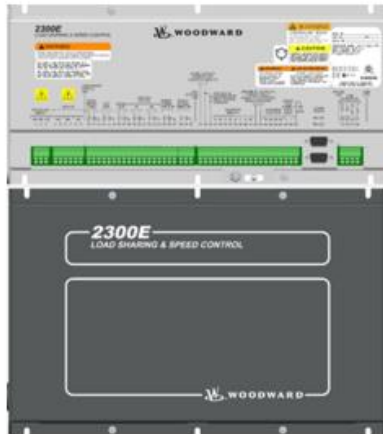




Product Manual 35243
(Revision -, 1/2025)
Original Instructions



2300E/2301E Digital Load Sharing and Speed 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.

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

Contents

| | |
|---|-----------|
| WARNINGS AND NOTICES..... | 3 |
| ELECTROSTATIC DISCHARGE AWARENESS | 5 |
| REGULATORY AND STANDARDS COMPLIANCE..... | 6 |
| CHAPTER 1. GENERAL INFORMATION..... | 7 |
| Purpose | 7 |
| Scope | 7 |
| References | 7 |
| Glossary | 7 |
| CHAPTER 2. INDUSTRIAL CYBER SECURITY BASICS..... | 8 |
| Introduction..... | 8 |
| What is Cybersecurity? | 8 |
| Hardening..... | 8 |
| Where Does the 2300E Series Exist in an OT Network? | 9 |
| CHAPTER 3. DEFENSE-IN-DEPTH (DID)..... | 10 |
| Physical Security | 10 |
| Service Tools | 11 |
| Configuring Your External PC | 12 |
| Denial of Service (DoS) Protection | 12 |
| Malware Prevention | 12 |
| External Interfaces | 12 |
| Policies and Procedures | 13 |
| Monitoring and Detection | 13 |
| Patching | 13 |
| CHAPTER 4. ATTACK SCENARIOS..... | 14 |
| CHAPTER 5. SECURITY REFERENCES..... | 15 |
| How are Users Notified if a Security Issue has Been Discovered? | 15 |
| How Can Users Ask Questions About Security or Report Security Issues to Woodward? | 15 |
| How are Users Notified About New Releases? | 15 |
| Firmware Upgrade | 15 |
| CHAPTER 6. PRODUCT SUPPORT AND SERVICE OPTIONS | 16 |
| Product Support Options | 16 |
| Product Service Options | 16 |
| Returning Equipment for Repair | 17 |
| Replacement Parts..... | 18 |
| Engineering Services | 18 |
| Contacting Woodward's Support Organization | 18 |
| Technical Assistance | 19 |
| REVISION HISTORY | 20 |

Illustrations

| | |
|--|----|
| Figure 2-1. Purdue Model | 9 |
| Figure 3-1. Defense in Depth Diagram | 10 |
| Figure 4-1. Potential Attack Vectors | 14 |

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 and Standards Compliance

For all hardware Regulatory Compliance including North America, Europe, International, and Marine compliance, refer to the Regulatory Compliance sections of Woodward manuals:

| Manual Number | Manual Description |
|---------------|--|
| 26641 | 2301E Digital Load Sharing and Speed Control for Engines Installation and Operation Manual |
| 26691 | 2300E Digital Load Sharing and Speed Control for Engines Installation and Operation Manual |
| 26694 | 2301E-ST Digital Electronic Load Sharing & Speed Control for Small Steam Turbines |
| 26818 | 2301E-J Digital Speed and Load Control |
| JA26818 | 2301E-J Digital Speed and Load Control (Japanese) |
| 35092 | 2301E-HT Hydro (Francis Turbines) |

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 2300E and 2301E 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 2300E series of Digital Load Sharing and Speed Control for Engines (2300E and 2301E). The manual covers security configurations, user access information, decommissioning, and security alert reporting and notification.

Scope

This manual covers the 2300E series of controls (2300E and 2301E). Both the 2300E and 2301E may sometimes be referred to as the 2300E. Unless stated otherwise, all information in this manual applies to both control versions.

References

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

Glossary

| | |
|--------|---|
| CAN | Controller Area Network |
| DDoS | Distributed Denial of Service |
| DiD | Defense in Depth |
| DoS | Denial of Service |
| Harden | The practice of reducing a system's vulnerability by reducing its attack surface. |
| IACS | Industrial Automation Control System |
| ICS | Industrial Control System |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| IT | Information Technology |
| OPC | Object linking and embedding for Process Control |
| OT | Operational Technology |
| SCADA | System Control and Data Acquisition |
| LON | Local Operating Network |

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 to 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 2300E series of controls appropriately will aid in establishing a security hardened system and a stable and secure operating environment.

Where Does the 2300E Series Exist in an OT Network?

Purdue Model for Industrial Control

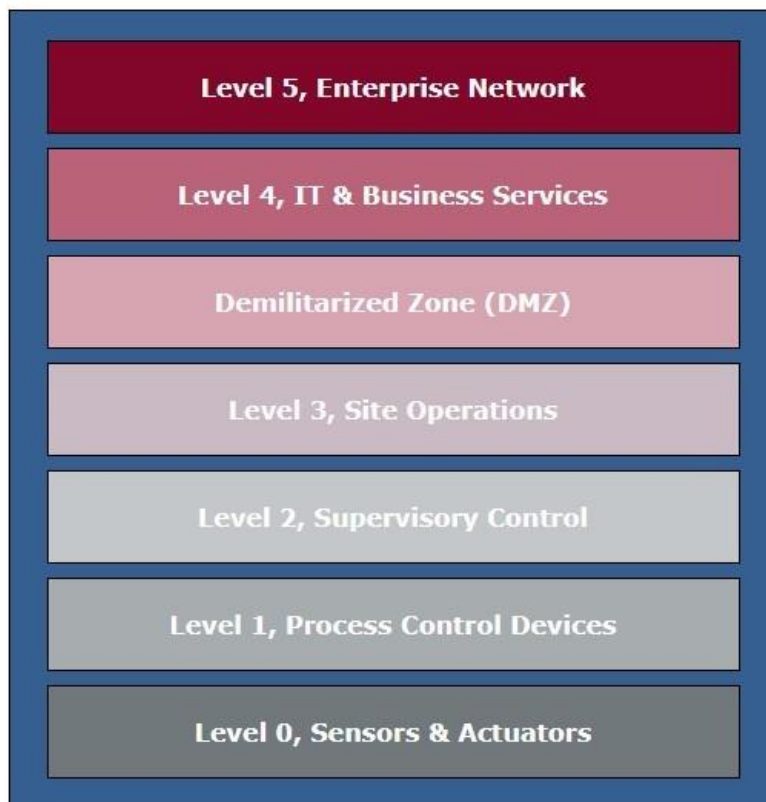


Figure 2-1. Purdue Model

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 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 HMIs.

Level 1 contains basic control equipment. These consist of complex controllers, PLCs, 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 2300E Series lives at Level 1 of the Purdue model illustrated in Figure 1-1. Operators at Level 2 can communicate with the control and 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.

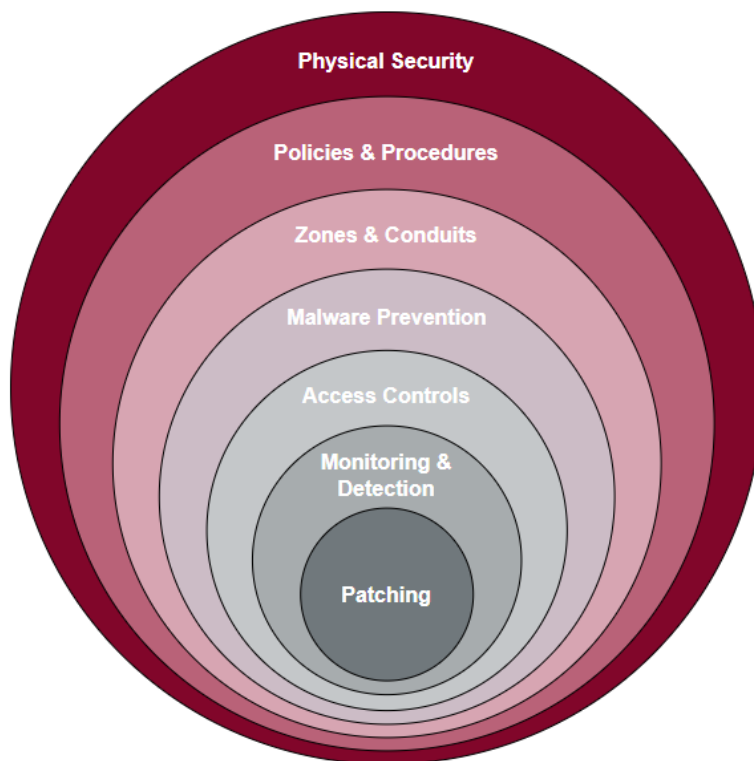


Figure 3-1. Defense in Depth Diagram

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 ensure that threats are stopped before the 2300E Series control is compromised.

The 2300E 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, due to the lack of routable protocols on the 2300E Series, a more secure installation is possible by following the Defense in Depth strategies in this manual.

Physical Security

Physical security refers to the physical protection put in place to protect a 2300E or 2301E 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 a 2300E Series is being used.

The 2300E Series is intended for installation in a closed electrical operating area or in an enclosed industrial control cabinet. 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 a 2300E Series must also be physically protected. Physical damage to the cabling can cause instability of the equipment that interacts with the control and damage to the actuator 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 the 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.

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.

Service Tools

The 2300E series of controls can be calibrated and monitored through either the 2300E/2301E Toolkit Service Tool, depending on the model, or the Control Assistant software. These tools can be downloaded to a computer or laptop from the Woodward website. Ensure that only Woodward-approved tools are used to connect with the 2300E Series. See “Configuring Your External PC” section for information on how to make computers that connect to the 2300E series of controls more secure.

Control Assistant – Woodward’s Control Assistant is a tool for service access to a control. It provides a means of shutting down and placing the control in the I/O Lock mode for Configuration, saving values in the control EEPROM, and resetting the control. Application tunable values can be uploaded, downloaded, and saved to a file.

PC Requirements for Control Assistant:

- Windows Vista, 7, 8, 10, 11
- .NET 4.6.2 Framework
- 1GHz or faster x86 or x64 processor
- 1GB of RAM
- Woodward’s SOS Servlink OPC Server version 4.15+

2300E/2301E Toolkit Service Tool – The 2301E Service Tool is used to configure, adjust, monitor, and troubleshoot a 2300E/2301E Load Sharing and Speed Control. This tool runs on a computer or laptop and communicates with the control through a serial connection. There are several versions of this tool based on the serial number of the 2300E/2301E control, so be sure to download the correct version.

PC Requirements for 2301E Toolkit:

- 1GHz or faster x86 or x64 processor
- 1GB of RAM
- Windows 2000, XP, Vista, 7 or greater

SOS Servlink – Woodward’s SOS Servlink OPC Server is a tool used to communicate OPC DA (Data Access) and OPC A&E (Alarms and Events) to client tools which know how to use it.

Example client tools:

- Monitor Gap
- Control Assistant
- Excel spreadsheets
- OPC-Ready HMI applications

PC Requirements for SOS Servlink:

- Windows Vista, 7, 8, 10, 11
- .NET 4.7.2 Framework

- 1GHz or faster x86 or x64
- 2GB of RAM

Woodward GAP 3.x & 4.x Software – Woodward's GAP 3.x and 4.x are Windows-based software programs that allow controls engineers to create block format application programs. The 2300E Series utilizes GAP software to create application specific software that can be downloaded to the control. Ensure that only authorized users have access to modifying the application software on the 2300E Series.

PC Requirements for Woodward GAP 3.x (Legacy Version):

- Windows Vista, 7, 8, 10
- .NET 4.6.2 Framework

PC Requirements for Woodward GAP 4.x:

- Windows Vista, 7, 8, 10, 11
- .NET 4.6.2 Framework
- 1GHz or faster x86 or x64 processor
- 1GB of RAM

Configuring Your External PC

Woodward recommends the following security measures for computers and laptops that connect to a 2300E Series control:

- Intrusion detection and 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
- Do not run NetMeeting in desktop sharing mode
- Do not run any unnecessary services

Denial of Service (DoS) Protection

The 2300E Series has no external routable network interfaces (i.e. Ethernet) and only uses non-routable system communications (CAN, Serial). Restricting physical access to the CAN network accessed by the CAN ports on the 2300E will prevent them from being used as a DoS attack vector.

Malware Prevention

While Woodward does not typically release upgrades for standard controls like the 2300E Series, every effort must be made to ensure that any software or firmware loaded to the 2300E Series is authentic Woodward or application developer software. While the 2300E Series software can be field updated, it requires specialized software tools and must be performed by authorized personnel. If you have any questions about this issue please refer to your installer, sales contact, or Woodward customer support for details.

External Interfaces

The 2300E Series has several interfaces that should be protected for security. These ports can be best protected through physical security and monitoring the environment in which the 2300E Series is installed. The following is a list of external interfaces found on the 2300E series of controls.

2300E:

- RS-232 Serial Communication Service Port
- RS-422 Serial Communication Port
- CAN Port 1

2301E:

- RS-232 Serial Communication Service Port
- RS-422 Serial Communication Port

Serial Interfaces

The 2300E Series has the same serial communication ports between models. The RS-232 Serial Communication Service Port is used to communicate with Control Assistant and Toolkit. The RS-422 Serial Communication Port is used for Modbus communication with distributed control systems or HMIs. Protect serial interfaces by utilizing physical security best practices.

2300E CAN Interface

The 2300E version of the control contains a CAN port for distributed I/O, distributed control, and HMI purposes, while the 2301E does not. As with the serial interface ports on the 2300E Series, utilizing physical security best practices along with monitoring the room in which the control is installed and detecting unauthorized user access can help prevent manipulation of CAN bus interfaces.

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.

Monitoring and Detection

Monitoring and detection tools can help catch attackers. On the 2300E Series, the connection for Control Assistant to the control will be through an RS-232 cable “null-modem” connection to the communication port, which is configured as a point-to-point only SOS Servlink OPC Server. This connection will allow users to locally view the Alarm and Events viewing from SOS servers/controls with AE (Alarm & Events) support when using Control Assistant to see when a change to the control was made and what the specific change was.

Utilizing the “WinPanel” in Control Assistant will allow live parameter monitoring.

Ensure that there is a plan in place to respond to threats and attacks after they have been detected. Detected threats should immediately notify security personnel, who can take the proper actions to contain the attack.

Patching

For a standard control like the 2300E Series, Woodward does not typically provide firmware releases for field upgrading. However, it is still possible for a firmware patch to be released so the 2300E Series can be re-flashed in the field using object files generated for the 2300E Series hardware platform. A misconfigured firmware update will cause the 2300E Series and the processes it controls to behave unpredictably. Due to this, field upgrading a 2300E Series should be done only if Woodward releases an official firmware update. If Woodward releases a firmware update, the system owner/operator should have an authorized person upgrade their control as soon as possible to prevent vulnerabilities from being exploited. Utilizing physical security best practices will help prevent an attacker from accessing the 2300E Series control to deploy a malicious update.

Chapter 4. Attack Scenarios

Figure 4-1 illustrates attack vectors that could impact the availability and integrity of the 2300E series of controls.

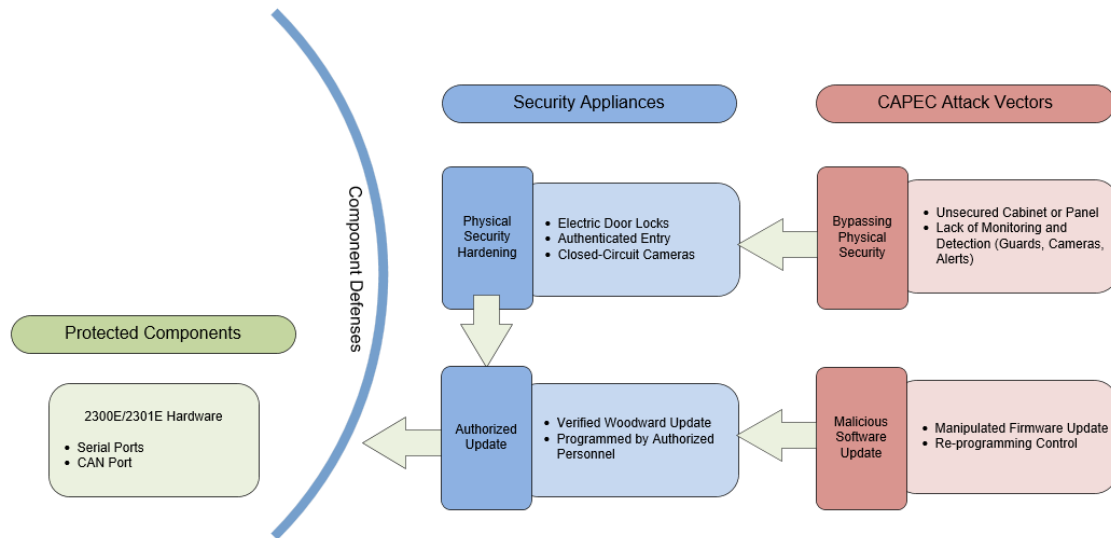


Figure 4-1. Potential Attack Vectors

Bypassing physical security and being able to physically interact with the 2300E/2301E is the main attack vector on the control. Due to the 2300E Series having no external routable network interfaces, an attacker will be unable to launch a remote attack on the 2300E/2301E control. However, direct physical access to the device will allow an attacker to cause damage or make the control behave unpredictably. Preventing unauthorized access using electronic door 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.

A **malicious software/firmware update** may be applied to the 2300E Series control. An attacker who makes it past physical security can plug a PC or laptop into the control using the service port and issue a flash update using a malicious firmware package. This attack can be prevented by making sure that only authorized users have access to the area where the 2300E Series control resides and verifying that firmware applied to the control is a genuine Woodward update. In the event of this attack being carried out, using the alarm and events log in Control Assistant can help to determine when the attacker acted and what changes they enacted on 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.woodward.com. Navigate to Support > Industrial Support > Manuals, Software, and License Keys > Manuals and Software > Application Notes.

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 affected Woodward customers.

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 distributors for dissemination to end customers.

The update notices list revisions to the product.

The Woodward website also lists all available software downloads, complete with revision descriptions. Go to www.woodward.com and navigate to Support > Industrial Support > Manuals, Software, and License Keys > Manuals and Software > Software.

Firmware Upgrade

Woodward and/or 2300E Series application developers may occasionally release firmware updates after a product release to fix functional issues. Firmware update notifications are available on the Woodward product support web site at www.woodward.com. Navigate to 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

| <u>Facility</u> | <u>Phone Number</u> |
|---------------------|---------------------|
| 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

| <u>Facility</u> | <u>Phone Number</u> |
|-----------------------|---------------------|
| 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

| <u>Facility</u> | <u>Phone Number</u> |
|-----------------------|---------------------|
| 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

We appreciate your comments about the content of our publications.

Send comments to: industrial.support@woodward.com

Please reference publication **35243**.



B 3 5 2 4 3 : -



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.