WOODWARD

Product Manual 35256
(Revision A, 8/2025)
Original Instructions

LS-5 Series Security Manual

Security Manual

Released

General Precautions

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

Practice all plant and safety instructions and precautions.

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

Revisions

This publication may have been revised or updated since this copy was produced. The latest version of most publications is available on the Woodward website.

Woodward Industrial Support: Get Help

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

Proper Use

Any unauthorized modifications to or use of this equipment outside its specified mechanical, electrical, or other operating limits may cause personal injury and/or property damage, including damage to the equipment. Any such unauthorized modifications: (i) constitute "misuse" and/or "negligence" within the meaning of the product warranty thereby excluding warranty coverage for any resulting damage, and (ii) invalidate product certifications or listings.

Translated Publications

If the cover of this publication states "Translation of the Original Instructions" please note:

The original source of this publication may have been updated since this translation was made. The latest version of most publications is available on the Woodward website.

Woodward Industrial Support: Get Help

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

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

Revisions— A bold, black line alongside the text identifies changes in this publication since the last revision.

Manual 35256

Contents

Illustrations

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, refer to the Approvals section (Section 8.1.7) of Woodward Manuals:

Manual Number	Manual Description
37542	LS-5 Series LS-511/521 Marine Technical Manual
37649	LS-5 v2 Series LS-5x1 Technical Manual
37650	LS-5 v2 Series LS-5x2 Technical Manual

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 LS-5 Series of Circuit Breaker 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 LS-5 Series of Circuit Breaker Controls. This manual covers security configurations, user access information, decommissioning, and security alert reporting and notification.

Scope

This manual covers the LS-5 Series Circuit Breaker Controls.

References

Refer to the Regulatory and Standards 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 Systems
ICS	Industrial Control System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
OT	Operational Technology
SCADA	System Control and Data Acquisition
SNTP	Simple Network Time Protocol
VNC	Virtual Network Computing

Chapter 2.
Industrial Cyber Security Basics

Introduction

Cybersecurity attacks are often carried out through IT and OT systems causing them to malfunction, become unstable, be disabled, or even be destroyed. OT systems are particularly vulnerable to cybersecurity attacks due to their complexity, making them difficult to harden against attacks. In addition, personnel needed to handle cybersecurity tasks are often overloaded or nonexistent, and the system components that need to be updated or replaced may be difficult to locate or be accessed by maintenance staff. Ensuring cybersecurity of an OT system requires knowledge, diligence, and team-wide collaboration. Following the guidelines in this manual can help mitigate the risk of a cybersecurity attack happening as well as help mitigate the extent of damage caused.

What is Cybersecurity?

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

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

Hardening

An important aspect of securing a system mentioned in this manual is the concept of “hardening”. Hardening refers to the practice of reducing a system’s vulnerability by reducing its attack surface. One of the goals of this manual is to help control owners harden their system and components that connect to their system to reduce the chance and impact of a cyber-attack. Following the defense-in-depth guidelines in this manual and configuring the LS-5 appropriately will aid in establishing a security hardened system and a stable and secure operating environment.

Where does the LS-5 Series exist in an OT network?

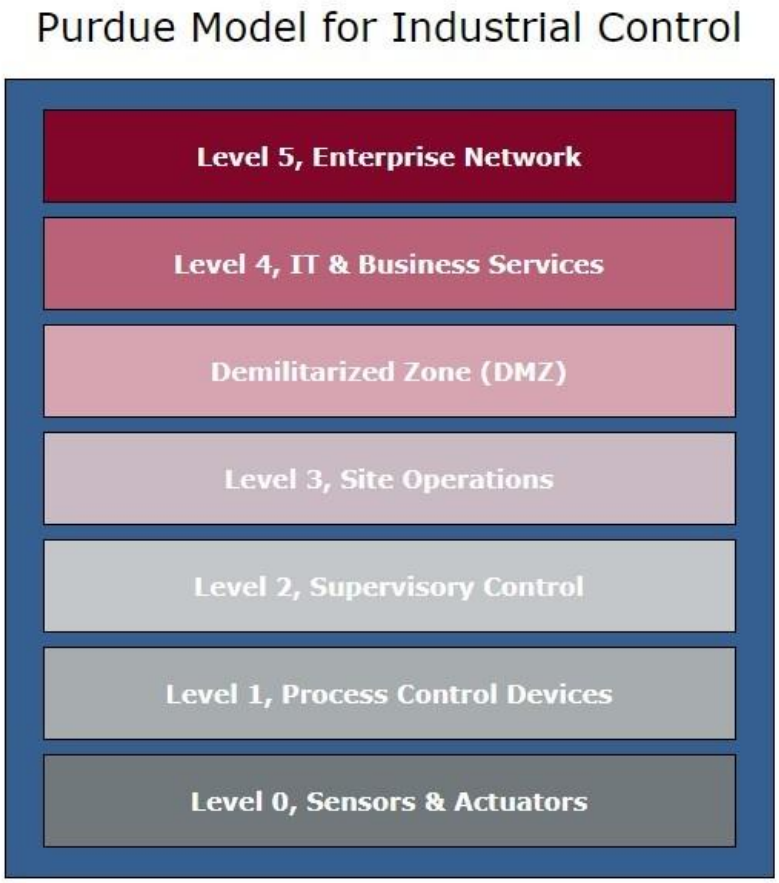

Figure 1-1. Purdue Model

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

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

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

Level 2, the supervisory layer, contains SCADA client functions, operators, engineering workstations, and HMIs.

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 LS-5 lives at level 1 of the Purdue Model. 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.

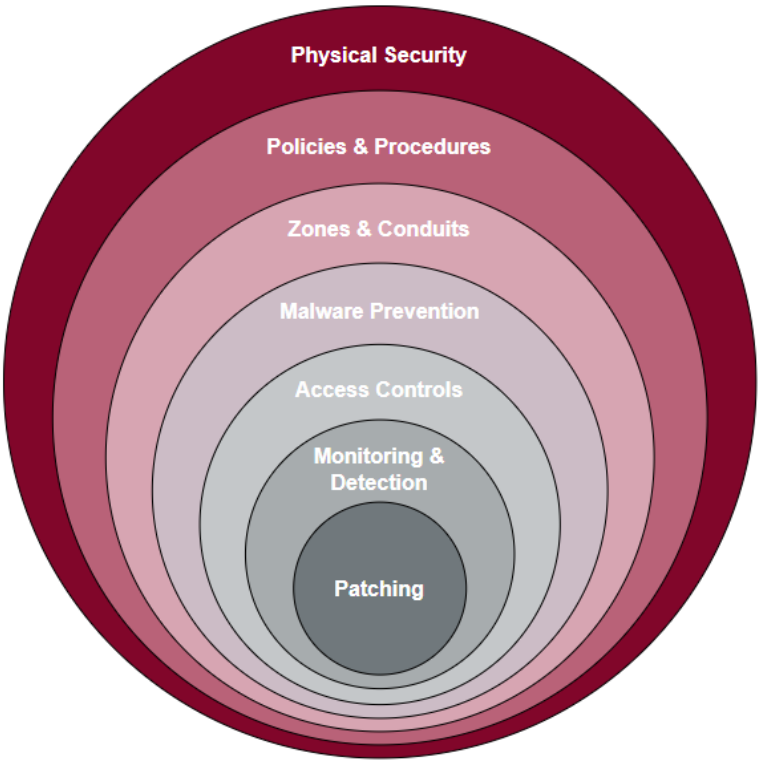

Figure 3-1. Defense in Depth Diagram

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 LS-5 is compromised.

Woodward Defense in Depth recommendations for secure LS-5 installations include:

- Updating default passwords to more secure passwords
- Ensure that users only receive passwords and access to the Code Level (permissions level) they need to carry out their job functions.
- Maintain physical security. Limit physical access to only authorized and trained personnel. Log who enters the control area and why.
- Minimize external Ethernet connections to HMI's, Engineering Workstations, and the LS-5.
- 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.

Physical Security

Physical security refers to the physical protection put in place to protect an LS-5 Series 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 an LS-5 is being used.

An LS-5 is a mounted control generally near, or on a prime mover. The prime mover and its environment should have secure access to ensure that only approved personnel have access to the control and prime mover. A good practice is to provide a method to alert operators that the control or its environment has been accessed.

The cabling attached to an LS-5 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 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 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.

Access Controls

Service Tools

The LS-5 series uses Woodward ToolKit to allow users to change settings on the control using a PC. ToolKit can be used to create and run custom administration tools for many Woodward electronic products. ToolKit can be installed via CD or downloaded from the Woodward website to a laptop or PC, then connected to the LS-5 to configure, calibrate, monitor and troubleshoot the device. For PC Requirements and additional information about installing and servicing the LS-5 Series using Toolkit, refer to section 5.1.1, “Install Toolkit”, of Woodward manuals 37542, 37649, and 37650.

Ensure that only Woodward or LS-5 provider-approved tools are used to interact with the LS-5. See Configuring Your External PC for more details on making the connected PC secure.

User Interface

Users can interface with an LS-5 control in several ways. LS-5 Series units with HMI’s allow users that have access to the environment where the LS-5 is installed to manipulate it by physically interacting with the control’s HMI screen or front panel access buttons. Changing the HMI passwords for code levels is recommended to prevent unauthorized access (See User Accounts section for more information). Front panel access buttons can be disabled by ToolKit using parameter “Lock keypad.”

LS-5 controls can also be configured by users using a Windows laptop or PC with Woodward ToolKit installed. ToolKit can be installed via CD or downloaded from the Woodward website on to a laptop or PC, then connected to the LS-5 to configure, calibrate, monitor and troubleshoot the device using the RS-232/USB Service Port, CAN port or RS-485 port.

The service port can only be used in combination with an optional Woodward direct configuration cable, which includes a converter box to provide either a USB or RS-232 port. Refer to Chapter 3.3.11, “Service Port” in Woodward Manuals 37542, 37649, and 37650 for more information about the Service Port.

A CAN bus connection is only possible if a suitable USB-to-CAN adaptor is used. Refer to section 5.1.4, “Connect ToolKit”, of Woodward manuals 37542, 37649, and 37650 for more information.

Configuring Your External PC

PCs running the Windows operating system may provide easy attack paths. Due to this, Woodward recommends the following security measures for computers and laptops that connect to an LS-5 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 & internet gateway
- WPA2 encryption for wireless control and Wireless Intrusion Prevention

User Accounts

The LS-5 Series utilizes a password protected multi-level access hierarchy through Code Levels to prevent unauthorized access to parameters, configuration, and calibration items. This allows varying degrees of access to the parameters by assigning unique passwords to each Code Level, then giving that password to designated personnel. When assigning passwords to users, limit access rights of each user to the minimum level necessary to perform job functions.

User Account Levels

Code Level	Standard Code Entry: Password (Default)	Permissions
CL0	None	This code level permits monitoring of the system and limited access to the parameters. Configuration of the control is not permitted. Only the parameters for setting the language, the date, the time, and the horn reset time are accessible. The unit powers up at this code level.
CL1	0001	This code level permits the user to change selected non-critical parameters, such as setting the parameters accessible in CL0 plus BAR/PSI, °C/°F. The user may change the password for Code Level 1. Access granted by this password expires two hours after the password has been entered, and the user is returned to the CL0 level.
CL2 (Temporary Commissioning Level)	Algorithm Password*	This code level grants temporary access to most parameters. Access granted by this password expires two hours after the password has been entered, and the user is returned

		to CL0. The password for the temporary commissioning level may be obtained from the vendor. *The password is calculated from the random number generated when the password is initially accessed. This grants a user one-time access to a parameter without having to give them a password that is in use.
CL3 (Commissioning Level)	0003	This code level grants complete and total access to most parameters. In addition, the user may also change the passwords for CL1, CL2, and CL3. Access granted by this password expires two hours after the password has been entered and the user is returned to CL0

Malware Prevention

Every effort must be made to ensure that any software or firmware loaded to the LS-5 is authentic Woodward or application developer software. Utilize methods such as hashing and signatures to help ensure the authenticity of software. A likely source of malware is the Window's PC or laptop that can connect to the LS-5 to adjust settings using the ToolKit service tool. Consider the security of this PC and harden it to prevent malware from being introduced to the control. See the "Configuring Your External PC" section for more information on PC hardening.

Zones and Conduits

Zones and Conduits refers to the idea of separating the components of a system into zones that share similar security requirements and the wiring, routers, etc. that link these zones together. The LS-5 series should reside in a zone that is not directly connected to any enterprise network or the greater Internet.

Some control owners may choose to use a remote communication gateway as a conduit to remotely access and monitor the zone and system that the LS-5 is a part of. When installing remote gateways, the owner and users should be aware of the security risks associated with placing components of a system on a network connected to the Internet. Although many remote gateways detail a strong security posture, additional security considerations should be made.

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

External Interfaces

The LS-5 has external interfaces that should be protected for security. These come in the form of an RS-232 interface with an RJ-45 port, CAN, and RS-485. These interfaces can be best protected through physical security and monitoring the environment in which the LS-5 is installed.

IMPORTANT **The RJ-45 connector on the LS-5 is used only for RS-232 serial communication, not Ethernet networking. Therefore, it cannot be exploited for Ethernet-based DoS attacks.**

Denial of Service (DoS) Protection

The LS-5 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 LS-5 will prevent them from being used as a DoS attack vector.

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; however, the LS-5 is limited in the monitoring and detection it can provide by itself. The LS-5 supports the security practice of repudiation in the form of Alarm List and Event History. These logs allow Administrators to verify what actions were taken on the control and when those actions took place. The Alarm List will display a list of alarm messages which have not been acknowledged or cleared yet. Repeated alarms about a certain activity on the control may be due to an attack and should be responded to and investigated quickly. Event History displays a list of system events along with a timestamp of when the action occurred and if the condition was activated or deactivated. During or after an attack, Event History can help pinpoint the time an attack happened, and the components or settings an attacker manipulated.

Additional monitoring and detection should be applied at the next control level higher (i.e. PLC, upper-level control module, ICS firewall).

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.

Updating

Woodward occasionally releases new software for controls that contain new or updated functions. These updates may also contain security updates required to keep the control secure. Users can flash update an LS-5 by connecting a security hardened PC using ToolKit with the appropriate configuration files installed (See Configuring Your External PC section for more information on securing your PC). If Woodward releases a firmware update, the system owner/operator should have an authorized person update their control in a timely manner, following the organization’s risk assessment, to prevent vulnerabilities from being exploited.

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

Decommissioning

When an LS-5 has reached end-of-life and is ready to be decommissioned, removing data from the control is recommended. This includes removing any potentially sensitive information from the control, such as configuration information or personally identifiable information, and restoring the control to factory default settings. Restoring the factory default settings will reset all parameters excluding customer defined passwords to their factory default values.

See section 4.1.4, System Management, in manuals 37542B, 37649, and 37650 for more information on restoring an LS-5 to factory default settings.

Chapter 4.
Attack Scenarios

Figure 4-1 illustrates attack vectors that could impact the availability and integrity of an LS-5 Circuit Breaker Control.

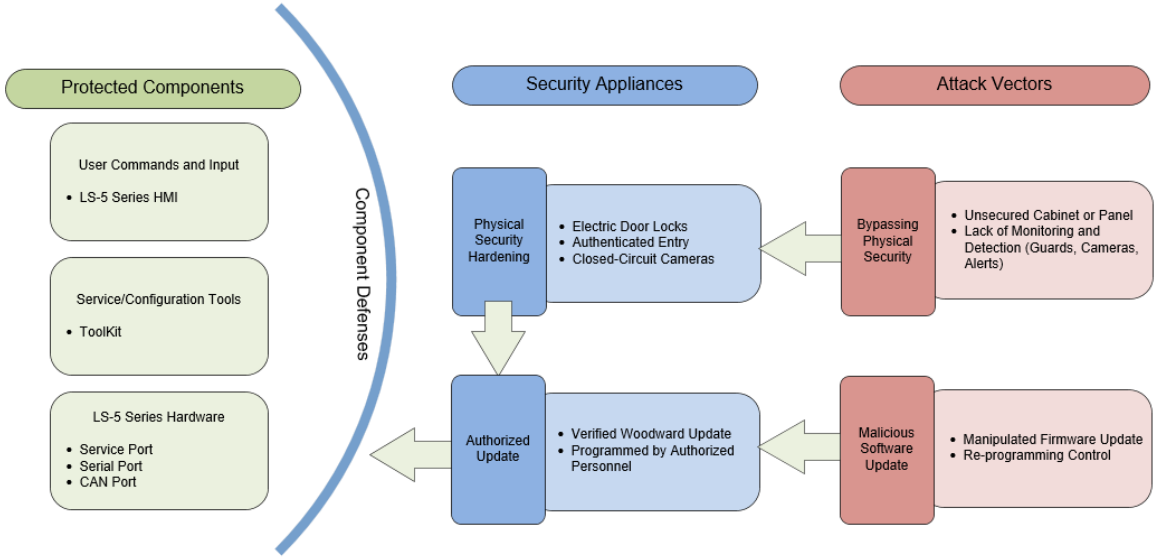

Figure 4-1. Potential Attack Vectors

Bypassing physical security and being able to physically interact with the LS-5 presents a large attack vector for the LS-5. 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 LS-5 by changing default passwords provides an additional layer of security in the case an attacker gains physical access to the control.

A **Malicious Software/Firmware Update** may be applied to an LS-5. An attacker who makes it past physical security can plug a PC or laptop into the control and issue a flash update using a malicious firmware package. This attack can help be prevented by making sure that only authorized users have access to the area where the LS-5 resides and verifying that firmware applied to the control is a genuine Woodward update.

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 Security Bulletin to www.woodward.com.

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

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

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

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

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

How are users notified about new releases?

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 LS-5 Series 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 https://www.woodward.com/support/industrial-support/.

Chapter 6.
Product Support and Service Options

Product Support Options

If you are experiencing problems with the installation, or unsatisfactory performance of a Woodward product, the following options are available:

- Consult the troubleshooting guide in the manual.
- Contact the manufacturer or packager of your system.
- Contact the Woodward Full Service Distributor serving your area.
- Contact Woodward technical assistance (see “How to Contact Woodward” later in this chapter) and discuss your problem. In many cases, your problem can be resolved over the phone. If not, you can select which course of action to pursue based on the available services listed in this chapter.

OEM or Packager Support: Many Woodward controls and control devices are installed into the equipment system and programmed by an Original Equipment Manufacturer (OEM) or Equipment Packager at their factory. In some cases, the programming is password-protected by the OEM or packager, and they are the best source for product service and support. Warranty service for Woodward products shipped with an equipment system should also be handled through the OEM or Packager. Please review your equipment system documentation for details.

Woodward Business Partner Support: Woodward works with and supports a global network of independent business partners whose mission is to serve the users of Woodward controls, as described here:

- A **Full Service Distributor** has the primary responsibility for sales, service, system integration solutions, technical desk support, and aftermarket marketing of standard Woodward products within a specific geographic area and market segment.
- An **Authorized Independent Service Facility (AISF)** provides authorized service that includes repairs, repair parts, and warranty service on Woodward's behalf. Service (not new unit sales) is an AISF's primary mission.

A current list of Woodward Business Partners is available at:
https://www.woodward.com/en/support/industrial/service-and-spare-parts/find-a-local-partner

Product Service Options

The following factory options for servicing Woodward products are available through your local Full-Service Distributor or the OEM or Packager of the equipment system, based on the standard Woodward Product and Service Warranty (Woodward North American Terms and Conditions of Sale 5-09-0690) that is in effect at the time the product is originally shipped from Woodward or a service is performed:

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

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

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

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

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

Flat Rate Remanufacture: Flat Rate Remanufacture is very similar to the Flat Rate Repair option with the exception that the unit will be returned to you in “like-new” condition and carry with it the full standard Woodward product warranty (Woodward North American Terms and Conditions of Sale 5-09-0690). This option is applicable to mechanical products only.

Returning Equipment for Repair

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

When shipping the item(s), attach a tag with the following information:
- Return authorization number
- Name and location where the control is installed
- Name and phone number of contact person
- Complete Woodward part number(s) and serial number(s)
- Description of the problem
- Instructions describing the desired type of repair

Packing a Control

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

NOTICE

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

Replacement Parts

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

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

Engineering Services

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

- Technical Support
- Product Training
- Field Service

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

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

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

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

Contacting Woodward's Support Organization

For the name of your nearest Woodward Full-Service Distributor or service facility, please consult our worldwide directory at **https://www.woodward.com/support**, which also contains the most current product support and contact information.

You can also contact the Woodward Customer Service Department at one of the following Woodward facilities to obtain the address and phone number of the nearest facility at which you can obtain information and service.

Products Used in Electrical Power Systems

Facility	Phone Number
Brazil	+55 (19) 3708 4800
China	+86 (512) 8818 5515
Germany	+49 (711) 78954-510
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+82 (51) 636-7080
Poland	+48 (12) 295 13 00
United States	+1 (970) 482-5811

Products Used in Engine Systems

Facility	Phone Number
Brazil	+55 (19) 3708 4800
China	+86 (512) 8818 5515
Germany	+49 (711) 78954-510
India	+91 (124) 4399500
Japan	+81 (43) 213-2191
Korea	+82 (51) 636-7080
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 35256.

B 3 5 2 5 6 : 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.