WOODWARD

Product Manual 35259
(Revision A, 8/2025)

Original Instructions

Atlas-II Digital Control

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 35259

Contents

Illustrations and Tables

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, European Union, International, and Marine compliance, refer to the Regulatory Compliance section of Woodward Manuals:

Manual Number	Manual Description
26415	Atlas-II Digital Control Installation and Operation Manual
35166	Atlas-II Digital Control Without LON Interface Installation and Operation Manual

Additional manuals may be available at www.woodward.com. Navigate to Service & Support > Industrial Service & Support > Manuals and Software.

Special Condition for Safe Use

The Atlas-II was developed without a secure development life cycle process and 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 Atlas-II Digital Control. The manual covers security configurations, user access information, decommissioning, and security alert reporting and notification.

Scope

This manual covers all variations of the Atlas-II Digital Control.

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
LON	Local Operating Network
OPC	Object linking and embedding for process control
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 attacks. In addition, personnel handling 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 Atlas-II appropriately will aid in establishing a security hardened system and a stable and secure operating environment.

Where does the Atlas-II exist in an OT network?

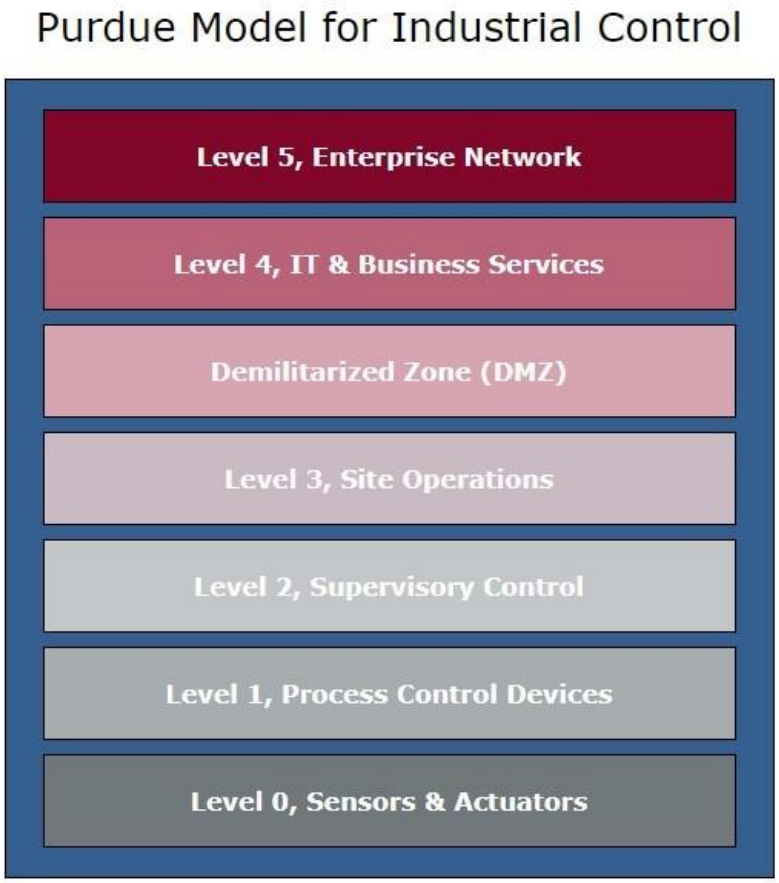

Figure 1-1. Purdue Model

The Purdue reference model illustrated above represents a typical OT network architecture. Level 5 represents the enterprise IT network and Level 4 represents services provided by IT.

The Industrial Demilitarized Zone (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 Atlas-II lives at Level 1 of the Purdue model illustrated in Figure 1-1. 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.

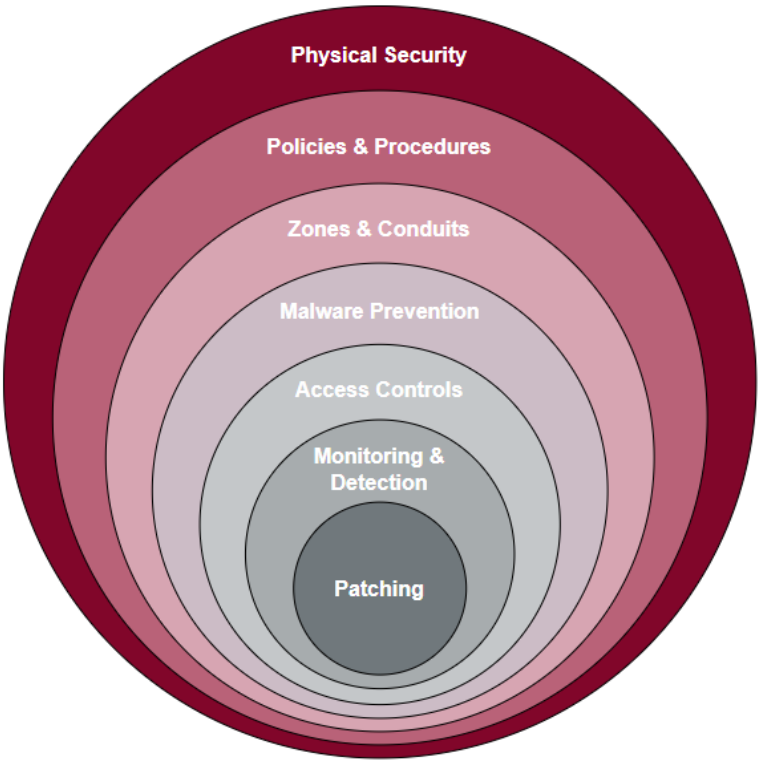

Figure 2-1. Defense in Depth Diagram

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 Atlas-II is compromised.

Woodward DiD recommendations for secure Atlas-II installations include:

- Updating default passwords to more secure passwords.
- Ensure that user levels are set correctly, and users are assigned to the lowest level required to perform their job functions.
- Ensure that each user assigns and maintains a secure password.
- 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 Atlas-II.
- 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 PCs).
- 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 Atlas-II series was developed without a secure development life cycle process and prior to the realization of current cybersecurity standards, and as such, shall not be considered a cybersecure product. However, there are many things that can be done to create a more secure environment for the Atlas-II Digital Control.

Physical Security

Physical security refers to the physical protection that is put in place to protect the Atlas-II control. This security can include electric door locks, authenticated entry, fences, closed-circuit cameras, guards, signage, motion sensors, etc. Physical security alarm devices must notify the appropriate personnel of unauthorized access in a timely manner so prompt action can be taken. Early warnings and swift responses are important when faced with an attack. Physical security requirements can vary depending on the environment in which the Atlas-II is being used.

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 Atlas-II 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.

The Atlas-II is designed for installation in a protective metal enclosure such as a standard 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.

HMI’s can be connected to the control to provide operator access and control of the application machinery without having direct physical access to the control. The same security procedures should be followed when protecting the cabling, service ports, and physical safety of connected HMI’s. See System Access Points - HMI section for more information on HMI’s.

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.

System Access Points

Service Tools

The Atlas-II is designed so that all interface, maintenance, and troubleshooting are done via serial and Ethernet ports. No local keyboard, monitor, or mouse is available to the user. With this “headless” set up, configuration and operation are accomplished using the following tools installed on a Window’s PC or laptop. See Configuring Your External PC for information on how to secure external PC’s connecting to the control.

For the current PC requirements of the Atlas-II service tools, please refer to the corresponding tool download page at www.woodward.com.

IMPORTANT

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

IMPORTANT **Woodward service tools will only work with the laptop connected to Ethernet Port 1 on the Atlas-II control.**

AppManager – Woodward's AppManager program is the user interface for managing applications and configuring security accounts on the control. On the Atlas-II control, AppManager can be used to load GAP Control software, monitor diagnostic faults, configure network settings (i.e. change Ethernet network addresses), administer accounts, and continuously retrieve datalog files. See Woodward Manual 26336, Woodward VxWorks RTOS Software Manual for more information on these features.

Monitor GAP – An Ethernet connection to the control allows online GAP monitoring, debug, and tunable configuration. Generally, service personnel use Monitor GAP for troubleshooting during the initial commissioning or subsequent system modifications.

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

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 compatible client tools.

Example client tools:

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

WinPanel – WinPanel is the replacement for the now-deprecated Watch Window tool and is a part of the Control Assistant tool. WinPanel allows read and write access to variables through SOS, and loading and saving of different configurations.

Current Versions

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

Component	Type	Part No.	Version
AppManager	Software Application	9927-785	3.#
Control Assistant	Software Application	9927-1237	4.##
GAP Editor	Software Application	9927-2662	4.##
GAP Programmer	Software Application	9927-2101	5.##
SOS	Software Application	9927-1223	5.##

These versions and part numbers are subject to change. For the latest software versions available for download and PC requirement information, navigate to www.woodward.com > Service & Support > Software License.

HMIs

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

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

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

Configuring Your External PC

Woodward recommends the following security measures for computers and laptops that connect to an Atlas-II control:

- Intrusion Detection & Prevention systems
- Proxy servers
- Web filtering software
- Spam control
- IPSec VPN
- Two-factor authentication for Remote Connectivity
- Anti-virus on e-mail gateway, e-mail servers & internet gateway
- WPA2 encryption for wireless control and Wireless Intrusion Prevention
- Disable Remote Desktop functionality
- Do not run NetMeeting in desktop sharing mode
- Do not run any unnecessary services

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.

DCOM and OPC

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

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

Configuring DCOM Security
To view and edit DCOM settings, run the program dcomcnfg from the run menu of Windows:
1. Select Start from the taskbar (usually bottom left)
2. Select Run…
3. Type dcomcnfg and select OK

Disabling DCOM Access to SOS
One way to disable DCOM access to SOS is to disable DCOM for all applications on the PC. This is the most secure choice:
1. Right-click on Component Services / Computers / My Computer
2. Select Properties
3. Select the Default Properties tab
4. Uncheck Enable Distributed COM on this computer

To disable DCOM access just for SOS:
1. Right-click on DCOM Config / Woodward.ServLinkOpcDa.1
2. Select Properties
3. Select the Location tab and uncheck all the Run… checkboxes (notably Run application on this computer)

Remote Access Hardening
If remote access to SOS is required, SOS must be configured to require credentials (select Enable OPC security interface in the Security tab of the Options window). DCOM should be configured as securely as possible.

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

Access Controls

NOTICE **The passwords of all default accounts should be changed to enable security upon installation and periodically (at least annually) from then on.**

Password Manager Default Settings

The Atlas-II control comes pre-configured with three levels: Administrator, ServiceUser, and Datalog. The privileges granted to each level increase as the level increases. Due to this, it is important to only allow authorized users access to the Administrator and ServiceUser levels.

It is recommended that Administrators of the control change the default passwords. This can prevent unauthorized users with knowledge of the default passwords from logging in. See Administrator Tools section for more information on password management.

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

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

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

account is changed, AppManager may be updated to use a different set of credentials for these functions.

User Account Levels

Different user accounts may be assigned different security levels (0-15). This provides a way to differentiate authority levels of different users. Account levels are created and maintained by an administrator. When assigning a user to an account level, limit access rights of each user to the minimum level necessary for them to perform their job functions.

1. Security levels protect privileged functionality in AppManager and in SOS.
2. Higher levels contain all the authority of lower levels.
3. Gaps are left in the level map to allow the application program to create intermediate levels. Application-generated levels apply only to Servlink (SOS) functionality. See item 5 below, Servlink (SOS) Security.
4. AppManager ("Vx-Service") security levels.
   a. Level 0
      i) Commands:
         - Connect
         - Login
         - Logout
         - Change Password
      ii) Level "0" is not a recommended account level. However, when the password expires on an account with a higher level, its level becomes "0" until the account is reset, or the password is changed.
      iii) This is the lowest level.
   b. Level 1
      i) Commands:
         - Read Control information
         - Read files
         - Explore module information
         - Explore RTN information
      ii) This is the minimum level for automatic Datalog retrieval feature.
      iii) This is the level of the default account "Datalog".
   c. Level 11
      i) Commands:
         - Write files
         - Delete files
         - Start applications
         - Stop applications
         - Stop automatic application start ("Clear Autostart")
         - Reboot control
         - Execute control service packs
         - Execute module service packs
         - Change network configuration
      ii) This is the level of the default account "ServiceUser"
   d. Level 15
      i) Commands
         - View accounts
         - Add account
         - Delete Account
         - Reset Account
      ii) This is the level of the Administrator account.
      iii) This is the highest level of privilege.
5. Servlink (SOS) Security – Systems with SSH encryption only:

a. Servlink security levels apply to reading and writing application values. They also apply to Servlink commands executed by SOS, such as Set Control Identifier, Reset and Shutdown.
b. Applications compiled for the Atlas-II have a default security configuration, which is recommended. It is possible to override this configuration by modifying parameters in the SYS_INFO block of the application (see SYS_INFO in the GAP Block Help). These parameters are fixed at application build time and can't be modified on-line.
c. Levels (**Note:** All default levels listed below only apply if not specified in SYS_INFO block):
   i) Default read security ("SYS_INFO.RD_SEC")
      - Default level: 4
      - Any value in the application without a specified read security level is given this level.
      - To override the default read security level for a value, the GAP application may be modified to connect an HMI_PT or HMI_ENUM block to the value. (See HMI_PT and HMI_ENUM in GAP – "Block Help" under the "Help" tab.)
   ii) Default write security ("SYS_INFO.WR_SEC")
      - Default level: 7
      - Any value in the application without a specified write security level is given to this level.
      - To override the default, write security level for a value, the GAP application may be modified to connect an HMI_PT or HMI_ENUM block to the value. (See HMI_PT and HMI_ENUM in GAP – "Block Help" under the "Help" tab.)
   iii) Browse security ("SYS_INFO.BROWSE_SEC")
      - Default level: 2
      - This is the authorization level required to browse the namespace of a Woodward control. The Control Assistant tool uses browsing to create the value tree shown at the left of the WinPanel. Other OPC client tools require this functionality to display available control values.
      - In some circumstances, it may be desired not to reveal the namespace (a map of all the value names in the application), but still provide access to some values through an HMI tool. The HMI tool can be configured using enough security to browse the namespace (e.g. by a developer with high authority) but can be run with less security (e.g. by an operator with limited authority).
   iv) Control read security ("SYS_INFO.CTL_RD_SEC")
      - Default level: 1
      - This is the authorization level required to read control information strings like the configuration ID.
   v) Control write security ("SYS_INFO.CTL_WR_SEC")
      - Default level: 7
      - This is the authorization level required to write control information strings like the configuration ID. It is also required for saving changes to non-volatile memory.
      - This level is required for uploading a control configuration.
      - Control start/stop security ("SYS_INFO.CTL_SS_SEC")
      - Default level: 11
      - This is the authorization level required to perform a shutdown or reset. This level is also required to change the control ID string.
      - Since this parameter control functionality in Servlink (Shutdown, Reset) which is very similar to AppManager functionality in level 11 (Stop, Start), it is recommended to leave this value at "11" in Atlas-II controls. However, this is not required.

Changing User Passwords

User passwords can be changed for the Atlas-II in AppManager by following these steps:

1. The account must be connected using the AppManager tool (for more information, use the Help drop down menu in AppManager and select "Help").
2. Use the Change Password command in the AppManager tool.

Note: The Account Name parameter for default accounts cannot be changed.

When selecting a new password, be aware that there are rules regarding password expiration and password length and characters:

1. Password Expiration
   a. Some user accounts may be configured by the Administrator to expire after the same password has been in use for a specified duration.
   b. When the password expires, the level of the account will be set to the minimum authority level, “0”, and the user will be prompted to change the password when they next attempt to log in through AppManager.
   c. If the password has expired, it is still possible to connect and change the password which starts a new expiration period.

2. Password Rules
   a. The new password must be different from the previous password.
   b. The password must be between 6 and 30 characters in length (inclusive).
   c. The password must contain at least 2 alpha (A-Z, a-z) and 2 non-alpha (0-9, !, @, #, etc.) characters.
   d. Passwords are case sensitive.

Administrator Tools

Administrator accounts have functions in AppManager that are not available to other account levels. For more complete instructions, in AppManager select the “Help” drop down menu and select the help option. In the help menu, click the search tab and search for Administrator Accounts.

The following functions are available to Administrator Accounts:

1. Creating New Accounts
   a. Account Name
      i) The account name must be unique.
      ii) The account name must be between 4 and 30 characters in length (inclusive).
      iii) The account name may consist of any combination of alpha (A-Z, a-Z) or non-alpha characters (0-9, !, @, #, etc.).
   b. Password
      i) The Administrator may specify an initial password or a fixed password.
      ii) The password must comply with the password requirements (see Changing User Passwords section).
   c. Level
      i) Any level between 0 and 14 (inclusive) may be specified.
      ii) Level 15 is reserved for the Administrator account, of which there may be only one.
   d. Password Duration
      i) The password duration may be set to any number of days after which the password will expire.
      ii) Since users may not change the password, it is the Administrator’s responsibility to periodically review and possibly change the password of these accounts.
      iii) If an account is given a fixed password and a non-zero expiration, the account may expire and require an Administrator’s intervention to provide a new password before the account is returned to full functionality.
2. Temporary Accounts
   a. To achieve a temporary account, a fixed password may be assigned together with the desired duration value. Once the password has expired, the account will no longer be usable, and the Administrator can delete or modify it at their convenience.
3. Deleting Accounts
   a. Select the account(s) you wish to remove and press the delete key.

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

Malware Prevention

Every effort must be made to ensure that any software or firmware loaded to the Atlas-II 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 be connected to the Atlas-II to utilize service tools. Consider the security of this PC and harden it to prevent malware from being introduced to the control. See Configuring Your External PC for more information on PC hardening.

Denial of Service (DoS) Protection

Denial of service attacks occur when a constant flow of data is sent to the Atlas-II’s communication ports to attack its availability and prevent normal control functions and operations. 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 Atlas-II.

The Atlas-II has functions at the GAP application level that can monitor the number of packets by each physical Ethernet port (see network security section for more information.) It is also recommended that the system and/or controller network implement real-time monitoring and Deep Packet Inspection (DPI) of network traffic to deter this type of attack and help mitigate cyber risks.

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 Atlas-II 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	TCP Servlink

667	TCP VxService
5133	Multicast Requests
5134	Multicast Listener
5135	Peer-to-Peer Requests
5136	Peer-to-Peer Reply

Network Security

The Atlas-II series contains routable protocols through its ports, so network security must be considered. The Atlas-II 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 Atlas-II needs to reside in a network, make sure that the network is isolated, with no connection to the greater Internet. If the Atlas-II 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 Atlas-II but should be within the same security zone.

Remote Gateways

Some control owners may choose to connect an Atlas-II or the network it is on to a remote communication gateway to be able 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 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 protect the area in which a remote communication gateway resides.

External Interfaces

4 Ethernet Ports
2 CAN Communication Ports
2 Isolated and Configurable RS-232 / RS-422 / RS-485 Serial ports
1 Isolated RS-232 Port (Reserved for Debug Service)

Ethernet Interfaces

The Atlas-II has four Ethernet connectors that are arranged in one connector. Do not use the Ethernet ports to connect the Atlas-II directly to the internet. See Remote Gateway section for information on connecting to and securing remote communication gateways.

At the GAP application level, there are functions available to monitor the Ethernet ports. Using these functions can help enhance the security posture of an Atlas-II by letting users know when a port is being attacked and allowing them to respond in a timely manner. The following functions can be implemented depending on the application requirements.

Ethernet Status Block (ENET_STAT)

- Monitors the number of packets received and transmitted by each physical Ethernet port.
- Provides diagnostic information about the low-level Ethernet interface.

Ethernet Based Distributed IO

- Distributed IO interfaces will have a timeout diagnostic like the link error function on the communication blocks. The application programmer must ensure that the timeouts and action taken when a timeout is detected are appropriate for the application requirements.

For network configuration, Ethernet port #1 can be re-configured for the customer network as desired. The Atlas-II is shipped with static IP addresses. To avoid Ethernet IP Address conflicts, consult the table below:

Port Name	IP Address	Subnet Mask
Ethernet #1	172.16.100.20	255.255.0.0
Ethernet #2	192.168.128.20	255.255.255.0
Ethernet #3	192.168.129.20	255.255.255.0
Ethernet #4	192.168.130.20	255.255.255.0
Default Gateway	<none>	

If available, use RJ-45 caps to protect ports that are not in use.

CAN Interfaces

The Atlas-II has two CAN ports for communication with Woodward valves and other CAN devices. As with the other external interface ports on the Atlas-II, utilizing physical security best practices along with monitoring the room the control is installed in and detecting unauthorized user access can help prevent manipulation of CAN bus interfaces.

Serial Interfaces

The Atlas-II digital control contains two isolated RS-232/422/485 serial ports and one isolated RS-232 service port. The two RS-232/422/485 ports are available for customer use and can be configured using the GAP software application. The RS-232 service port is for operating system use only and cannot be configured for software use. This port is to be used by trained field service personnel only. Protect serial interfaces from unauthorized access by utilizing physical security best practices.

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 Atlas-II 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.

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.

History

1. The following files are stored in the Atlas-II and can be retrieved using the Retrieve System Log Files command from the Control drop-down menu in AppManager.
   a. PMLog.txt
      i) Contains all successful logins and logouts.
      Note: There may be more than one entry per successful login.
      ii) Contains password changes.
      iii) Contains other account modifications made by the Administrator.
      iv) All entries are marked with the date and the account name of the user accessing it.
   b. Log.txt
      i) Contains application events.

ii) Identifies and dates privileged access which modify control contents. The modifiable control content includes:
- Start Application
- Stop Application
- Clear Autostart
- Execute Service Pack
- Update Module
- Write File
- Reboot Control
- Change Network Configuration

2. PMLog.txt and Log.txt files are limited in size to 1 MB. When a log file is about to exceed this size, it is copied to a backup file (“PMLog.old” or “Log.old”) and a new file is started. For this reason, the amount of history that can be captured is somewhere between 1 MB and 2 MB of ASCII text. This is likely to represent a long period of use, but there is no easy correlation between the size of the file and the length of the history. It is recommended to periodically retrieve and store these files with a date-based name to avoid losing history.

Decommissioning

When an Atlas-II 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.

Chapter 4.
Attack Scenarios

Figure 4-1 illustrates attack vectors that could impact the availability and integrity of the Atlas-II Digital Control.

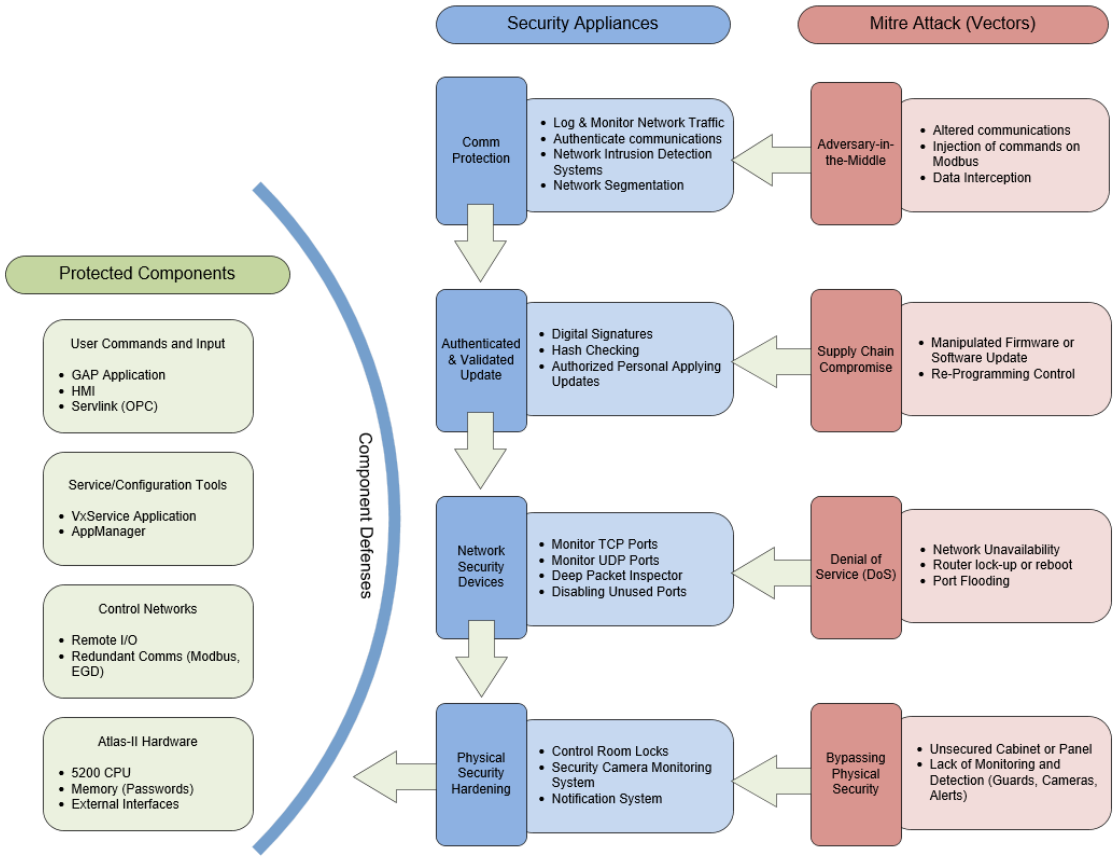

Figure 4-1. Potential Attack Vectors

An adversary-in-the-middle attack (AiTM) could exploit vulnerabilities of OPC or Modbus communication networks. One scenario for this type of attack involves an attacker controlling and possibly altering messages, packets, or data between two parties. In an adversary-in-the-middle attack, the integrity of sensor data or output commands could be compromised leading to the loss of an asset. 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 monitoring network traffic. Mitigations include authenticating communications to the control, network intrusion detection systems, and segmenting the network on which the control is on.

A replay attack can have a similar impact, but it exploits valid messages, packets, or data which are repeated or delayed, fooling the parties into believing a false context exists. One scenario for this type of attack could be the replay of a valid start permissive which disrupts the intended sequence of operation.

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

and Deep Packet Inspection (DPI) of network traffic, to help deter attacks and mitigate cyber risks. These appliances are external to the Atlas-II 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. Download service tools that interact with a control from a verified Woodward website.

Bypassing physical security and being able to physically interact with the Atlas-II presents a large attack vector. Even though the Atlas-II is usually mounted in a locked cabinet and is difficult to access, if an unauthorized user gains access to the control, they could damage it or cause it to behave unpredictably. 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 Atlas-II 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 Cybersecurity Support Portal | Woodward.

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.

Additionally, users may navigate to Cybersecurity Support Portal | Woodward to report vulnerabilities.

How are users notified about new releases?

Update notices will be sent to Woodward Distributers and OEMs for dissemination. Additionally, navigate to the Woodward website (www.woodward.com/software/) for all available software downloads, complete with revision descriptions.

For products with GAP Coder, version update notices are sent to Woodward distributors for dissemination to end customers.

Firmware Upgrade

Woodward and/or Atlas-II application developers may occasionally release firmware updates after product release to fix functional issues. Firmware update notifications are available on the Woodward product support web site at Woodward Industrial Support: Get Help.

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 receive 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
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
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 A—

- New manual release

Released

We appreciate your comments about the content of our publications.

Send comments to: industrial.support@woodward.com

Please reference publication 35259.

B 3 5 2 5 9 : A

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.