HMIs, and any other component of a system that sends and receives communications can all be targeted assets of an AiTM attack. AiTM attacks can be detected using logs and network traffic monitoring. Mitigations include authenticating communications to the control, network intrusion detection systems and segmenting the network the control is on.

A Denial-of-Service attack (DoS) is intended to attack a system's availability and prevent normal control functions and operations. The attack accomplishes this by either sending a high volume of requests in a short amount of time or sending a request that a control does not know how to handle. This attack usually targets routers and network adaptors but many externally facing interfaces can also be targeted. To combat DoS attacks and keep the easYgen functional, the system should include network appliances to detect intrusion, provide rate limiting, and provide deep packet inspection. These appliances will be external to the easYgen but should be within the same security zone.

A supply chain compromise is the manipulation of devices and/or software before the end customer receives it. It is important to be aware of this attack vector when applying patches and software updates to the control. A compromised file can be detected by verifying the binaries through hash checking, other integrity checking mechanisms, and scanning downloads for malicious signatures.

Bypassing physical security and being able to physically interact with the easYgen presents a large attack vector for the easYgen-3000XT. If an unauthorized user gains access to an easYgen or easYview remote panel and has knowledge of the control, there are many attacks the user can carry out. Preventing unauthorized access using control room locks, security camera monitoring, and limiting access to the area where the control resides to only authorized personnel can mitigate the chance of direct access and manipulation of the control. Hardening the defense posture of the easYgen by changing default passwords provides an additional layer of security in the case an attacker gains physical access to the control.

Chapter 5.
Security References

How are users notified if a security issue has been discovered?

When defects or vulnerabilities in Woodward control software are discovered, a corrective action committee reviews the issue. Typically, the NIST NVD will publish vulnerabilities prior to the availability of a patch or update. In these cases, or if a third-party component supplier is working to resolve the issue, the committee will publish a Woodward Application Note to www.www.woodward.com.

When a patch, update, or mitigation procedure is available and critical to the correct operation of the control system, the committee will create a service bulletin. The service bulletin will explain the problem and a suggested course of action and will be emailed to all Woodward product distributors and customers who have purchased or downloaded the product directly from Woodward.

How can users ask questions about security or report security issues to Woodward?

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 offer quick fixes to help minimize risk in the short term.
- Place security event notices on the Woodward product support web site.
- Schedule low priority fixes in the product patching schedule to provide security updates in the next service pack release.

Woodward has also established a help desk for security-related issues. Please email questions or reports to cybersecurityhelpdesk@woodward.com.

How are users notified about new releases?

GAP Coder version update notices are sent to Woodward distributers for dissemination to end customers.

The update notices list revisions to the product.

The Woodward website (www.woodward.com/software/) also lists all available software downloads, complete with revision descriptions.

Firmware Upgrade

Woodward and/or easYgen application developers occasionally release firmware updates after product release to fix functional and security issues. It is vital that updates be installed as soon as possible to keep the easYgen secure. Firmware updates are available on the Woodward product support website 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

Revision -

- New manual

Released

We appreciate your comments about the content of our publications.

Send comments to: industrial.support@woodward.com

Please reference publication 35244.

B 3 5 2 4 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.