





**Product Manual 35233
(Revision -, 11/2024)
Original Instructions**





Large Engine Control Module (LECM)

Security Manual

	General	Read this entire manual and all other publications pertaining to the work to be performed before installing, operating, or servicing this equipment.
	Precautions	Practice all plant and safety instructions and precautions.
		Failure to follow instructions can cause personal injury and/or property damage.

	Revisions	This publication may have been revised or updated since this copy was produced. The latest version of most publications is available on the Woodward website.
		Woodward Industrial Support: Get Help
		If your publication is not there, please contact your customer service representative to get the latest copy.

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

	Translated Publications	If the cover of this publication states "Translation of the Original Instructions" please note:
		The original source of this publication may have been updated since this translation was made. The latest version of most publications is available on the Woodward website.
		Woodward Industrial Support: Get Help
		Always compare with the original for technical specifications and for proper and safe installation and operation procedures.
		If your publication is not on the Woodward website, please contact your customer service representative to get the latest copy.

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

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

Contents

WARNINGS AND NOTICES	3
ELECTROSTATIC DISCHARGE AWARENESS	5
CHAPTER 1. GENERAL INFORMATION	7
Purpose	7
Scope	7
References	7
Glossary	7
CHAPTER 2. INDUSTRIAL CYBERSECURITY BASICS	8
Introduction.....	8
What is Cybersecurity?	8
Denial of Service (DoS) Protection	9
CHAPTER 3. DEFENSE IN DEPTH (DID)	10
Defense in Depth Concept	10
CHAPTER 4. COMMUNICATION PORTS	13
CHAPTER 5. ATTACK SCENARIOS	14
CHAPTER 6. LECM SECURITY OVERVIEW	16
CHAPTER 7. SECURITY REFERENCES	18
CHAPTER 8. SECURITY NOTIFICATIONS AND PATCHING	19
CHAPTER 9. PRODUCT SUPPORT AND SERVICE OPTIONS	20
Product Support Options	20
Product Service Options	20
Returning Equipment for Repair	21
Replacement Parts.....	21
Engineering Services	21
Contacting Woodward's Support Organization	22
Technical Assistance	23
REVISION HISTORY	24

Illustrations and Tables

Figure 1-1. Purdue Model	9
Figure 3-1. Defense in Depth	10
Figure 5-1. Potential Attack Vectors	15
Table 6-1. LECM EID and LECM Aux Woodward Standard Applications	16
Table 6-2. LECM Main Common Protocol Usage	17
Table 6-3. LECM Application Programming & Configuration Access Security	17

The following are trademarks of Woodward, Inc.:

- LINKnet and LINKnet HT
- Servlink
- MotoTune

The following are trademarks of their respective companies:

- Modbus (Schneider Electric)

The following are associated with their respective organizations or entities:

- ISA (International Society of Automation)
- Purdue Model - Purdue Enterprise Reference Architecture (PERA) (Theodore Williams)
- NERC (North American Reliability Corporation)
- NIST (National Institute of Standards and Technology)

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 Prime Mover. 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

IOLOCK. When a CPU or I/O module fails, watchdog logic drives it into an IOLOCK condition where all output circuits and signals are driven to a known de-energized state as described below. The System **MUST** be designed such that IOLOCK and power OFF states will result in a SAFE condition of the controlled device.

- CPU and I/O module failures will drive the module into an IOLOCK state.
- CPU failure will assert an IOLOCK signal to all modules and expansion racks to drive them 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.

The IOLOCK state is asserted under various conditions including:

- CPU and I/O module watchdog failures
- PowerUp and PowerDown conditions
- System reset and hardware/software initialization
- Entering configuration mode
- User selection

NOTE: Additional watchdog details and any exceptions to these failure states are specified in the related CPU or I/O module section of the 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.

! CAUTION

RISKS OF CALIBRATION AND CHECKOUT—The calibration and checkout procedure should only be performed by authorized personnel knowledgeable of the risks posed by live electrical equipment.

FUSE POWER SUPPLY MAINS—The power supply mains should be properly fused according to the National Electrical Code. The recommended fuse is a European Type T fuse.

DISCONNECTING DEVICE—A switch or circuit breaker shall be included in the building installation that is in close proximity to the equipment and within easy reach of the operator and that is clearly marked as the disconnecting device for the equipment. The switch or circuit breaker shall not interrupt the protective earth conductor.

Electrostatic Discharge Awareness

NOTICE

Electrostatic Precautions

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

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

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

Follow these precautions when working with or near the control.

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

IMPORTANT

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

Regulatory Compliance

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

Manual Number	Manual Description
26757	LECM LARGE ENGINE CONTROL MODULE

Special Condition for Safe Use

The Large Engine Control Module (LECM) was developed without a secure development life cycle process prior to the realization of current cybersecurity standards, and as such, shall not be considered a cybersecure product.

Chapter 1.

General Information

Purpose

This manual provides a description of the cybersecurity (“security”) context and strategies for the LECM control. The manual covers security configurations, user access information, decommissioning, and security alert reporting and notification.

Scope

This manual covers the LECM control family.

References

Woodward Manual 26757, LECM Hardware Installation Manual

[ISA/IEC 62443 Series of Standards](#)

Glossary

CAN	Controller Area Network
DDoS	Distributed Denial of Service
DiD	Defense in Depth
DoS	Denial of Service
IACS	Industrial Automation Control Systems
ICS	Industrial Control System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
LECM	Large Engine Control Module
OT	Operational Technology
SCADA	Supervisory Control and Data Acquisition

Chapter 2.

Industrial Cybersecurity Basics

Introduction

Cybersecurity events are becoming more and more common. Attackers are refining their strategies, and attacks are becoming more diversified. Electricity suppliers are experiencing disruptions, petroleum companies are shutting down, and ransomware is running rampant. These can all be traced back to cyber attackers making their way into company IT and OT systems and causing these systems to malfunction or become unstable, even shutting down and having critical control systems disabled or destroyed.

OT systems are particularly vulnerable to cybersecurity attacks due to their complexity. Large systems are difficult to harden against attack. Personnel to handle cybersecurity tasks are overloaded or nonexistent. The system components that need to be updated or replaced may be very difficult to locate and access by maintenance staff.

What is Cybersecurity?

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

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

Following the guidelines in this manual and configuring the LECM appropriately will aid in establishing a stable and secure control system.

Purdue Model

Purdue Enterprise Reference Architecture (PERA), Purdue model was designed as a reference model for data flows in computer-integrated manufacturing where a plant's processes are completely automated. It defines the standard for building an ICS network architecture in a way that supports OT security, separating the layers of the network to maintain a hierarchical flow of data between them. ^{1,2}

The Purdue model illustrated in Figure 1-1 represents a typical OT network architecture.

Where Does the LECM Live in a Purdue Model-based OT Network?

The LECM lives at level 1 of the Purdue model illustrated in Figure 1-1.

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

Level 1 contains basic control equipment. These consist of complex controllers, PLCs, monitoring equipment, and other equipment required to maintain control of the process.

Level 2, the supervisory layer, contains SCADA client functions, operators, engineering workstations, and HMI's.

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

Level 4 represents services provided by IT and is not considered part of the OT network.

Level 5 represents the enterprise IT network and is not considered part of the OT network.

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.

¹ A Reference Model for Computer Integrated Manufacturing, ISA, Williams, Theodore, 1991

² PERA Master Planning Guide, Enterprise Consultants, International, Rathwell, Gary, 2009

Purdue Model for Industrial Control

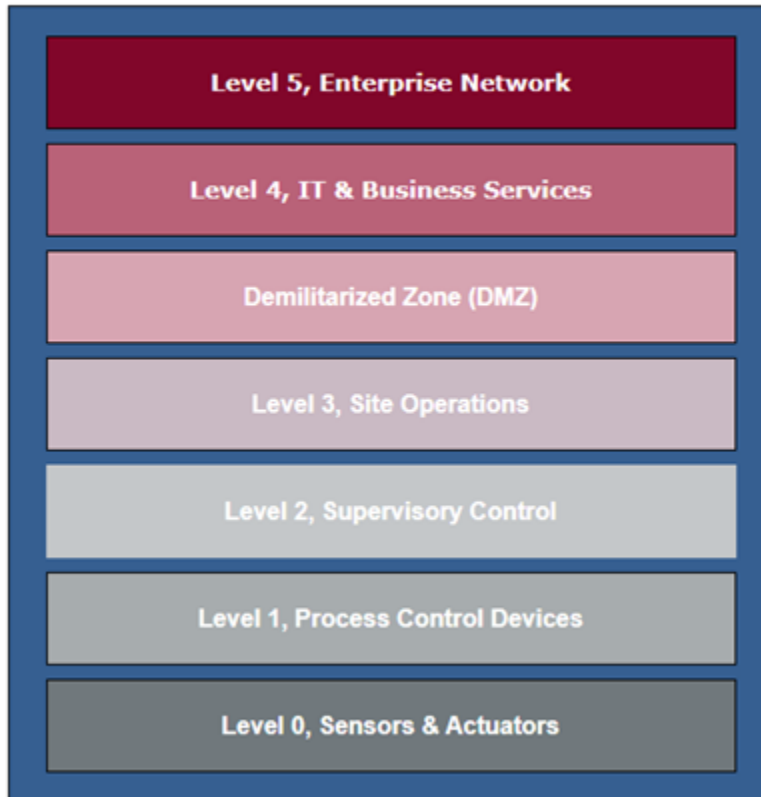


Figure 1-1. Purdue Model

Denial of Service (DoS) Protection

Denial of service attacks typically involve a deluge of valid and/or invalid information sent to the LECM's communication ports, causing the ports to slow down substantially or possibly crash. This information can consist of a combination of valid requests at such a high rate that the port handler cannot keep up, resulting in malformed messages that the port cannot resolve in a timely manner. DoS attacks can occur on the Ethernet and CAN interfaces. The LECM does not have integrated capabilities to deal with these attacks. It is up to the system and/or controller network to ensure that communications are clean and do not overload the LECM.

Refer to the LECM Hardware Installation Manual 26757 for communication port details, including CAN and Ethernet information.

Chapter 3. Defense in Depth (DiD)

Defense in Depth is a strategy that leverages multiple layers of security to protect an organization's assets. The concept is that if one layer of defense is compromised, additional layers exist to help ensure that threats are stopped before the LECM is compromised.¹

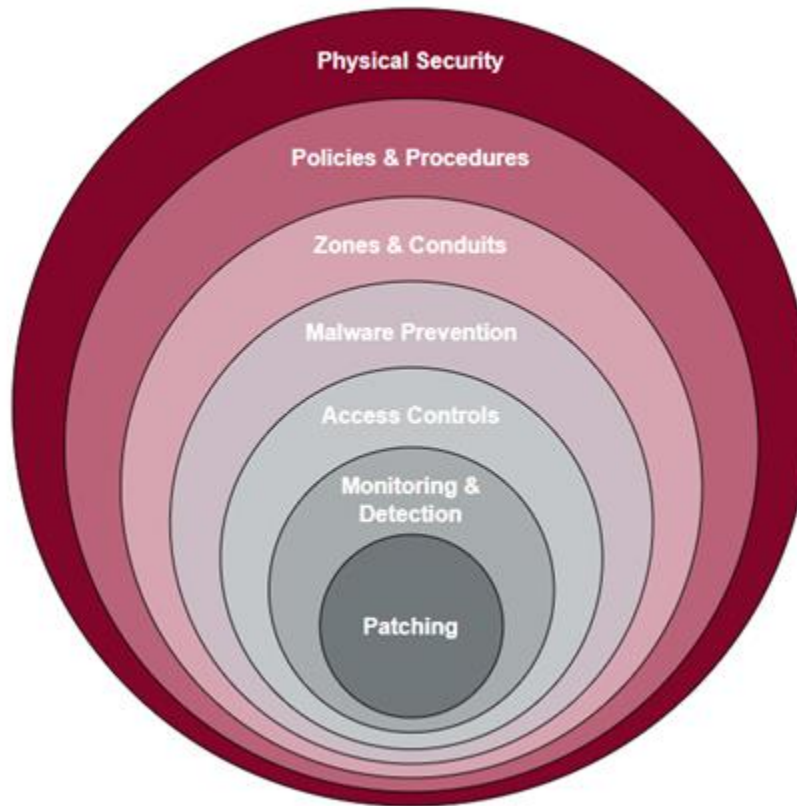


Figure 3-1. Defense in Depth

Defense in Depth Concept

Physical Security

Physical security must be tailored to the environment the LECM is used in. Here are a few guidelines.

Physical access control is an aspect to a Defense in Depth strategy for securing the LECM in an application. Physical security can include fences, closed-circuit cameras, guards, signage, and motion sensors, etc. The idea is to detect and deter attackers before they can access the control system. Ensure that physical security devices notify the appropriate personnel in a timely manner so action can be taken if needed. The earlier the warning occurs the better.

The LECM is generally mounted on an engine, so physical protection for the engine and its environment should be provided to ensure that only approved personnel have access to the engine. Provide some method to alert operators that the engine or its environment has been accessed.

Equally important to physically protecting the LECM is protecting the cabling attached to the control. Physical damage to the cabling can cause instability of the equipment controlled by the LECM and damage to the LECM 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 significant damage and instability.

Driver signals to the equipment being controlled can be corrupted, lost, or shorted to each other or ground, causing damage or instability.

Another concern for cabling is the ability of an attacker to tap into the cabling. An attacker could create false or inaccurate information by delaying messages or injecting false information, causing damage or instability. 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.

Policies and Procedures

The control owner should have policies and procedures in place to raise awareness of security practices for IACS. Having a security-aware staff greatly 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.

The control should not be directly accessible from any public network including the Internet. Networks are a very common attack path for electronic controls that can be operated remotely. Isolating the LECM to a secure plant control network should be a high priority.

If complete isolation from a public or insecure network is not possible, protect and secure the network in which the LECM resides from attacks originating from the network. Firewalls, routers, IDS and IPS equipment can help ensure cybersecurity for the control.

Zones and Conduits

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

Malware Prevention

Every effort must be made to ensure that any software or firmware loaded to the LECM is authentic Woodward or application developer-supplied software. Utilize methods such as hashing and signatures to help ensure authenticity. The LECM cannot perform verification on its own, so it is up to the user to ensure software integrity.

Access Controls

User Interface

Control access should be through hardened (security enhanced, incorporating special security hardware and/or software) PC's or HMI's. PC's running Windows provide an exceptionally easy attack path. Ensure that all software and firmware patches and updates are applied and that security tools are installed and kept up to date on the user interface. Any user interface connected to the LECM should be hardened.

When LECM control access is necessary, consideration of the security posture for the computer accessing the LECM is important. A connection may be necessary for a Human Machine Interface (HMI) interaction or to configure the LECM. Security practices, for example a PC with a Windows operating system, include device hardening, elimination of unneeded services, malware/anti-virus protection, and user account management. The Windows operating system does provide an easy attack path. Ensure that all software and firmware patches and updates are applied and that security tools are installed and kept up to date.

Service Tools

Woodward provides an array of software tools that can provide functions from monitoring to full LECM operation and configuration. Ensure that only Woodward or LECM provider-approved tools are used to interact with the LECM. Refer to your installer, sales contact, or Woodward customer support for details.

Monitoring and Detection

From a cybersecurity perspective, monitoring and detection during system operation will help in detecting unusual activity that may be caused by interference of the physical control system or an attacker intruding into the system. Contact your Woodward sales or support representative for further information about cybersecurity tools and appliances.

Patching

Woodward occasionally releases new software for controls that update the control with new or updated functions. These patches may also contain security updates required to keep the control secure. It is critical that the system owner/operator installs these updates as soon as practicable when they are released.

There are two scenarios where patches could be applied. The first covers boot-type patches to update the boot-level firmware of the LECM. The second scenario covers application patches for the application firmware. Application patches could be supplied by Woodward or the application developer.

Contact your Woodward sales or support representative for further information.

¹ IEC 62443-1-1 (Definition) and IEC 62443-4-1 SD-2, Defense in Depth

Chapter 4. Communication Ports

Ports that will not be used must be disabled. The fewer open ports on a device, the fewer access points an attacker will have to get into the device. Often a system operator may not be aware of open ports. This could be due to maintenance and troubleshooting activities, or by using software that opens ports by default for its own use. Regularly scan the device to check for open ports that should not be open and reconfigure any that are found to make them unavailable.

Default Open Ethernet Ports

Below is a list of commonly used ethernet ports for LECM service and application interfacing with external devices; however, not all ports may be in use for a particular application. Contact your application provider for a list of open ports.

- 13400 – Reserved for XCP on TCPIP or UDPIP
- 123 – SNTP
- 666 – Servlink
- 502 – Modbus

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

Chapter 5.

Attack Scenarios

The attack vectors in Figure 5-1 illustrate a few examples of attacks that could impact the availability and integrity of the LECM.

Man-in-the-Middle Attack

A man-in-the-middle attack (MITM), achieved by accessing communications signals to and from the control, could exploit vulnerabilities of protocols such as Modbus communication networks which are natively insecure. One scenario for this type of attack involves an attacker controlling and possibly altering messages/packets/data between two parties. In a MITM attack, the integrity of sensor data or output commands could be compromised, leading to unexpected and hazardous operation of the LECM and LECM-controlled devices.

Replay Attack

An MITM replay attack exploits valid messages/packets/data which are captured, then repeated or delayed, fooling the user into believing a false control context exists or causing engine operation to become unstable. One scenario for this type of attack could be the replay of a valid start or stop which disrupts the intended sequence of operation. MITM attacks are best prevented by protecting communications associated with the LECM (user interface, sensors) from access by an attacker.

DoS or DDoS

A Denial-of-Service (DoS) or a Distributed-Denial-of-Service (DDoS) are intended to attack a system's availability and prevent normal control functions and operations. DoS attacks often exploit network vulnerabilities by overwhelming routers and network adapters with unnecessary traffic.

To help combat DoS attacks, the system should provide network appliances to detect intrusion, provide rate limiting, and provide deep packet inspection. The appliances should be external to the control, but within the same secure network zone. This will help ensure that the LECM remains responsive.

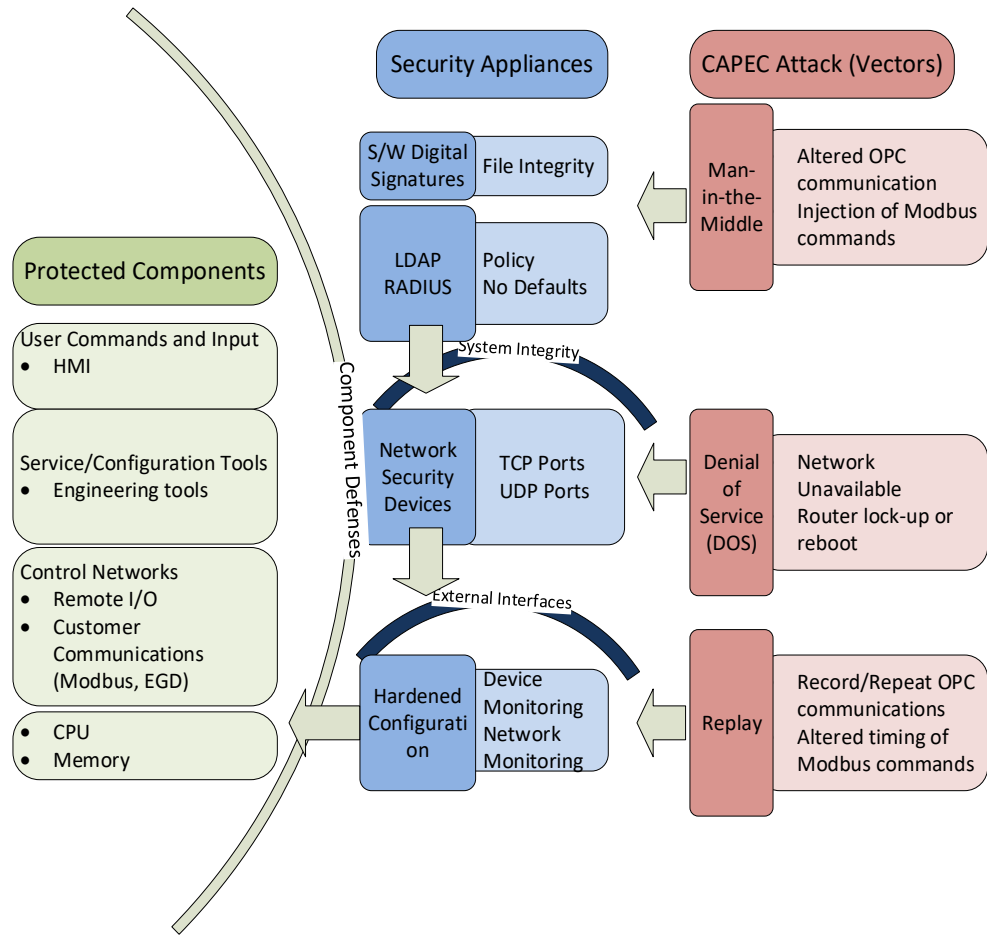


Figure 5-1. Potential Attack Vectors

Chapter 6.

LECM Security Overview

The LECM was developed without a secure development life cycle process prior to the realization of current cybersecurity standards, and as such, shall not be considered a cybersecure product. From a networking perspective, the LECM is required to be located within a secure OT network as a component that requires further layers of protection provided at the system-level. All ethernet and CAN datalink interfaces require protection from DoS attacks and malicious messaging. From a physical accessibility perspective, the LECM can either be on-engine mounted or located within a cabinet. As such, the engine/cabinet and cabling shall be safeguarded in order to protect datalink and hardwired sensor and actuation interfaces with the LECM.

Despite the lack of intrinsic security limitations within the LECM, service protocols (e.g., XCP, Servlink, MotoTune) can support user accounts and passwords. For system integrators and LECM application end-users, protocol security features are a property of the LECM application and the respective application manuals shall be referenced for details on service protocol security implementations.

For Woodward standard LECM EID or LECM Aux software applications, please refer to the software manuals for security implementations.

Table 6-1. LECM EID and LECM Aux Woodward Standard Applications

Module	Application	Manual
LECM EID	EID Mixed Mode	35014
LECM EID	EID Injection	35175
LECM EID	EID Ignition	35100
LECM Aux	Aux Knock	35138
LECM Aux	Aux RTCDC	35079
LECM Aux	Aux Thermocouple	35112
LECM Aux	Protection IO	35188

LECM Application Developer Protocol Security Notes

For LECM Main application developers, there are three external CAN, one ethernet, and two serial (RS232/RS485) datalink interfaces that are used for external communications with sensors, actuators, and/or service tools for application configuration management and LECM programming. Although not necessarily a complete list of protocols or custom communication implementations, the following table represents the most common protocols used in LECM Main applications:

Table 6-2. LECM Main Common Protocol Usage

Protocol	Supported Datalinks	Typical Usage	Supports Security
XCP	CAN, Ethernet (TCP/IP, UDP/IP)	Application service, configuration management, and programming	Yes
Servlink (Woodward proprietary)	Ethernet (TCP/IP), RS232[485]	Application service and configuration management	Yes
MotoTune (Woodward proprietary)	CAN, RS232[485]	Application service, configuration management, and programming	Yes
UDS	CAN (ISO15765)	Application service, configuration management, diagnostic reporting, and programming	Yes
J1939	CAN	Sensor/Actuation interfacing, external commands, and diagnostic reporting	No
Modbus	Ethernet (TCP/IP), RS232[485]	Sensor/Actuation interfacing, external commands, and diagnostic reporting	No

As an LECM Main application developer, there are two different types of LECM security that need to be considered: **Boot security** and **Application security**.

The LECM boot application is maintained by Woodward and is responsible for validating and executing the user application in addition to reprogramming the LECM unit while in a bootstrapped operational mode. The boot supports three protocols to program the LECM: MotoTune (CAN), XCP (Ethernet or CAN), and UDS (CAN). By default, all protocols are secured and require a security library (XCP or UDS) or a special key to the USB Cryptoken device (MotoTune) in order to program the LECM unit while in a bootstrapped state; however, boot security can optionally be disabled at the discretion of the application developer.

If the LECM is in a normal operational mode and is executing the user application, then programming and servicing security is handled by the application. Application programming and service access is controlled by the security implementation of one of the following supported protocols if instantiated by the application developer:

Table 6-3. LECM Application Programming & Configuration Access Security

Protocol	Security Description
MotoTune (CAN or RS232[485])	Requires special keys on a silver USB Cryptoken device. Boot has different keys than LECM application.
XCP (Ethernet or CAN)	Secured via a seed/key algorithm the developer implements OR a password-version of the seed/key implementation. Boot has a different security implementation than LECM application.
UDS (CAN)	Secured via a seed/key algorithm the developer implements OR a password-version of the seed/key implementation. Boot has a different security implementation than LECM application.

For application developers, please refer to Woodward customer support for more information. For system integrators, please refer to your LECM application provider for more information on application security.

Bootstrapping details can be found in the LECM Hardware Installation Manual 26757 on page 93 of Revision C.

Chapter 7. Security References

Security references, such as those from IEC/ISA 62443, NIST, and NERC, are guidelines to help ensure that the product is designed and developed in such a way that it can guard against attacks and actions that would compromise performance. Examples of these actions range from simple human error up to and including malicious attacks resulting in damage to the LECM and damage to equipment connected to the LECM.

Chapter 8.

Security Notifications and Patching

Security Notifications

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

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

Customers can report security problems through Woodward customer service cybersecurityhelpdesk@woodward.com or the Woodward web site.

Firmware Upgrade

Woodward and/or LECM application developer occasionally release firmware updates after product release to fix functional and security issues. It is vital that updates be installed as soon as practical to keep the LECM secure. Firmware updates are available on the Woodward product support web site at <https://www.woodward.com/en/support/industrial/technical-help-desk>.

Chapter 9.

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: www.woodward.com/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 www.woodward.com/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 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 (32) 422-5551
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 (32) 422-5551
The Netherlands	+31 (23) 5661 111
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 (32) 422-5551
The Netherlands	+31 (23) 5661 111
Poland	+48 (12) 295 13 00
United States	+1 (970) 482-5811

Technical Assistance

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

General

Your Name _____

Site Location _____

Phone Number _____

Fax Number _____

Prime Mover Information

Manufacturer _____

Turbine Model Number _____

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

Power Output Rating _____

Application (power generation, marine,
etc.) _____

Control/Governor Information

Control/Governor #1

Woodward Part Number & Rev. Letter _____

Control Description or Governor Type _____

Serial Number _____

Control/Governor #2

Woodward Part Number & Rev. Letter _____

Control Description or Governor Type _____

Serial Number _____

Control/Governor #3

Woodward Part Number & Rev. Letter _____

Control Description or Governor Type _____

Serial Number _____

Symptoms

Description _____

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

Revision History

Revision-

- New manual

We appreciate your comments about the content of our publications.

Send comments to: industrial.support@woodward.com

Please reference publication **35233**.



B 3 5 2 3 3 : -



PO Box 1519, Fort Collins CO 80522-1519, USA
1041 Woodward Way, Fort Collins CO 80524, USA
Phone +1 (970) 482-5811

Email and Website—www.woodward.com

Woodward has company-owned plants, subsidiaries, and branches, as well as authorized distributors and other authorized service and sales facilities throughout the world. Complete address / phone / fax / email information for all locations is available on our website.