Application Note 51654
(Revision A, 6/2025)
Original Instructions

Legacy Products
System Security Practices

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.

Application Note 51654

Contents

WARNINGS AND NOTICES **3**

ELECTROSTATIC DISCHARGE AWARENESS **4**

CHAPTER 1. INTRODUCTION **5**

CHAPTER 2. SECURITY VULNERABILITIES **6**
Woodward's Approach to Product Security 6
Inquiring about Security and Reporting Security Issues to Woodward 6
Download the Security Bulletin 7

CHAPTER 3. SYSTEMS SECURITY **8**
ICS Defense in Depth 10
Network Architecture 11
Device Hardening 13

CHAPTER 4. SECURITY ASSESSMENTS **16**

REVISION HISTORY **17**

Illustrations and Tables

Figure 2-1. Typical Gas Turbine Control System with Legacy Woodward Supplied Devices 8
Figure 2-2. Typical Engine Control System with Legacy Woodward Supplied Devices 9
Figure 2-3. ICS Defense in Depth Diagram 10
Figure 2-4. Network Architecture of Typical ICS Systems 11
Figure 2-5. Subzones in Level 0-2 Zone 12

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

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.

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. Do not remove the printed circuit board (PCB) from the control cabinet unless absolutely necessary. If you must remove the PCB from the control cabinet, follow these precautions:
   - Do not touch any part of the PCB except the edges.
   - Do not touch the electrical conductors, the connectors, or the components with conductive devices or with your hands.
   - When replacing a PCB, keep the new PCB in the plastic antistatic protective bag it comes in until you are ready to install it. Immediately after removing the old PCB from the control cabinet, place it in the antistatic protective bag.

Chapter 1. Introduction

Up until recently, the term "cybersecurity" was relatively uncommon in the industrial controls industry. However, in recent times, the frequency and complexity of cyberattacks targeting industrial control systems (ICS) and critical infrastructure have increased significantly. Cybersecurity breaches and ransomware attacks have led to plant failures, system downtime, and other availability issues. As a result, the industrial cybersecurity landscape is continually evolving, and it has become more critical than ever for ICS systems to integrate cybersecurity measures into their design. This includes implementing various security mechanisms and protections to address the challenges posed by these attacks.

In response to these growing concerns, numerous regulations, standards, and security frameworks have been developed as industry norms for such applications. One of the most widely accepted standards is ISA/IEC 62443. Additionally, other frameworks, such as the National Institute of Standards and Technology (NIST) 800 series and IACS UR-E27 are also available to guide cybersecurity practices. However, some Woodward controllers and systems were designed before these standards were introduced. As a result, certain criteria, such as adherence to the Secure Development Lifecycle (SDL), were not considered during their development.

This does not mean that these devices are less secure; they include various security mechanisms. However, during their design, priority was primarily placed on equipment availability, process reliability, and equipment safety. The intent of this application note is to provide guidelines to assist users in securely deploying legacy controllers within their systems.

Chapter 2.
Security Vulnerabilities

Understanding and Addressing Security Vulnerabilities

A security vulnerability is an unintended characteristic of a component or system configuration that increases the risk of an adverse event or loss occurring. These vulnerabilities can arise from accidental exposure, deliberate attacks, or conflicts with new system components. Essentially, a vulnerability is a weakness within a system, its security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Addressing these vulnerabilities is critical to ensuring robust security and minimizing risks.

Risk and vulnerability assessments are the foundation of any effective security policy implementation. These assessments examine the current state of security from multiple angles, including technologies, policies, procedures, and user behaviors. By conducting a vulnerability assessment, organizations can gain a comprehensive understanding of their security posture (current risk state) and identify the mitigation techniques required to reach an acceptable risk state.

A thorough vulnerability assessment typically involves collaboration between a multidisciplinary team, including members from both Operational Technology (OT) and Information Technology (IT) departments. This collaborative approach ensures that all facets of security—technical, procedural, and behavioral—are addressed during the assessment and subsequent policy development.

Woodward's Approach to Product Security

As an Original Equipment Manufacturer (OEM), Woodward recognizes the importance of security in its products and has proactively invested in both people and technology to address vulnerabilities. Woodward's approach to security involves providing detailed and actionable information about vulnerabilities to help customers make informed decisions on how to improve their security. By adopting a proactive stance, Woodward demonstrates its commitment to helping customers manage risks and maintain secure systems. Below is the typical process flow diagram followed by Woodward to address security-related issues.

Inquiring about Security and Reporting 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.

Download the Security Bulletin

When defects or vulnerabilities in Woodward control software are discovered, an internal Woodward team 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. Navigate to:
Support > Industrial Support > Product Documentation and Software > Manuals, Software, and License Keys.

Chapter 3.
Systems Security

Woodward is a leading manufacturer of a wide variety of components that are integral to equipment and systems operating in various industries, plants, and sectors. Woodward's products are deployed in mission-critical applications, making security a top priority. To ensure the safety and reliability of these systems, it is essential to understand the security risks associated with the devices and their applications. Below are the typical examples of systems where Woodward products are used in the field.

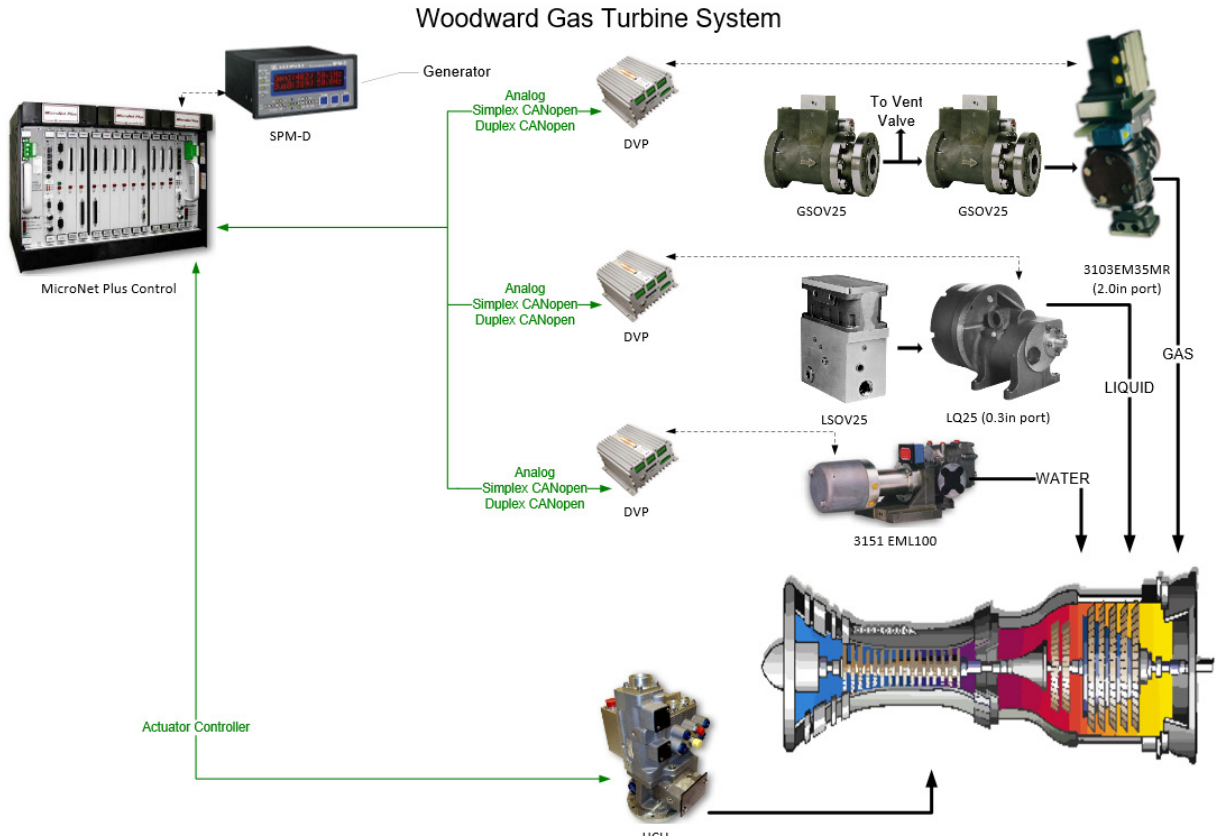

Figure 2-1. Typical Gas Turbine Control System with Legacy Woodward Supplied Devices

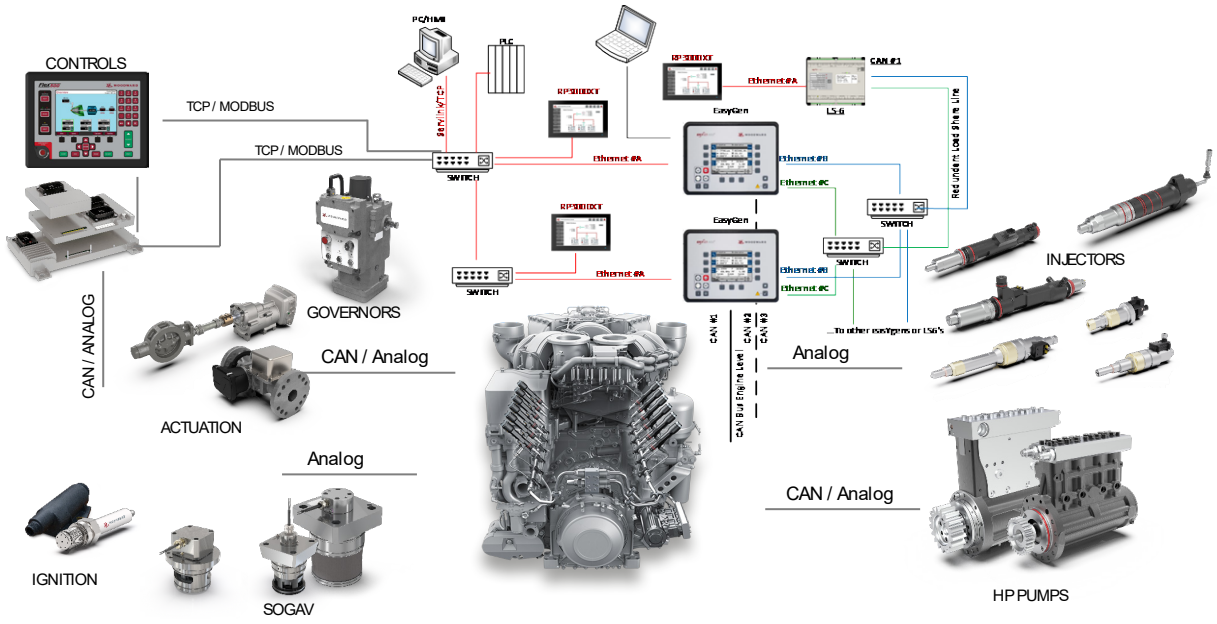

Figure 2-2. Typical Engine Control System with Legacy Woodward Supplied Devices

In typical systems like the ones shown above, various components such as mechanical valves, electro-mechanical actuators/solenoids, programmable controllers, and drivers work together to ensure seamless prime mover operation. Each of these components plays a distinct role within the system, but the cybersecurity risks associated with them can vary significantly due to their unique functions, levels of connectivity, and exposure to external threats. For instance, mechanical valves, which primarily rely on physical mechanisms, may have minimal exposure to cyber risks unless they are integrated with sensors, controllers, or external networks. Conversely, programmable controllers, being highly programmable and often connected to routable interfaces, are more susceptible to cyber threats such as unauthorized access, malware, or denial-of-service attacks. This diversity in risk profiles underscores the need for a tailored approach to cybersecurity for each device type.

These systems typically incorporate both routable and non-routable communication protocols. Routable communication in OT environments refers to data transmissions that utilize addressable protocols, such as TCP/IP, enabling devices to communicate across different network segments. For example, programmable controllers often rely on routable protocols for tasks like remote monitoring, control, and data exchange with systems such as plant Distributed Control Systems (DCS). In contrast, non-routable communication involves data confined to local devices or systems, using protocols or interfaces that lack network-layer addressing. Examples of non-routable protocols include serial communication standards like RS-232, RS-485, CAN, and direct point-to-point connections between sensors, actuators, and controllers. Non-routable communication is typically employed in isolated or legacy systems where external connectivity is unnecessary or undesirable.

Given the varying risks associated with routable and non-routable communication, security strategies must be tailored to address the specific vulnerabilities of each type. For routable communication, robust network defenses are essential, including firewalls, intrusion detection systems, network segmentation, and encrypted data transfers to mitigate threats like unauthorized access, malware, and denial-of-service attacks. Devices such as programmable controllers, which depend on routable protocols, require strict access controls and regular audits to maintain their integrity. For non-routable communication, security measures focus on safeguarding physical and logical access to components. Physical security controls, such as restricted access to devices, and secure firmware updates are vital for mitigating risks in systems where external connectivity is unnecessary or poses additional vulnerabilities.

By tailoring security measures to the distinct characteristics of routable and non-routable communication, organizations can effectively minimize vulnerabilities, protect critical system components, and enhance the overall resilience of their OT systems. This targeted approach ensures that each type of communication is secured according to its risk profile, reducing the likelihood and impact of cyber threats.

ICS Defense in Depth

While securing Industrial Control Systems (ICS) may initially appear complex, implementing a Defense-in-Depth strategy can be streamlined into practical, actionable steps. This multi-layered security approach begins by addressing fundamental questions:

1. Where can attackers gain entry into the ICS?
2. What actions could attackers take once inside?
3. What are the ultimate objectives of an attack?

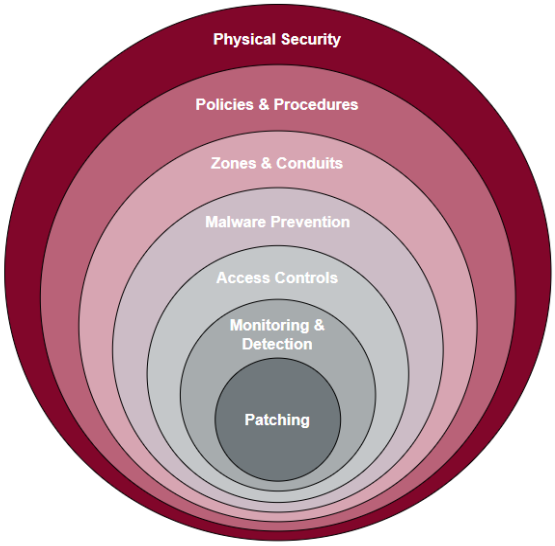

Figure 2-3. ICS Defense in Depth Diagram

By systematically answering these questions, organizations can design and implement layered security measures tailored to their systems. One layer involves securing entry points through firewalls, intrusion detection systems, and physical access controls to prevent unauthorized access. Another layer emphasizes creating barriers to slow, detect, or deflect attackers, such as network segmentation, endpoint protection, and encrypted communications. Additionally, hardening the most critical system components ensures that even if earlier defenses are breached, attackers are unable to achieve their intended objectives.

The primary objective of Defense in Depth is to create a robust and resilient system that makes attacks exceedingly challenging and resource-intensive, ultimately deterring or preventing them altogether. This strategy combines technical controls, physical safeguards, and procedural measures to restrict access to the ICS and tailor user privileges based on roles and responsibilities.

The effectiveness of this approach is enhanced by fostering a security-conscious culture within the organization, ensuring that technical defenses are complemented by active organizational commitment and employee engagement. An ICS fortified with layered defenses and supported by a proactive workforce is exceptionally well-equipped to resist and recover from threats. Through the integration of strategic planning, technical controls, and operational practices, ICS Defense in Depth provides a professional and effective solution for securing critical systems against evolving cyber risks.

Network Architecture

Network segmentation is a foundational strategy for protecting Industrial Control System (ICS) environments by dividing networks into smaller, more manageable zones with controlled communication between them. This approach limits the potential impact of cyber threats, prevents unauthorized access, and enhances system resilience against attacks. By isolating critical ICS components from less secure or external networks, organizations can effectively reduce attack surfaces while ensuring the integrity, availability, and reliability of industrial processes. To implement network segmentation effectively, industry standards such as ISA/IEC 62443 and PERA (Purdue Enterprise Reference Architecture) provide valuable guidance on designing secure and resilient system architectures. In the following sections, we will explore how these principles are applied to Woodward systems.

ISA/IEC 62443 and PERA are widely recognized as best practices for designing secure system architectures in industrial environments. ISA/IEC 62443 offers a structured approach to cybersecurity, focusing on layered defenses, risk assessment, and tailored security measures for various zones and components within the system. PERA complements this by providing a hierarchical model for system design, dividing networks into distinct levels to effectively separate enterprise IT systems from operational technology (OT) systems. Together, these frameworks enable system designs to incorporate robust network segmentation, secure data flows, and access controls, reducing vulnerabilities while ensuring compliance with industry regulations. Building upon these standards, Woodward systems are typically implemented using a structured architecture that incorporates the principles of zones and conduits.

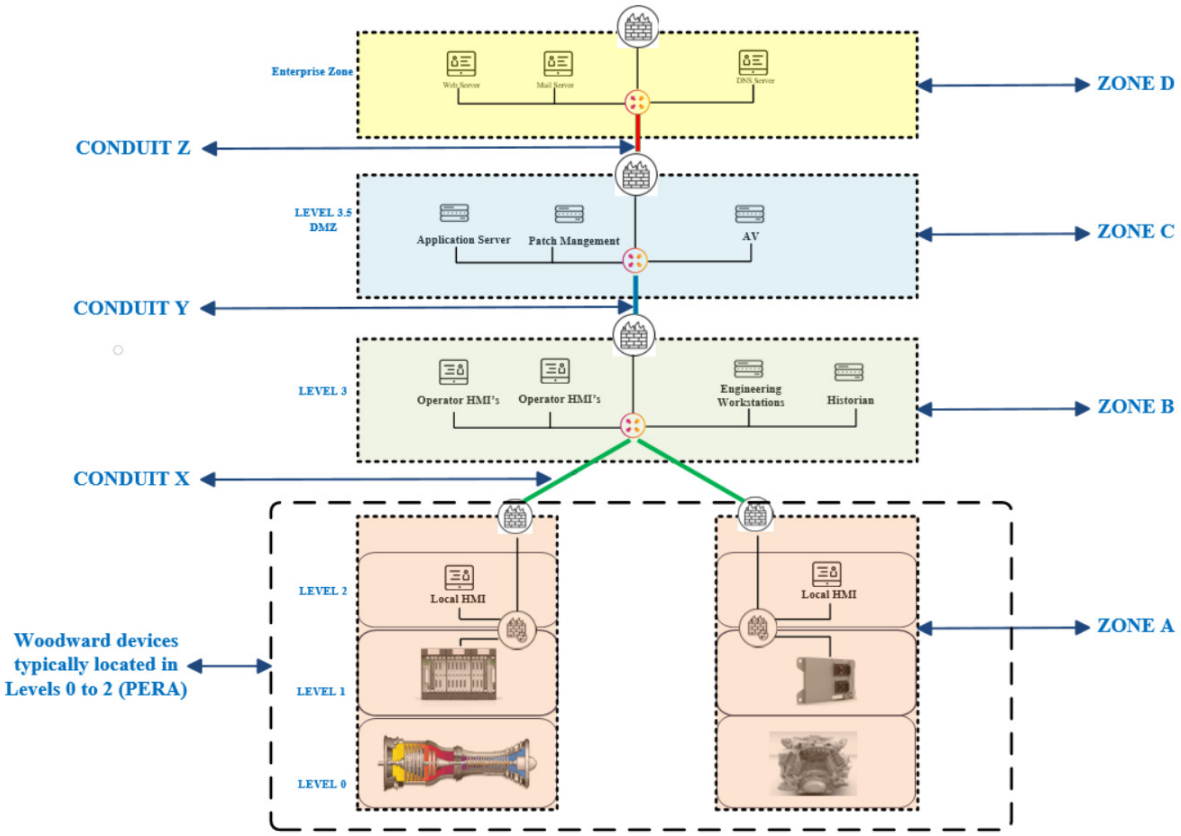

Figure 2-4. Network Architecture of Typical ICS Systems

Above is the typical architecture for Woodward systems, where most of the equipment supplied falls under Levels 0-2 (Physical, Policy, Zones, and Conduits) of the Purdue Enterprise Reference Architecture (PERA). In such architectures, networks are typically divided into zones and conduits to enhance security and ensure proper segmentation. According to the ISA/IEC 62443 standard, a security zone is a collection of physically and functionally united assets that share similar security requirements. These zones are defined based on the physical and functional models of the industrial system control architecture, grouping assets with common security needs to simplify management and protection. While

zones group assets with similar security needs, conduits serve as the communication pathways between these zones, ensuring secure and controlled information exchange. As described in the ISA/IEC 62443-3-2 standard, conduits are a special type of area that contains communication channels, such as networks, cables, routers, switches, and firewalls, which connect two or more zones. Conduits enable the secure flow of information within, into, or out of a security zone, including communication with programming terminals, mobile devices, and vendor connections. Trusted conduits typically remain within the same security level, while untrusted conduits connect zones with differing security levels. Secure communication methods can enhance the trustworthiness of these conduits, virtually extending the security properties of a zone. Within this zone-and-conduit architecture, Woodward devices are deployed to ensure secure and efficient operation of industrial processes.

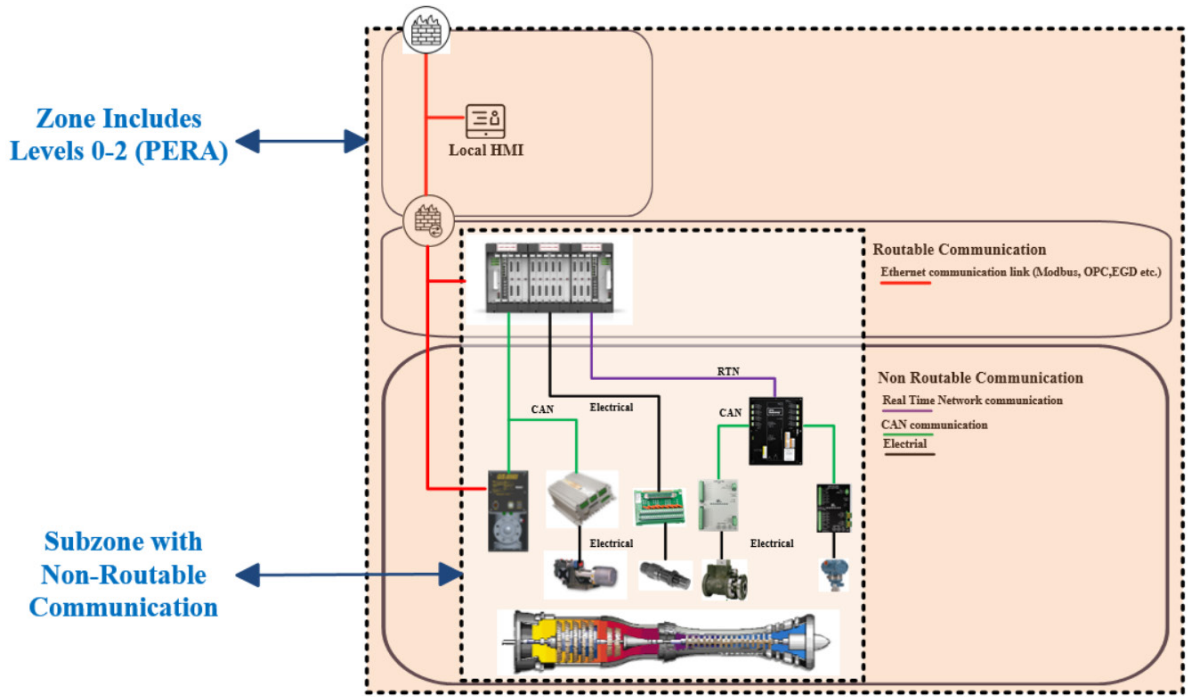

Figure 2-5. Subzones in Level 0-2 Zone

Within an industrial control system (ICS) environment, zones can be further divided into smaller subzones to enhance security. One such subzone may consist of components that rely on non-routable communication. Protection for this type of subzone is typically implemented through strict physical access controls, and it is essential for organizations to enforce robust physical security measures to prevent unauthorized access. For any routable traffic, communication should be directed through boundary protection mechanisms, such as secure routers or firewalls, which are strategically placed at the perimeter of each zone or subzone. These boundary protection devices serve as gatekeepers, ensuring that only validated and trusted traffic is allowed to flow between zones and subzones. Proper configuration and management of these boundary protection devices are critical to maintaining the security and reliability of ICS equipment, such as Woodward devices, in industrial applications. These devices are programmed to filter network traffic based on predefined security policies, enabling administrators to control parameters such as communication ports, IP addresses, and protocols. By deploying secure routers or firewalls, organizations can mitigate network threats, including denial-of-service (DoS) attacks, IP spoofing, and unauthorized access attempts. This layered security approach provides an additional defense mechanism, ensuring that only authorized and trusted traffic reaches critical ICS components. The ability to configure port filtering, protocol restrictions, and IP address controls allows organizations to design a tailored security framework that meets the specific requirements of their deployment.

Effective communication management between Woodward devices and other components in the network relies on adhering to strict security guidelines. The communication ports used by Woodward controllers and devices are outlined in the respective product security manuals provided by Woodward. These

manuals should be consulted during integration to ensure that the boundary protection devices are configured to allow the necessary communication channels. Additionally, project-specific network architecture drawings should be referenced to obtain a detailed IP address list for the devices. This ensures that all devices are properly integrated into the network and that communication flows are securely managed.

Deploying Woodward devices within secure zones and utilizing boundary protection devices is a critical step in designing resilient and secure industrial networks. By adhering to industry standards such as ISA/IEC 62443 and PERA, organizations can implement robust network segmentation, secure communication flows, and tailored security measures to protect critical systems. Consulting product manuals, referencing project-specific network architecture drawings, and following best practices will ensure the safe and efficient operation of Woodward devices while maintaining a strong defense against evolving cyber threats.

Device Hardening

Device hardening is a critical aspect of securing industrial control systems, particularly in environments where a variety of legacy devices with differing features are utilized. As these devices often lack uniform security capabilities, it is essential to consult individual product manuals for detailed information on available features. However, there are several universal best practices that can be applied to enhance the security of all devices. This chapter will outline these practices, focusing on physical security measures and supply chain risk mitigation.

Physical Security Measures

Protecting the physical integrity of devices is the first line of defense against unauthorized access or tampering. The following measures can help secure both devices housed in cabinets and those without enclosures.

To safeguard industrial control devices from unauthorized access and tampering, utilizing locked cabinets specifically designed for such equipment is crucial. These cabinets should be installed in restricted areas equipped with controlled access and video surveillance to enhance security. For added durability, consider cabinets with impact-resistant designs to resist forced entry or environmental damage. Additionally, tamper-evident seals featuring unique serial numbers and authorized personnel signatures should be applied to cabinet doors and critical components. Broken seals act as a clear indicator of potential tampering and must prompt immediate investigation. To further bolster security, maintain a logbook to record the application and removal of seals, including timestamps and the names of responsible personnel. Audit seals can also be used on specific device ports or access points to effectively monitor and deter unauthorized access attempts.

If cabinets are not feasible, alternative physical security strategies can be explored. Use designated secure areas with restricted access to limit exposure to unauthorized personnel. Install physical barriers such as cages or enclosures to create restricted zones or mount devices on secure walls or surfaces to prevent unauthorized removal. For standalone devices, applying tamper-evident labels can help detect and deter tampering attempts.

Regular inspections and audits are key to maintaining physical security. Conduct routine inspections to identify damage or signs of tampering in security measures. Additionally, perform periodic audits to ensure logbooks are properly maintained and seal application protocols are consistently followed.

Supply Chain Risk Mitigation

Securing devices begins well before they are deployed in the field. Supply chain risks, such as counterfeit or tampered equipment, can compromise system integrity. Implementing robust supply chain risk mitigation practices is essential to ensure the authenticity and safety of devices.

To detect tampering and counterfeiting, establish procedures to confirm the authenticity of received equipment. These may include visually inspecting the product for physical discrepancies or anomalies, comparing serial numbers against purchase orders and manufacturer records, and verifying that the

equipment was supplied by an authorized distributor offering anti-counterfeiting measures. Ensuring authenticity is critical to maintaining the integrity of the supply chain.

Purchasing equipment exclusively from Woodward authorized distributors is another vital step in mitigating supply chain risks. Creating a policy to avoid unauthorized resellers or grey market sources minimizes the risk of acquiring counterfeit or tampered products. Trusted sources ensure that the equipment meets required standards and safety protocols.

Packaging verification is an important process that should not be overlooked. Upon receipt, inspect the packaging for signs of tampering or inconsistencies with the manufacturer's standard packaging. Look for broken seals, mismatched labeling, or other irregularities that may indicate tampering. Establish clear protocols for handling and reporting damaged or improperly sealed packaging, ensuring that such equipment is not deployed until its authenticity is verified.

Finally, when downloading software or firmware updates, always use Woodward's official download portal. Avoid third-party websites or unauthorized sources, which may host outdated, counterfeit, or malicious software versions. This ensures that the software being deployed is genuine and secure, protecting the devices from potential vulnerabilities in the supply chain.

Workstation Hardening

To ensure robust system security and operational efficiency, organizations must adopt a comprehensive approach that encompasses workstation management, endpoint protection, access control, peripheral security, backup processes, and timely patching. Workstations should be dedicated exclusively to operator (HMI, Historian, etc.) and engineering functions (Configuration, commissioning and software update etc), with all unnecessary applications, services, and ports removed. This approach minimizes the system's attack surface and eliminates vulnerabilities stemming from extraneous software or configurations. By streamlining workstation functionality, organizations can ensure optimal performance while reducing exposure to security risks.

Endpoint protection is a critical component of system security. Antivirus and anti-malware software must be installed on all systems to detect, block, and remove malicious threats. To maintain effectiveness against emerging threats, definition files must be kept up to date, ensuring the software can identify and address the latest vulnerabilities. Regular updates are essential for safeguarding systems against advanced malware and cyberattacks, which are constantly evolving.

Minimizing access to administrative rights is another vital security measure. Administrative privileges should only be granted to essential personnel who require them to perform specific functions. Restricting administrative access reduces the risk of accidental or intentional changes to system configurations and prevents malware from exploiting elevated privileges to compromise systems. This principle of least privilege ensures tighter control over sensitive system settings and operations.

Peripheral devices, such as USB, CD, and DVD drives, are common vectors for malware and unauthorized data transfers. To mitigate these risks, organizations must secure these devices and restrict their use to authorized purposes only. Policies should be implemented to regulate access and ensure that only trusted personnel can utilize these peripherals. This reduces the likelihood of data breaches and malicious software propagation.

Implementing a validated backup and restore process is crucial for protecting critical data and systems. Regular backups ensure that important information is preserved, while periodic validation through test restores confirms the integrity of the backup data and the reliability of restoration procedures. A robust backup strategy should include redundant storage solutions, such as offsite and cloud-based repositories, to safeguard against localized damage or disasters. Integration of the backup process into the organization's disaster recovery plan ensures rapid restoration of systems during emergencies, minimizing downtime and operational disruptions.

Finally, installing up-to-date security patches validated by the engineering team is essential for addressing known vulnerabilities and enhancing system resilience. These patches provide critical updates that mitigate risks posed by exploits, bugs, and outdated configurations. Prompt installation of

validated patches ensures that systems remain secure and capable of withstanding evolving threats. Regular collaboration between the engineering team and IT personnel is key to ensuring that patches are properly tested and deployed without introducing disruptions to operations.

By combining these measures, dedicated workstations, endpoint protection, restricted administrative access, secure peripherals, validated backup processes, and timely patching—organizations can create a robust security framework that protects critical systems, reduces vulnerabilities, and ensures operational reliability in the face of evolving cybersecurity challenges.

Chapter 4.
Security Assessments

Organizations undergoing security assessments for legacy devices are recommended to adopt a comprehensive, system-level security approach to address the inherent limitations of these devices. Legacy devices, often classified as Security Level 0 (SL0) under the ISA/IEC 62443 standard, lack inherent security capabilities and should rely on physical and environmental controls for their protection. Measures such as securing devices in locked enclosures, cabinets, or restricted areas, and limiting physical access to authorized personnel, supported by audit trails and tamper-evident measures, are essential to mitigating risks. This approach is particularly critical for legacy devices integrated into larger plant control systems, where security must be managed holistically within the system context.

For Ethernet-enabled legacy devices, organizations should implement foundational security practices to mitigate the higher risks of cyber intrusion. These devices should be placed within secure, segmented network zones, separated by appropriate network security devices, and never within unprotected network boundaries. Security solutions, such as firewalls, intrusion detection systems, and secure remote access tools, compliant with ISA/IEC 62443-4-2 standards, should be used to protect these devices. Additionally, role-based access control (RBAC) and strong authentication mechanisms should be implemented to ensure that users only have access to resources necessary for their roles. These practices will enhance the security of Ethernet-enabled devices and reduce risks associated with network-based attacks, ensuring secure integration within the ICS environment.

For organizations seeking additional assurance, some legacy devices, such as Flex and Micronet Plus CPUs, have achieved Achilles Level 1 certification, an internationally recognized benchmark for device-level security. This certification confirms that the devices have been tested for robustness and resilience against known vulnerabilities and threats. Organizations can request Achilles certificates for certified products from Woodward, providing valuable evidence of compliance with established security standards during security assessments.

To address the risks posed by legacy controllers, organizations should adopt a system-level security approach that places these devices within secure zones. These zones should incorporate strong physical and network security measures to isolate and protect legacy controllers while maintaining their operational functionality within the broader plant control system. By adopting this perspective, organizations can address the limitations of legacy controllers while ensuring compliance with applicable security standards and best practices.

In summary, organizations are advised to implement physical and environmental restrictions for SL0 legacy devices, adhere to foundational security practices for Ethernet-enabled devices, utilize certified devices like those with Achilles Level 1 certification, and adopt a system-level security approach for legacy controllers. By following these recommendations, organizations can effectively address security assessments and strengthen the overall security posture of their ICS environments.

Revision History

Revision A—

- New release

Released

We appreciate your comments about the content of our publications.

Send comments to: industrial.support@woodward.com

Please reference publication 51654.

B 5 1 6 5 4 : 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.