System Security Design Guidelines

Allen-Bradley
by ROCKWELL AUTOMATION

Reference Manual

Original Instructions

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.

SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

This publication provides guidelines for how to use Rockwell Automation products to improve the security of your industrial automation system.

For information on patch management options, security advisory details, and general news and awareness on industrial security from the Rockwell Automation Office of Product Safety and Security, see the Industrial Cybersecurity capabilities web page.

The Knowledgebase Technote *Industrial Security Advisory Index* points to specific product security alerts, advisories, and recommendations. Subscribe to this index to receive notifications.

To address specific concerns, or to report issues, contact us at secure@ra.rockwell.com. Communicate securely via our PGP Public Key Block.

How Can I Get Help To Manage My Security Risk?

Rockwell Automation Network & Security Services consulting services are available to assist customers assess and improve the state of security of industrial control systems that use Rockwell Automation and other vendor control products. We provide a holistic approach to manage your network infrastructure and security throughout its lifecycle. For more information, see Industrial Cybersecurity Services.

Summary of Changes

This manual contains the following new information as indicated.

Topic	Page
New chapter on vulnerabilities, how to report suspected vulnerabilities, and how Rockwell Automation responds to reports.	7
Updates to patch management	31
Updates to version descriptions for software and firmware	33

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

Resource	Description
Security Configuration User Manual, SECURE-UM001	Describes how to configure and use Rockwell Automation products to improve the security of your industrial automation system.
CIP Security with Rockwell Automation Products Application Technique, SECURE-AT001	Describes how to implement the Common Industrial Protocol (CIP™) Security standard in your control system.
Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, publication ENET-TD001	Provides guidelines for how to design, implement, and manage industrial Ethernet networks.
Industrial Firewalls within a Converged Plantwide Ethernet Architecture White Paper, publication ENET-WP011	Provides guidelines for how to implement industrial firewalls.
Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD002	Outlines use cases for how to design, deploy, and manage industrial firewalls.
Guidelines on Firewalls and Firewall Policy	Recommendations of the National Institute of Standards and Technology
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for how to install a Rockwell Automation industrial system.
Product Certifications website, http://www.rockwellautomation.com/global/certification/overview.page	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at http://www.rockwellautomation.com/global/literature-library/overview.page. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

Vulnerabilities

A vulnerability is a flaw or weakness in a product or system that can be exploited to compromise product or system confidentiality, integrity, or availability.

Risk and vulnerability assessments are the starting point for any security policy implementation. Vulnerability assessments examine your situation from technologies, policies, procedures, and behaviors. An assessment provides a picture of your current security posture (current risk state) and what you need (mitigation techniques) to get to a preferred state (acceptable risk state). Rockwell Automation recommends the formation of a multi-discipline team of operations, engineering, IT, and safety representatives to collaborate in the development and deployment of your industrial security policy.

A vulnerability assessment provides, at a minimum:

- An inventory of existing devices and software.
- Detailed observation and documentation of intended system operation.
- Identification of possible vulnerabilities.
- Prioritization of each vulnerability based on the impact and exploitation potential.

The Common Vulnerability Scoring System (CVSS) is a free, open industry standard for assessing the severity of vulnerabilities. Rockwell Automation includes CVSS-based scores in Product Security Advisory notices to help customers assess their risk and exposure, including how prioritize responses and resources according to a specific threat. For more information, see Common Vulnerability Scoring System Specification Document.

The outcome of a vulnerability assessment can include mitigation techniques that bring an operation into an acceptable risk state.

Actions that are taken after a risk assessment can include the following:

- New firewall controls
- New switch ports to lock down
- Stronger password policies
- Removal of unused software programs
- Improved procedures for managing the connection of external devices, such as USB devices
- New or patched versions of firmware or software

How Rockwell Automation Handles Vulnerabilities

Rockwell Automation recognizes the importance of security in industrial control systems and is investing in its products, people, partnerships, and integrated consulting services (Network & Security Services – NSS) to enhance the security in our products and maintain productivity. Rockwell Automation provides detailed and actionable information about security vulnerabilities to help customers make informed decisions on what steps they need to take to improve their security.

Report a Suspected Product Vulnerability

Rockwell Automation encourages submissions of suspected vulnerabilities as soon as they are discovered. Rockwell Automation maintains a formalized process to identify, assess, and remediate reported vulnerabilities for those products that are in the Active or Active Mature state.

The Product Security Incident Response Team (PSIRT) at Rockwell Automation responds to suspected vulnerabilities within Rockwell Automation products. Reporters are strongly encouraged to file a vulnerability report with the PSIRT via email at secure@ra.rockwell.com.

The PSIRT works with reporters to understand and validate reports. The PSIRT:

- Requests that the reporter keep any communication confidential
- Assigns a tracking ID to the vulnerability report
- Reviews and responds, usually within two business days
- Advises the reporter of significant changes in the status of any vulnerability reported to the extent possible without revealing information provided to us in confidence
- Works to remediate reported vulnerabilities in a timely manner.

The Rockwell Automation PSIRT encourages the encryption of sensitive information prior to sharing over email. To request instructions on how to use our public key, contact us at secure@ra.rockwell.com.

The Rockwell Automation PSIRT may contact the reporter via email or an another agreed upon communications mechanism throughout the disclosure process.

The PSIRT asks that reporters adhere to the following:

- Play by the rules. This includes following the guidelines, as well as any other relevant agreements.
- Report any vulnerability discovered promptly.
- Avoid violating the privacy of others, disrupting our systems, destroying data, or harming user experience.
- Use only our PSIRT email to discuss vulnerability information with us, unless otherwise agreed upon with the PSIRT.
- Keep the details of any discovered vulnerabilities confidential until Rockwell Automation identifies a resolution.
- If a vulnerability provides unintended access to data, limit the amount of data you access to the minimum required to demonstrate the issue. Cease testing and submit a report immediately if you encounter any user data during testing, such as personally identifiable information (PII), personal healthcare information (PHI), credit card data, or proprietary information.
- Only interact with test accounts you own or with explicit permission from the account holder.
- Do not engage in extortion.
- Comply with all applicable laws.

Public Vulnerability Disclosure

The PSIRT discloses vulnerability details, mitigations, and solutions via the Knowledgebase Technote *Industrial Security Advisory Index*.

You can find additional information on the Industrial Cybersecurity capabilities web page.

Rockwell Automation recognizes the hard work of reporters and provides recognition within the advisories, unless otherwise specified. We recognize reporters if they are the first to report a unique vulnerability and the report triggers a product change.

The Rockwell Automation Vulnerability Disclosure Policy draws on the United States Core Terms compiled by disclose.io, the vulnerability disclosure guidance set forth by the CERT Coordination Center (CERT/CC) at Carnegie Mellon University, and ISO 29147 and ISO 30111, which define standards for receiving and processing vulnerability reports. Rockwell Automation defines a reporter as an individual or organization that notifies a vendor or coordinator of a suspected product vulnerability. Coordinators, on the other hand, are defined as an individual or organization that coordinates vulnerability information to affected parties.

When conducting vulnerability research according to this policy, Rockwell Automation considers the research to be:

- Authorized in accordance with the Computer Fraud and Abuse Act (CFAA) (and/or similar state laws). Rockwell Automation will not initiate or support legal action against you for accidental, good faith violations of this policy.
- Exempt from the Digital Millennium Copyright Act (DMCA). Rockwell Automation will not bring a claim against you for circumvention of technology controls.
- Exempt from restrictions in our Terms & Conditions that would interfere with conducting security research. Rockwell Automation waives those restrictions on a limited basis for work done under this policy.
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please email secure@ra.rockwell.com. before going any further.

Supply Chain Vulnerabilities

Rockwell Automation also prioritizes supply-chain vulnerabilities, especially if a vulnerability affects more than one Rockwell Automation product. The PSIRT accept reports regarding third-party components if the vulnerabilities are disclosed in a multi-party, coordinated effort supported by a third-party coordinator such as DHS CISA or the CERT/CC.

Threat Model

Threat modeling is a procedure to analyze network, application, and physical security. A threat model identifies objectives and vulnerabilities, and then defines countermeasures to mitigate the effects of threats to the system.

1. Describe the assets to protect.

   Create classes of assets and information that you want to protect. For example, a controller, the controller configuration, or recipe data in the controller. Be as specific as possible. For example, include the following:

   - serial number
   - MAC ID
   - IP address
   - user access
   - device dependencies

   Prioritize the assets. Define the type of protection for each asset - confidentiality, integrity, or availability.

2. Describe the policies that govern the assets

   The policies are typically control-based in that they define who can do what to which asset. Other policies can define attributes such as asset availability, version control, or confidentiality requirements.

   Because policies are written in a general manner, they are supported with procedures, standards, and guidelines to provide the details on how to implement, enforce, and monitor the policy.

3. Characterize the assets and their supporting systems

   Examine the assets in their information systems and identify information flows that affect the assets. Characterize the systems and software that are part of the information flow.

   - How are the assets accessed?
   - Who can copy, move, or modify them?
   - What methods can be used to interact with them?
   - Do they exist in multiple locations?
   - How are multiple copies synchronized?

4. Identify threats to the assets

   For each asset, identify how and where to enforce the policy that governs the asset. Based on the type of protections for the asset, examine the information flows, systems characterizations, and enforcement mechanisms. Identify potential threats (such as threats to confidentiality, threats to integrity, and threats to availability).

   For example:

   - 'System goes off line' is a threat to availability.
   - 'Database synchronization fails' is a threat to integrity.

5. Characterize the threats

   For each threat, enumerate the mechanisms (vulnerabilities) that can cause the potential threat to become an actual threat. Keep the vulnerabilities as broad as possible in scope.

6. Visualize

   Use a network diagram and overlay system information, asset locations, information flows, enforcement points, and vulnerabilities. Annotate the diagram with available resources (people, money, equipment).

   Use this visualization as a method to divide the system into manageable pieces. This visualization also shows relationships and possible consequences when you make changes.

7. Strategize

   Use the visualization to find:

   - Patterns that suggest enterprise-wide solutions rather than local or point solutions.
   - Interactions of resources and ease of affecting the network.
   - Possibilities of vulnerabilities being exploited.
   - Develop backup and restore procedures.

   Group vulnerabilities and their locations. Identify methods to address as many of the vulnerabilities as possible with one change or small set of changes.

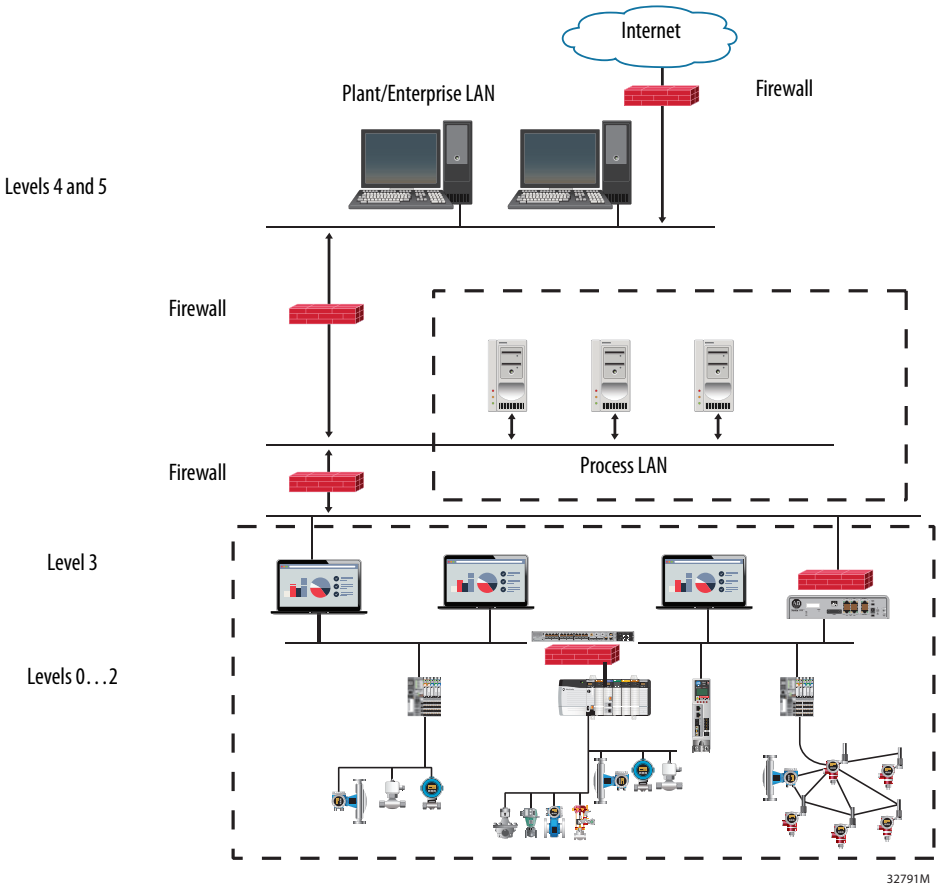
   Remember that not all vulnerabilities need new technology to address the issues. Proper configuration, privilege, and access control are key, and can often be improved without harming production facilities.

8. Verify
   - Map every proposed change directly to a threat to an asset.
   - Make sure that the change does not introduce a new threat to another asset.

Verify that no policy enforcement point can be circumvented.

System Security

Just as the nature of manufacturing and industrial operations has changed, so have the security risks. More connected operations can create more potential entrance points for industrial security threats. Threats can come in many forms – physical versus digital, internal versus external, or malicious versus unintentional.



In the industrial automation and control system (IACS), follow common industry standards, such as the Purdue Enterprise Reference Architecture model, to define:

- Security zones - those assets that have the same security requirements
- Trusts within security zones - relationships between assets that support identification, authentication, accountability, and availability.

Industrial security must address a wide range of concerns, including:

- Safeguard intellectual property and other valuable information.
- Safeguard operations from intrusions that could impact productivity, product quality, operator safety, or the environment.
- Maintain critical infrastructure systems, especially systems in regulated areas like energy and water/waster-water management.
- Maintain high-availability traffic policies for networks.
- Enable and control remote access to industrial operations.

Security Basics

Industrial security must be comprehensive. Extend security policies from the enterprise through the plant level and to end devices. Address risks across your people, processes, and technologies. Involve collaboration between IT and OT personnel for design, management, and regular communication on expected system functional requirements and policy compliance.

A robust approach to security includes the development and implementation of the appropriate activities to complete the following steps:

- Identify the cybersecurity risk to systems, assets, data, and capabilities.
- Protect critical infrastructure services.
- Detect cybersecurity events.
- Respond to a detected cybersecurity event.
- Recover from and restore any capabilities or services that were impaired due to a cybersecurity event.

Cybersecurity is the collection of technologies, processes and practices that help protect networked computer systems from unauthorized use or harm. Cybersecurity addresses cyber- attacks, which are offensive in nature and emphasize network penetration techniques, and cyber-defenses, which are defensive in nature and emphasize counter-measures intended to help eliminate or mitigate cyber- attacks.

The main goals of cybersecurity in an industrial setting:

- **Availability:** maintain and never give up control in a control system
- **Confidentiality:** protect proprietary information and only let individuals with a need-to-know have access to the information
- **Integrity:** ensure that the information flowing through the system has not been tampered with

Security Standards

There are a number of resources that organizations can use as a basis to manage security and risk within the IACS. These resources can help organizations develop a security management program.

Resource	Description
ISA/IEC 62443 Standard	Industrial Automation and Control Systems (IACS) Security (formerly ISA-99) This standard addresses network and system security and defines the provision of multiple security protections, especially in layers, with the intent to delay, if not block, an attack. This standard also recommends password structures.
NIST 800-82 Framework	Guide to Industrial Control Systems (ICS) Security This framework provides recommendations for securing an IACS. The standard covers the use of firewalls, the creation of demilitarized zones and intrusion detection capabilities, along with effective security policies, training programs, and incident response mechanisms.
NIST Cybersecurity Framework	This framework provides guidelines that help organizations align cybersecurity activities with business requirements, risk tolerances, and resources.
NCCIC Agency	National Cybersecurity and Communications Integration Center This agency provides recommendations for secure architecture design.

The United States Department of Homeland Security (DHS) includes the Cybersecurity & Infrastructure Security Agency (CISA). CISA manages a repository of alerts, advisories, and reports (ICS-CERT) for industrial control systems.

- **Alerts:** provide timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks.
- **Advisories:** provide timely information about current security issues, vulnerabilities, and exploits.
- **Reports:** provide Technical Information Papers (TIPs), Annual Reports (Year in Review), and 3rd-party products applicable to industrial control system owners/operators.
- **Newsletters:** periodic publication of security news and information applicable to industrial control system owners/operators.

For more information, see Cybersecurity and Infrastructure Security Agency > Industrial Control Systems.

Defense-in-Depth Security

Industrial security is best implemented as a complete system across your operations. Common to security standards is the concept of defense-in-depth (DiD). DiD security establishes multiple layers of protection based on diverse technologies through physical, electronic, and procedural safeguards. Just like a bank uses multiple security measures – such as video cameras, a security guard, and a vault – DiD helps make sure that threats encounter multiple lines of defense. DiD also assumes the implementation of cybersecurity policies that include operations planning, user training, and physical access security measures.

A defense-in-depth security approach consists of six main components:

- Policies and Procedures
- Physical
- Network
- Computer
- Application
- Device

Defense-in-depth employs a comprehensive approach to leverage multiple methods to mitigate risks. To apply defense-in-depth, understand the relationship of intruders (threats and threat actors) and vulnerabilities to the controls (standards, detection methods, and countermeasures).

A threat actor, through intent, capability, or opportunity, poses a threat to the IACS when the threat compromises operations, personnel, or technology and exploits an existing weakness or vulnerability. Base countermeasures on best practices, standards, and established company security policies. Countermeasures protect critical assets through multiple layers of defense. Organizations must constantly adjust and refine security countermeasures to maintain protection against known and emerging threats.

Notifications That Rockwell Automation Provides

Rockwell Automation provides these types of product notices.

Notification	Description	Customer Action
Product Safety Advisory (PSA)	Issued when a product failure may result in significant loss of capital equipment, personal injury, or death.	Required
Product Notice (PN)	Issued when a product failure may result in significant commercial loss or customer dissatisfaction.	Strongly Recommended
Product Security Advisory	Issued for security alerts and security recommendations where such risks stem from cyber-attacks. These advisories are intended to raise customer awareness of risks to affected product operation or performance and also supply relevant recommendations for how to reduce or remove the risk associated with a vulnerability.	Strongly Recommended

Security with Rockwell Automation Products

Security is not a static end state, it is an interactive process. No single product, methodology, or technology fully secures control networks. The remaining chapters in this reference manual highlight Rockwell Automation products that help manage:

- Identification, authentication, and user access
- Network segmentation and data flow
- Data confidentiality
- System integrity
- Resource availability and response to events

Standard Security Components

In addition to the Rockwell Automation products described in this publication, there are also references to these additional technologies.

Component	Description
Microsoft® Active Directory service	Use Active Directory for authentication and authorization in a Windows domain. Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. A server that runs the Active Directory Domain Services (AD DS) is called a domain controller. The domain controller authenticates and authorizes all users and computers in a Windows domain type network. The domain controller assigns and enforces security policies for all computers and software updates.
RADIUS protocol	You can use the Remote Authentication Dial-In User Service (RADIUS) protocol to manage access to the Internet or internal networks, wireless networks, and integrated email services. The RADIUS protocol is a network protocol that provides centralized authentication, authorization, and accounting (AAA) management for users. The RADIUS protocol is often used by Internet service providers (ISPs) and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated email services.
Cisco® TACACS+ protocol	You can use the Cisco Terminal Access Controller Access-Control System Plus (TACACS+) to manage remote authentication for networked access control through a centralized server. The Cisco TACACS+ protocol manages authentication, authorization, and accounting (AAA) services. The TACACS+ protocol uses the Transmission Control Protocol (TCP). Since TCP is a connection-oriented protocol, TACACS+ does not have to implement transmission control. TACACS+ encrypts the full content of each packet.
IEEE 802.1x authentication	You can use 802.1x authentication to manage port-based access for devices that want to connect to a network. 802.1x authentication secures communication between authenticated and authorized devices. You can connect this access control to the Active Directory to create a central administration connection for both network management and network access. This access control is the preferred method to create a central network access layer.

Notes:

Secure Networks and Communication

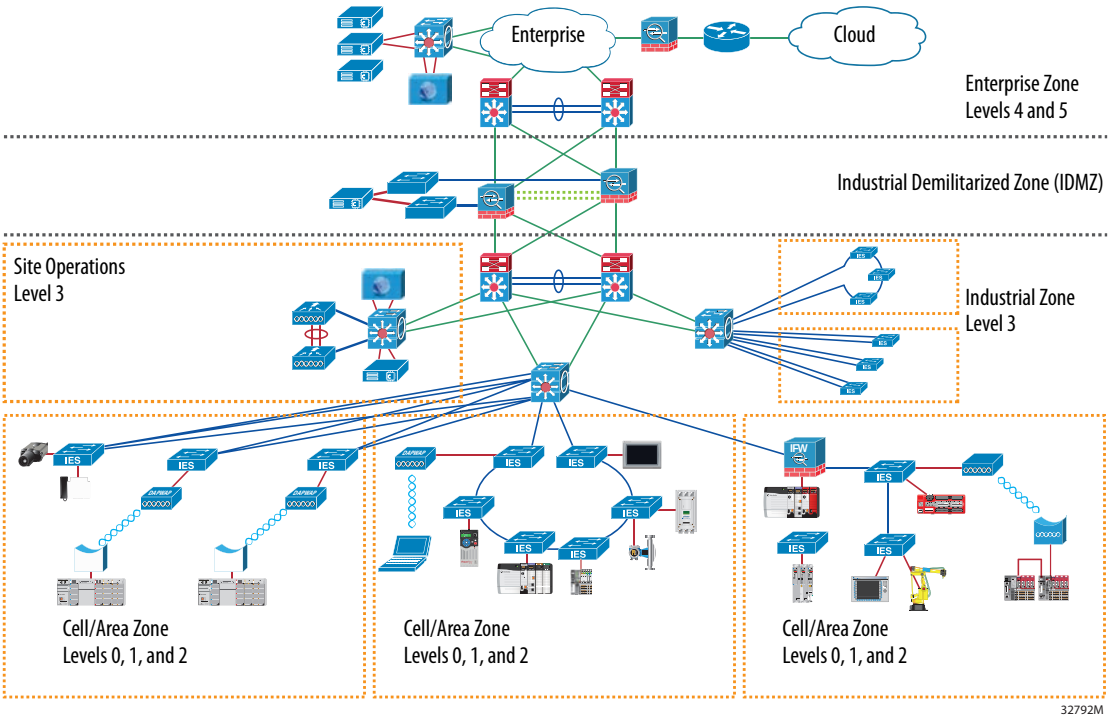
The continuing trend in networking is the convergence of technology, operational technology (OT) with information technology (IT). Technologies like the Ethernet and EtherNet/IP™ (Common Industrial Protocol over an Ethernet network) protocols help enable network technology convergence.

Network technologies that filter, block, and control access help secure networks. You can also select control products that offer security options.

Converged Plantwide Ethernet (CPwE)

Converged Plantwide Ethernet (CPwE) reference architectures, a Rockwell Automation and Cisco® collaboration, use industry standards to model characterized network architectures for use in an industrial network security framework. This industrial network security framework establishes a foundation for network segmentation for both traffic management and policy enforcement. The industrial network security framework uses a defense-in-depth approach and is aligned to industrial security standards.

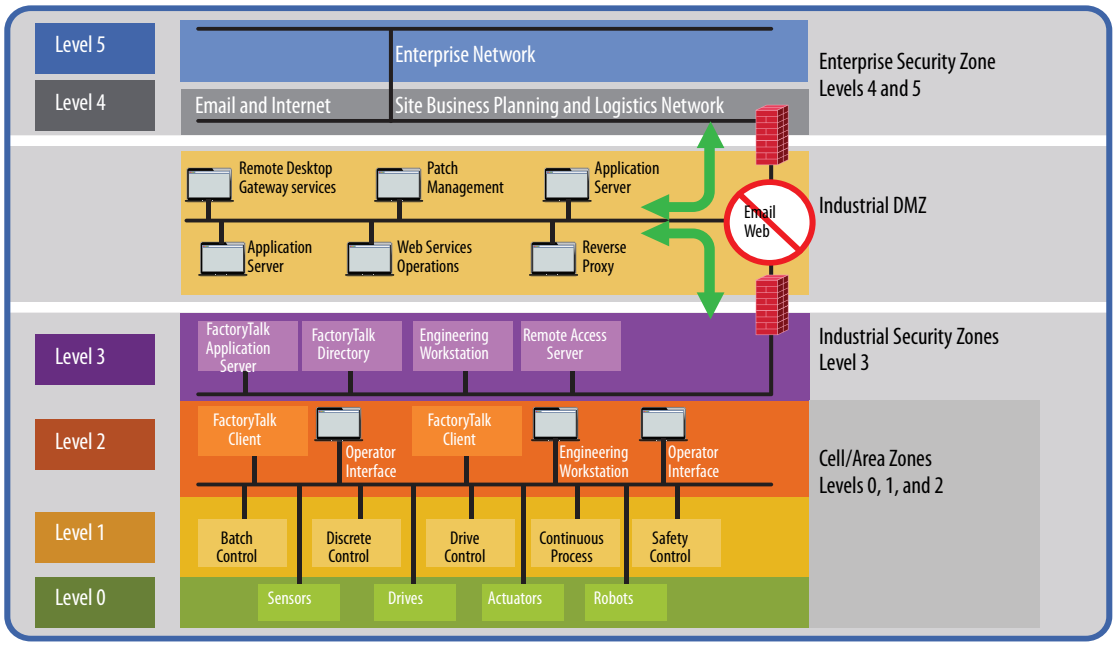
For more information, see Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, ENET-TD001



Logical Zones

CPwE logical zones employ common industry standards to organize the plant functions into levels, and the IEC-62443 (formerly ISA-99) standard to organize the levels into functional and security zones. The goal is to define smaller, more manageable areas, such as:

- connected LANs
- broadcast domains
- fault domains
- domains of trust



32796M

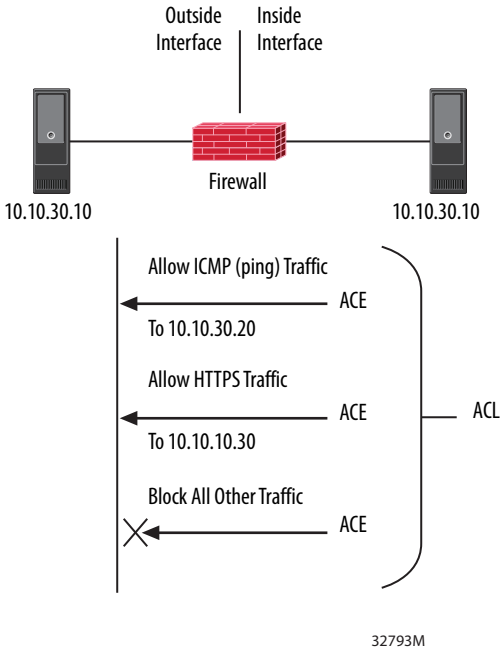
You can use physical or logical segmentation to define zones.

Infrastructure	Benefits
Segmented physical: simplex, unidirectional	A unidirectional network only lets data pass from one side of a network connection to another, and not the other direction. The controlled interface that comprises the send and receive elements of a unidirectional network acts as a one-way communication protocol break' between the two network domains.
Segmented physical: duplex, bidirectional	A bidirectional network lets data pass from both sides of a network connection. Connect, segment, encrypt, and cloak your critical assets and networks with crypto-IDs.
Segmented logical: duplex, bidirectional	CPwE industrial network security framework – IDMZ, VLANs, VRF, switch hierarchy (Layer 2 / 3)

Network Firewalls

A firewall is a software or hardware device that separates zones. A firewall permits or denies network traffic based on preconfigured policies or rules.

One type of preconfigured rule is an access control list (ACL). An ACL contains permit and deny statements. Each permit or deny statement is an access control entry (ACE).



This type of firewall control is stateful packet inspection (SPI) and operates by tracking legitimate connections. SPI rejects attempted connections from sources without a connection history. If you use a packet crafting tool in an attempt to gain access, the firewall rejects packets with sequence numbers that are out of range.

Firewall Guidelines

Firewalls are good security boundary appliances.

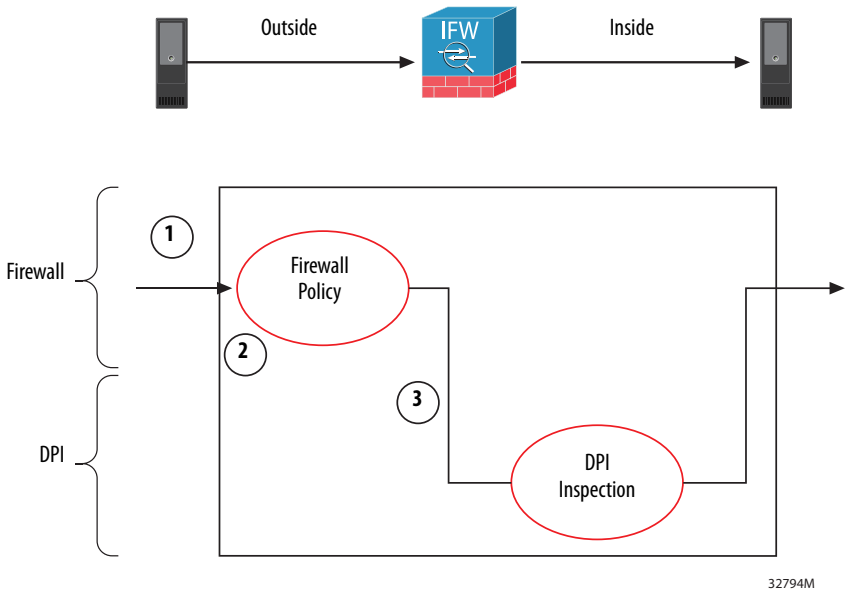
- Your firewall is only as good as your rules.
- If a rule permits traffic from a host on one side of the firewall to the other side of the firewall, a compromised host is hard to detect.
- Use Network Address Translation (NAT) to isolate private network addresses from public addresses.
- Inspect traffic for conformance with proper protocol behavior.
- Regularly monitor the firewall for rule updates, reports and metrics, and firmware and software patches.

Deep Packet Inspection

Another type of firewall control is deep packet inspection (DPI). DPI inspects application-layer traffic and examines packets traversing the firewall. This inspection examines IP address and port information, as well as the type of traffic and the data (if unencrypted), to enforce rules.

DPI examines the contents of a particular packet, and then either records that information for statistical purposes or performs an action on the packet. This information can then be forwarded to intrusion detection systems (IDS) and intrusion prevention systems (IPS).

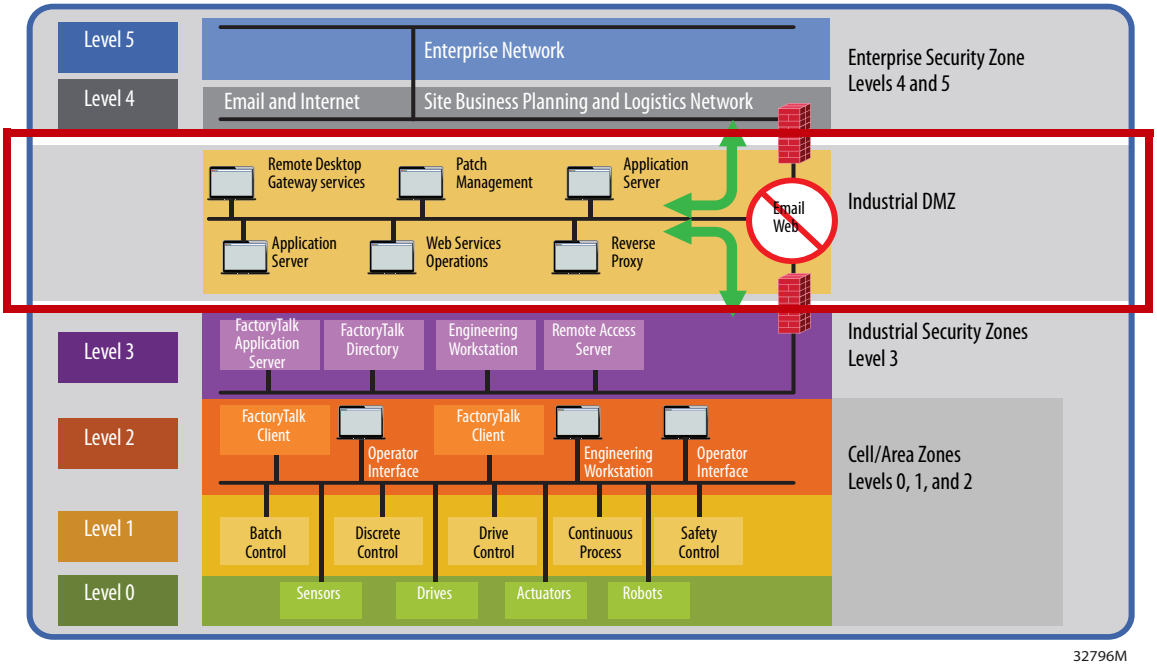
- Intrusion detection systems (IDS) inspect traffic on a network but do not affect traffic in any way; IDS only logs or alerts on malicious traffic.
- Intrusion prevention systems (IPS) inspect traffic on a network and can block malicious traffic.



1. Traffic enters the firewall.
2. Firewall policies are applied.
3. If a DPI rule applies, the packet is sent to an IDS or IPS rules engine for action.

Industrial Demilitarized Zone (IDMZ)

The industrial demilitarized zone (IDMZ) is a critical perimeter that acts as a buffer zone. The IDMZ provides a barrier between the Industrial and Enterprise Zones and lets the zones securely share data and services.



32796M

IDMZ Best Practices

Practice	Consideration
Services	Replicate critical services in the industrial zone, consider the following: • Domain Services, such as LDAP or Active Directory • Naming services, such as DNS and WINS • IP address services, such as DHCP • Time services, such as NTP and PTP
Availability	Apply redundant network routers, switches, firewalls, and links to maintain overall network availability
Scalability	At small sites, use combined core and distribution switches. Larger or growing sites separate core and distribution switches to avoid over-subscription on uplinks.
Routing	Use link-state routing protocols or EIGRP for Layer 3 load balancing and convergence Use EIGRP to simplify configuration If standard protocols are required, use OSPF

IDMZ Guidelines

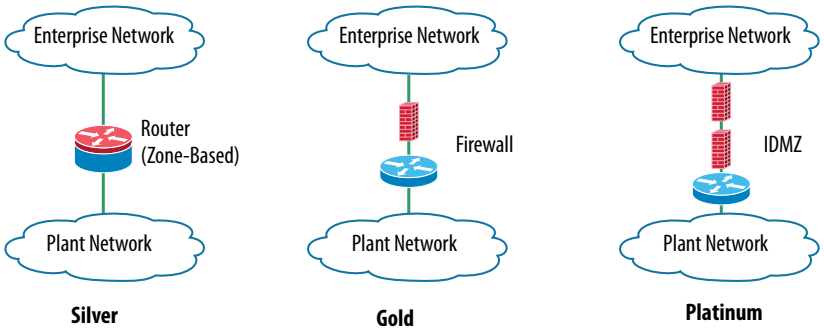
- All network traffic from either side of the IDMZ terminates in the IDMZ; no traffic directly traverses the IDMZ.
- The IDMZ is the only path between Industrial and Enterprise Zones.
- There are no common protocols in each logical firewall.
- EtherNet/IP control traffic does not traverse the IDMZ; it remains in the Industrial Zone.
- The IDMZ does not store primary services.
- All data is transient; the IDMZ does not store data.

- Use an application data mirror to move data in and out of the IDMZ.
- Limit outbound connections from the IDMZ.
- Be able to turn off access to the Industrial Zone via the firewall
- Set up functional subzones within the IDMZ to segment access to data and services (IT, OT, trusted partner)
- The IDMZ is also a demarcation line for segmenting network policies between the Enterprise and Industrial Zones.
- Segment network services such as Quality of Service (QoS), Virtual LANS (VLANs), and multicast traffic. These services exist in both the Enterprise and Industrial Zones and should be segmented.

Control Access to the Industrial Zone

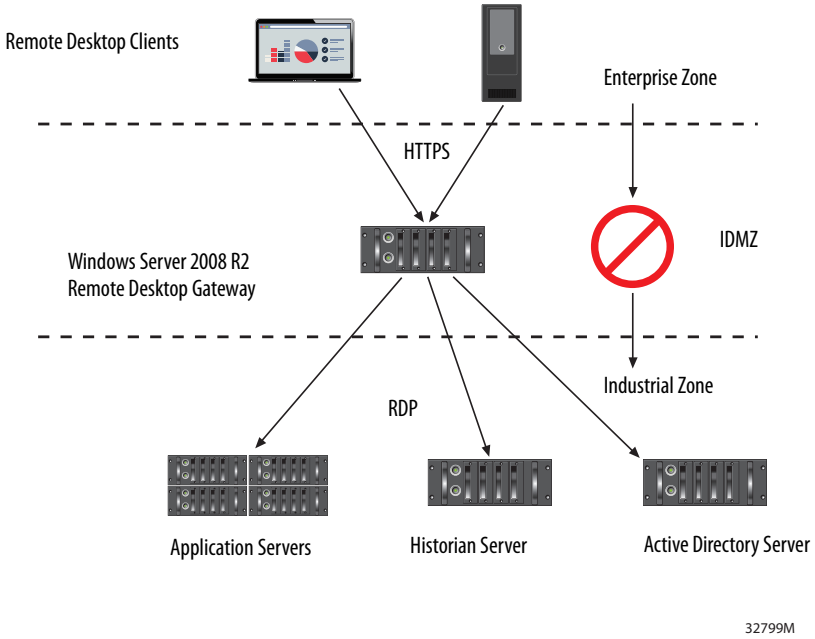
Set up functional subzones in the IDMZ to segment access to data and services. The IDMZ acts as the buffer between the Enterprise and Industrial Zones.

Most attacks attempt to pivot to other machines on the same network. Use the firewall, intrusion detection, and intrusion prevention to stop the 'pivot.'



Remote Desktop Gateway

The Remote Desktop Gateway is a server role in the Remote Desktop Services function of Windows Server 2012 and later. The gateway enables authorized remote users to connect to an internal corporate or private network.



Remote Desktop Gateway Guidelines

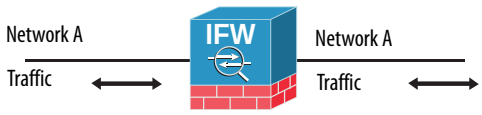
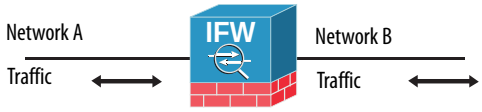
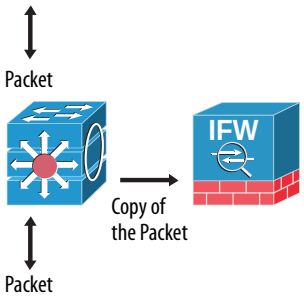
- Remote users connect to internal network resources by using an encrypted connection, without virtual private network (VPN) connections.
- The security configuration model lets you control access to specific internal network resources (point-to-point connection).
- Remote users can connect to resources that are behind firewalls in private networks and across network address translators (NATs).
- Configure authorization policies to define conditions for remote users to connect to network resources. For example, specify:
  - Who can connect to network resources (user group).
  - What network resources (computer group) users can connect to.
  - Whether client computers must be members of Active Directory security groups.
  - Whether device redirection is allowed.
  - Whether clients need smart card authentication, password authentication, or either.
- Configure clients to use Network Access Protection (NAP).

  NAP is a health policy technology that lets administrators enforce requirements, such as security updates, computer configurations, and other settings.

Industrial Firewall Zones

Stratix 5950 Security Appliance

The Stratix® 5950 security appliance provides firewall, threat defense, and VPN services. The appliance operates as an industrial DPI firewall with IDS and IPS capabilities. The security appliance provides firewall, threat defense, and VPN services. The Stratix 5950 security appliance can operate in the following modes:

Architecture Mode	Description
Inline Transparent	Default mode Use to segment a machine, skid, or unit from the Cell/Area Zone network. This mode supports different security requirements between the larger control network and the machine/skid or to restrict ingress and egress traffic. **Default** 
Inline Routed	Use as a Layer 3 ingress and egress router hop between a production line and a machine/skid. Monitor or control traffic firewall or DPI security policies. 
Passive Monitor	To avoid the possibility of the firewall affecting traffic, configure a traffic-forwarding interface and connect that interface to a SPAN port on a switch. 

Stratix 5950 Guidelines

- Use CIP™ (Common Industrial Protocol) Access Control Policy rules to block specific CIP traffic
- Block CIP actions like CIP Reads, CIP Writes, CIP Administration Firmware Update, and CIP Administration Download instead of permit actions.
- CIP DPI rules include host addresses but are not granular enough to a block specific users or tags.

For more information, see the Stratix 5950 Security Appliance User Manual, publication 1783-UM010.

Control Device Communication Ports

Customers using firewalls may want to configure communication ports on devices so that routers forward only Transmission Control Protocol (UDP and TCP) ports.

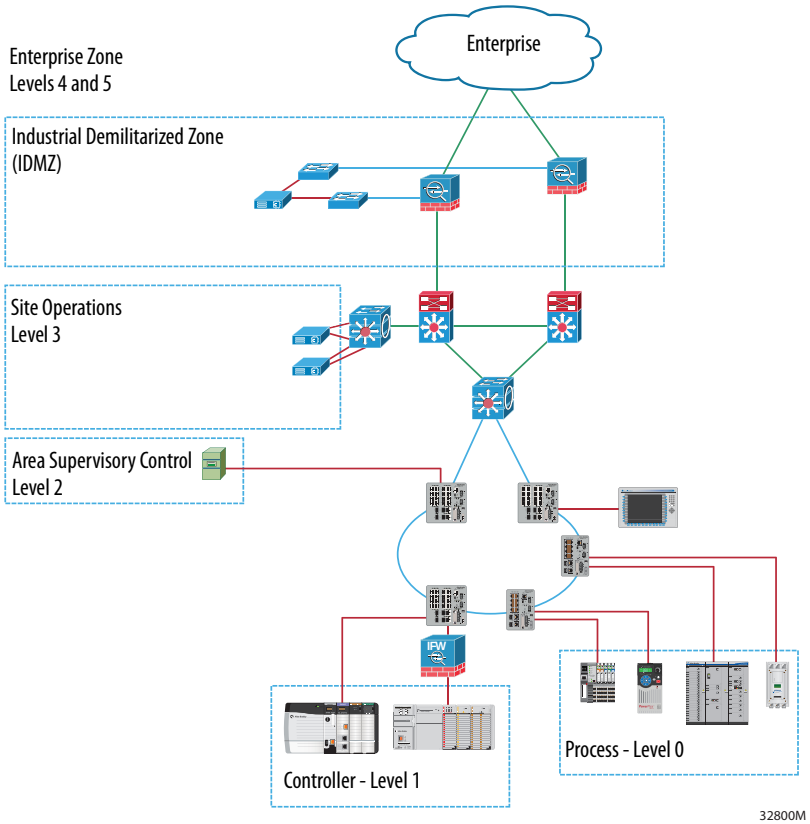
For more information, see Knowledgebase Technote *TCP/UDP Ports Used by rockwell Automation Products*.

Switch and Routing Platforms

Stratix Managed Switches

Configure Stratix managed switches to restrict access and segment your network architecture.

Restriction	Guidelines
Physical	Restrict access to the control panel or zone enclosure to authorized personnel only. Use Panduit block-outs for open access ports and lock-ins for copper and fiber media.
Electronic	Configure layer 2 media access control address (MAC) security on access ports. Configure layer 3 access control lists (ACLs). Define virtual local area networks (VLANs) to segment the cell/area zone into smaller domains of trust. Disable access ports from the controller and operator interface. Configure traffic threshold settings to monitor denial-of-service (DOS) attacks. Enable a cryptographic version of the switch operating system (SSH, HTTPS, SNMPv3). Manage access to maintenance ports via authentication to the local HMI.



For more information, see the following publications.

Resource	Description
Stratix Managed Switches User Manual, publication 1783-UM007	Covers: • Stratix 5400 switches • Stratix 5410 switches • Stratix 5700 switches • ArmorStratix™ 5700 switches • Stratix 8000 and 8300 switches
Stratix 6000 Managed Switches User Manual, publication 1783-UM001	Covers Stratix 6000 switches.
Stratix 2500 Lightly Managed Switches User Manual, publication 1783-UM009	Covers Stratix 2500 switches.

Secure Communications

Secure communications between devices to support data integrity, data confidentiality, and device authenticity.

CIP Security

CIP Security™ is a standard, communication method that helps to provide a secure data transport across an EtherNet/IP network. The secure data transport is used between certain connected devices to help protect the devices from threats posed by unauthorized users with malicious intent.

Rockwell Automation uses the following products to implement CIP Security:

- FactoryTalk® Policy Manager
- FactoryTalk Linx
- Studio 5000® Design Environment
- CIP Security-enabled Allen-Bradley products

For more information on CIP Security, see the CIP Security Application Technique, publication SECURE-AT001.

This additional layer of security reinforces the depth-in-defense approach. The CIP Security technology does not replace firewalls or other network infrastructures.

Wireless Connectivity

In a wireless architecture, always use Wi-Fi Protected Access II (WPA2) security with Advanced Encryption Standard (AES) encryption.

Option	Description
WPA2-PSK (pre-shared key) authentication	• One password for all clients, no user-based authentication • PSK is part of device configuration • Does not provide fast roaming times • Does not satisfy corporate security policy
WPA2 Enterprise (802.1x) authentication	• WPA2-Enterprise with EAP-TLS is the most secure method • Uses individual user credentials and (optional) security certificates Requires additional infrastructure and support • Active Directory • RADIUS server • Certificate infrastructure

Wireless Guidelines

Category	Guidelines
Wireless node limitations	• The number of wireless clients affects the performance • Do not exceed 20 wireless nodes per access point • Do not exceed 19 wired clients per workgroup bridge • Keep the total number of Ethernet devices on a VLAN (wired or wireless) below 200 to restrict the amount of broadcast traffic
Latency and jitter	• Make sure a channel load is below the limit and the proper wireless QoS policy is applied • A small percentage of packets is delayed significantly so the application should handle delayed packets • Low RPIs (faster than 5 ms) are not useful for wireless applications • Overloading a channel leads to excessive latency and timeouts • A larger number of wireless nodes increases latency
Packet loss and reliability	• If a wireless frame is not received, it is retransmitted until the retry limit is reached • An application must tolerate occasional packet loss • An excessive packet rate causes high packet loss and application timeouts • A large number of wireless nodes increases the chance of timeouts • Changes in the RF environment, interference, or unauthorized channel transmissions can decrease reliability or disrupt wireless communication
Unicast versus multicast	• Multicast and broadcast traffic is much less reliable than unicast traffic • Multicast wireless frames are not acknowledged and not repeated if lost • Use only unicast EtherNet/IP connections with I/O or produced/consumed tags • Do not use a ControlLogix® redundancy system with wireless communication • Configure IGMP snooping and querier in the network infrastructure

Additional Resources

The following publications provide details related to secure network connections.

Resource	Description
Design and Implementation	
Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD002	Use cases for designing, deploying, and managing industrial firewalls throughout an IACS network infrastructure.
Site-to-Site VPN to a Converged Plantwide Ethernet Architecture Design an Implementation Guide, publication ENET-TD012	Use cases for connecting remote IACS assets to a plant-wide network architecture. This guide highlights the key application requirements, technology, and supporting design considerations.
Deploying Identity Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD008	The requirements and design considerations to deploy the Cisco Identity Services Engine (Cisco ISE) within an IACS architecture.
Securely Traversing IACS Data across the Industrial Demilitarized Zone Design and Implementation Guide, publication ENET-TD009	The requirements and design considerations to deploy an industrial demilitarized zone (IDMZ) within an IACS architecture.
Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture, publication ENET-TD006	Wireless LAN network capabilities, with emphasis on equipment connectivity.
Application	
Industrial Firewalls within a Converged Plantwide Ethernet Architecture White Paper, publication ENET-WP011	Guidelines for designing, deploying, and managing industrial firewalls throughout an IACS.
Deploying Identity Services within a Converged Plantwide Ethernet Architecture White Paper, publication ENET-WP037	Guidelines for designing, deploying, and managing identity services throughout an IACS.
Securely Traversing IACS Data Across the Industrial Demilitarized Zone White Paper, publication ENET-WP038	Guidelines for designing, deploying, and managing industrialized demilitarized zones throughout an IACS.
Design Considerations for Securing Industrial Automation and Networks White Paper, ENET-WP031	Guidelines for designing, deploying, and managing secure networks throughout an IACS.

Harden the Control System

For guidelines on system hardening, see Knowledgebase Technote *Rockwell Automation Customer Hardening Guidelines*.

Patch Management

Keep security updates (patches) for both operating system and IACS software up-to-date. Patches can be critical to mitigate risk.

Verify any update to Rockwell Automation products or third-party products before implementation. Verify that configuration settings are still correct.

Microsoft Patches

Microsoft® releases a range of security updates for operating systems and other software products. Rockwell Automation qualifies certain Microsoft updates that impact Rockwell Automation software products.

It is recommended that you implement a controlled system suitable for your application and environment. Follow the guidance for Microsoft Patch Qualifications at:
http://www.rakb-patchtests.com/data/MS_Patch_Qualification/start.htm

Before implementing any Fully Qualified Microsoft updates, verify them on a non-production system, or when the facility is non-active, to ensure that there are no unexpected results or side effects.

Microsoft regularly releases security updates. If your system is not connected to the Internet, you will not automatically receive these updates.

Rockwell Automaton has a MS Patch Qualification team (PQUAL) to qualify Microsoft security updates against the most popular set of products available from Rockwell Automation. Results are posted on the Patch Qualification Portal. For more information, see the Knowledgebase Technote *Microsoft Patch Qualifications*.

Product Change Management

Keep your Rockwell Automation systems current to help you achieve improved security in your systems. Rockwell Automation uses product and version status policies to help you plan how to keep your system current.

Rockwell Automation assigns the status of a product based on the product catalog number.

Status	Definition
Active	Most current offering within a product category.
Active Mature	Product is fully supported, but a newer product or family exists. Gain value by migrating.
End of Life	Discontinued date announced - actively execute migrations and last time buys. Product generally orderable until the discontinued date.
Discontinued	New product no longer manufactured or procured. Repair/exchange services may be available.

To check the lifecycle status of a product, see the Product Lifecycle Status website.

Rockwell Automation further classifies product changes to catalog numbers (versions and revisions) to help customers manage their system.

Change Type	Description
Series Change	A series change indicates that there was a backward compatible hardware modification or non-field upgradeable firmware modification to a product. A series for product with firmware increments the major firmware revision number.
Direct Replacement	A direct replacement is any new product that emulates an earlier product. Form, fit, and function are backward compatible. No user application changes are needed.
Functional Replacement	A functional replacement is any new product with minor form, fit, and function differences. It is not a direct replacement and it does not emulate the earlier product. Minor application changes are required.
Engineered Replacement	An engineered replacement is any new product with major form, fit, and function differences. Major application changes are required.

Hardware Series

An alphabetical designator at the end of the product catalog number indicates the series of the product. The series indicator increments when there is a hardware change related to form, fit, or function.

- If a product has firmware, a series changes also requires a firmware revision. However, a firmware revision does not necessitate a series change.
- A series change can also require a new device profile. The new device profile is backward compatible to older series of the product.
- An older series product cannot replace a newer series product.

Software and Firmware Versions

To further understand the state of your system and help you keep the system current, Rockwell Automation assigns a lifecycle state to each individual version of a product.

Version State	Description
Preferred	Versions to adopt to stay current. • Major release versions of Active and Active Mature products remain in the Preferred state for 3 years following release • The latest version of an Active or Active Mature product is always preferred When a new minor or sub-minor version is released, the new minor or sub-minor release inherits the major version lifecycle state and the previous minor or sub-minor version transitions to be a Limited or Retired version.
Managed	Versions to adopt when you cannot use Preferred, typically for following reasons: • Maintain compatibility between non-discontinued hardware and software • Customer IT/OT lifecycle planning requires extended security coverage through Rockwell Automation patch updates. Major release versions of select Active and Active Mature products remain in the Managed state for 2 years following the Preferred state period.
Limited	Versions that are available for download, but that are not the recommended versions to use. In general, these versions remain available to support customers who have chosen not to stay current.
Retired	Versions that are no longer available for download because of security or safety concerns, or lack of support viability.

For more information see the Knowledgebase Technote *What is the Rockwell Automation Software and Firmware version lifecycle policy?*.

To check the lifecycle state of a product version, see the product's entry in the Product Compatibility and Download Center website.

Rockwell Automation designs, develops, maintains, and supports Preferred and Managed versions in accordance with the ISA/IEC 62443-4-1 certified secure, product development lifecycle.

For Preferred and Managed versions, Rockwell Automation:

- Notifies you of security-related issues in our products, and maintains a way for you to report back if you encounter security-related issues with our products.
- Notifies you if security patches for other products used in conjunction with our products (such as operating systems or anti virus programs) interfere with the correct operation of our products.
- Makes sure that qualified engineers and cybersecurity experts assess security-related issues for risk to our products and customers.
- Issues security updates accordingly and updates documentation with the latest information for how to secure our products.
- Makes software and firmware updates available through our support website and other support channels.

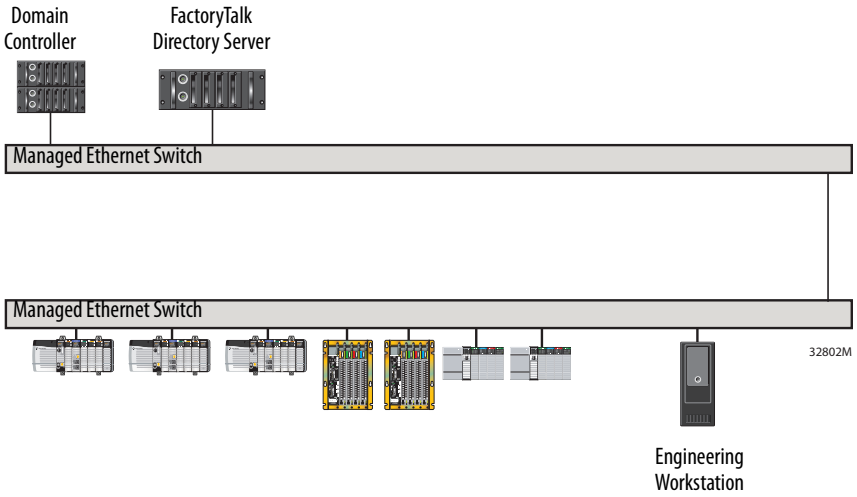
Workstation Hardening

Many IACS solutions use computers and servers to run applications. Consider these workstations and their operating systems in the overall security plan.

- Use Microsoft Active Directory for authentication and authorization.
- Secure Group security policies.
- Join all workstations to the domain.
- Dedicate workstations to operator and engineering functions, and remove all other unnecessary applications, services, and ports.
- Install endpoint protection, such as anti virus and anti-malware software, and keep the definition files up-to-date.
- Minimize users with access to administrative rights.
- Secure USB, CD, and DVD drives so they are available only for authorized purposes.
- Regularly restart workstations to prevent against memory-only infections.
- Implement a validated backup and restore process for important data and systems.

FactoryTalk Directory Application

The FactoryTalk® Directory application is a common service that is used by FactoryTalk View Site Edition and other Rockwell Automation software products. The FactoryTalk Directory server hosts a common address lookup of shared resources among FactoryTalk-enabled products.



Network FactoryTalk Directory Guidelines

- Host the role of the Network server on a dedicated computer. Do not co-locate a FactoryTalk Directory server or any other FactoryTalk software on a domain controller.
- The FactoryTalk Directory server can host other system components:
  - FactoryTalk Activation software
  - FactoryTalk Alarms and Events software
  - Centralized FactoryTalk® Diagnostics server in the absence of FactoryTalk AssetCentre software
  - FactoryTalk Historian software
- Use a server operating system that is optimized to service network requests. Do not use a domain controller.
- Install the FactoryTalk Directory server on a Microsoft Windows Server operating system (as opposed to a workstation or desktop operating system).
- Use caching instead of redundancy.
- FactoryTalk Directory servers do not communicate with each other.

Physical Access

To secure physical access to the system, consider these options:

- Subscribe to the Rockwell Automation Security Advisory Index to access information about security matters that affect Rockwell Automation products.
- Limit physical access to authorized personnel: control room, cells/areas, control panels, and devices.
- Provide training and communication to personnel to raise awareness of threats.
- Implement physical barriers, such as locked cabinets.

Device Hardening

Individual devices have their own capabilities that can be enabled or disabled. A common best practice is to disable the capabilities that your application does not use. See individual product documentation for guidance.

Digitally Signed Firmware and Software

Digitally signed firmware and software helps to make sure that users download and use authentic Rockwell Automation content.

Only download firmware and software from the Rockwell Automation official download portal at:

https://compatibility.rockwellautomation.com/Pages/home.aspx

Do not download firmware or software from non-Rockwell Automation sites.

To verify whether a file is a signed image, you can use the Microsoft SignTool utility. This utility is a command-line tool that digitally signs files, verifies signatures in files, or time stamps files. The tool is installed in the \Bin folder of the Microsoft Windows Software Development Kit (SDK) installation path.

Additionally, when you update the firmware in a device, use the ControlFLASH™ or ControlFLASH Plus™ utility.

For more information on how to configure and use ControlFLASH software, see the ControlFLASH online help and ControlFLASH Firmware Upgrade Kit User Manual, publication 1756-UM105 or ControlFLASH Plus Quick Start Guide, publication CFP-QS001.

High Integrity Add-On Instructions

Generate a signature on an Add-On Instruction to determine whether the Add-On Instruction is ever modified. The signature is required when an Add-On Instruction is used in SIL 3 safety-related functions, and can be required for regulated industries. Use the signature when your application calls for a higher level of integrity.

Once generated, the instruction signature seals the Add-On Instruction, including rung comments, tag descriptions, and any instruction documentation.

When an instruction is sealed, you can perform only these actions without affecting the signature:

- Copy the instruction signature
- Create or copy a signature history entry
- Create instances of the Add-On Instruction
- Download the instruction
- Remove the instruction signature
- Print reports

Edits to a sealed Add-On Instruction invalidate the signature. These changes include:

- Add, delete, or move parameters, local tags, or members in referenced User-defined Data Types.
- Change the name, data type, or display style of parameters, local tags, or members in referenced User-defined Data Types.

For more information how to secure Add-On Instructions, see Logix 5000 Controllers Add-On Instructions Programming Manual, publication 1756-PM010.

Additional Resources

The following publications provide details that are related to hardening the IACS.

Resource	Description
Add-On Instructions Programming Manual, publication 1756-PM001	Generate a signature to identify Add-On Instructions.
Computer System Security Updates White Paper, publication SECUR-WP002	Best practices for a patch management process.
Knowledgebase Technote *Rockwell Automation Customer Hardening Guidelines*	Best practices to harden computers and servers.
Knowledgebase Technote *Industrial Security Advisory Index*	Current security matters that affect Rockwell Automation products.

Notes:

Manage User Access

Comprehensive security depends on identification and 'AAA':

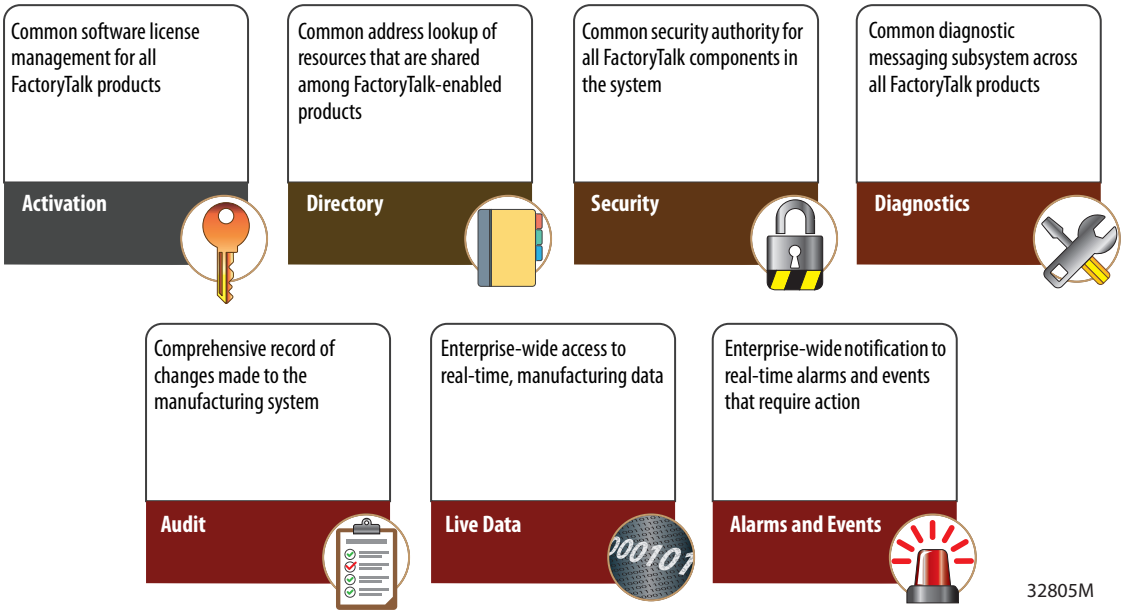
- Authentication (you are who you say you are)
- Authorization (you can do only what you have been authorized to do)
- Accounting (I keep track of what you do)

Give users only the privileges that they need (this is known as least privilege access). Passwords must meet current industry-standards and best practices for password strength. Grant a limited set of privileges to reduce the possibility of foreign software accessing privileges to perform a malicious act – a common technique that is used by malware.

Avoid local passwords (user name/password combinations that are stored locally on a device) to reduce the overhead required to manage the system. Instead you must manage users and passwords in a central system (FactoryTalk® Security or Microsoft® Active Directory applications). In the event an employee leaves or you make changes to user authorities, you can manage access from a central location rather than on each separate device.

FactoryTalk Services Platform

The FactoryTalk Services Platform software combines software components and services that are used by multiple products. These shared software services form a services-oriented architecture (SOA) that enable applications to share definitions, administration settings, and data.



FactoryTalk Services Guidelines

- FactoryTalk Services Platform CPR9 versions are compatible between all Service Releases (SRs). For example: CPR9 SR6 hosts can co-exist with CPR9 SR5 hosts.
- Where possible, maintain the same FactoryTalk Services Platform version and patch level across all hosts.
- Upgrade the FactoryTalk Directory server to the highest FactoryTalk Services Platform version currently installed.
- Do not co-locate a FactoryTalk Services Platform instance on a domain controller.

Control Data Access

Centralize security to better control data access.

FactoryTalk Administration Console Software

The FactoryTalk Administration Console software provides the interface to configure centralized application security.

Security Component	Description
Product and system policies	System-wide rules that govern how security is implemented
Computer accounts	Which computers can access your system
Networks and devices	Secure access to control hardware
User accounts	Who can access your system

For more information on how to create and manage permission sets, see the online help in the FactoryTalk Administration Console software or Logix 5000 Controllers Security Programming Manual, publication 1756-PM016.

Studio 5000 Logix Designer Application

Configure access to controller logic within the controller project.

Security Component	Description
Match the project to a controller	Match the project file to a controller serial number to minimize inadvertent downloads. You see a prompt if there is a mismatch between serial numbers during a download.
Secure tags	Restrict tag write access by user, group, or permission set.

The Studio 5000 Logix Designer® application has two tag attributes that control access to tag data. The External Access attribute controls how external applications can access tags. The Constant attribute value determines if controller logic can change a tag.

The External Access attribute sets read/write access to tags from external CIP™-capable devices, such as HMIs and other controllers. Grant the minimal read/write permissions needed for a tag and set External Access to None by default. Set the External Access attribute on the Edit Tags tab in Controller Tags editor.

The Constant tag attribute denies write access to both internal and external modification. An attempt to mark a tag as Constant that has External Access set to read/write results in an error.

For more information on how to configure these tag attributes to manage data access, see the online help in the Logix Designer application or Logix 5000 Controllers I/O and Tag Data Programming Manual, publication 1756-PM004.

FactoryTalk Security Software

FactoryTalk Security software acts as a centralized authority to manage user authentication and authorization. FactoryTalk Security software grants or denies user requests to perform actions on resources within the system.

Policies and Actions

Policies and actions can apply to all users and all computers or to specific users on specific computers.

Policy or Action	Description
System Policy	Policies that affect all software System policies affect the behavior of the software that is integrated with the FactoryTalk Directory application For example, password length, complexity, and expiration
Product Policy	Sets of securable features for the individual products in your FactoryTalk system Product policies affect specific products. For example, in the Logix Designer application, set a policy on who can create projects. This policy does not affect other software products
Securable Action	Allow or deny functionality to resources • Apply to all products that use that action • Apply to a resource or resources within a specific context, such a FactoryTalk Directory, application, or area) • Grant or deny permission to perform action by users and computers • Can inherit security settings from a parent context For example, Tag > Write Value controls whether a user or group can write to tags that are on a data server. This action applies to all software products that attempt to write to the tag on that data server.

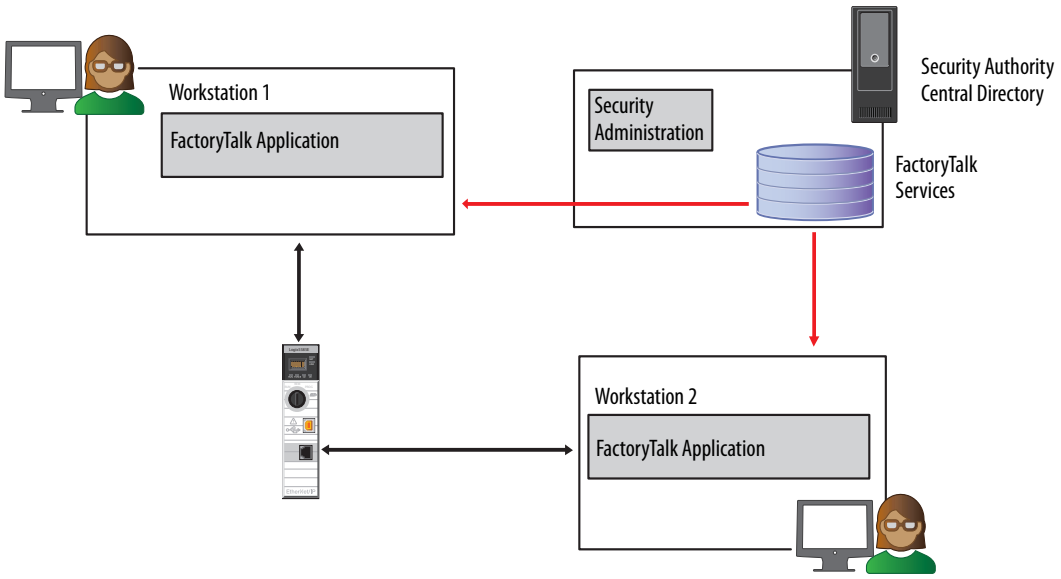
For more information on how to configure and manage access controls for users and groups, see the online help in the FactoryTalk Security software or Logix 5000 Controllers Security Programming Manual, publication 1756-PM016.

FactoryTalk Security Guidelines

- Secure a project file with a permission set to use the same policies for many controllers
- Apply permission sets to routines, Add-On Instructions, and tags to have different policies for different components

Centralized Security Authority

Every workstation shares a common authority. Each client workstation has a copy of the common authority.



32804M

Security Authority Identifier (SAID)

The security authority identifier (SAID) is a unique identifier for each FactoryTalk Directory instance. Use the SAID with FactoryTalk Security services to require that all users authenticate from a specific FactoryTalk Directory instance before they access the controller. The SAID is stored in the controller project (project binding) to secure the offline file.

This binding reduces the attack surface for security server spoofing because the client software and the security software determine the identity of the security authority responsible for controlling access.

For more information on how to configure and manage access controls for users and groups, see the online help in the FactoryTalk Directory software or Logix 5000 Controllers Security Programming Manual, publication 1756-PM016.

SAID Guidelines

- Both the ACD file and downloaded project are secured
  - Can only be opened by authorized users
  - Authorization can only be provided by a specific FactoryTalk Directory instance
- Maintain a backup of the SAID
  - If a FactoryTalk Directory instance is lost, you must be able to restore the SAID or you lose access to secured projects
  - A backup can be encrypted with a passphrase or password
  - A backup lets you duplicate and distribute multiple FactoryTalk Directory instances with the same SAID
- Requires a Network FactoryTalk Directory implementation

FactoryTalk View Site Edition

HMI applications support additional configuration options that secure user actions based on roles, such as maintenance or operator. The HMI displays can show different resources based on these roles.

FactoryTalk View SE applications use FactoryTalk Security services to authenticate and authorize application users. In a FactoryTalk View Studio project, create user and group accounts. Then determine which accounts have access to which resources, such as the local directory or the application.

FactoryTalk Security services use FactoryTalk View SE settings to provide two services:

- User authentication verifies a user identity, and whether a request for service that is actually originated with that user.
- User authorization verifies a user request to access a software resource, based on the access rights and privileges defined for that user.

Perform the following tasks to secure access to system resources:

- Remove ALL USERS from the FactoryTalk Local or Network Directory list.
- Create FactoryTalk accounts for the users, groups, and computers you want to secure.
- Assign security permissions to FactoryTalk user and group accounts.
- Configure system-wide security and product policies.

Protect Controller Logic

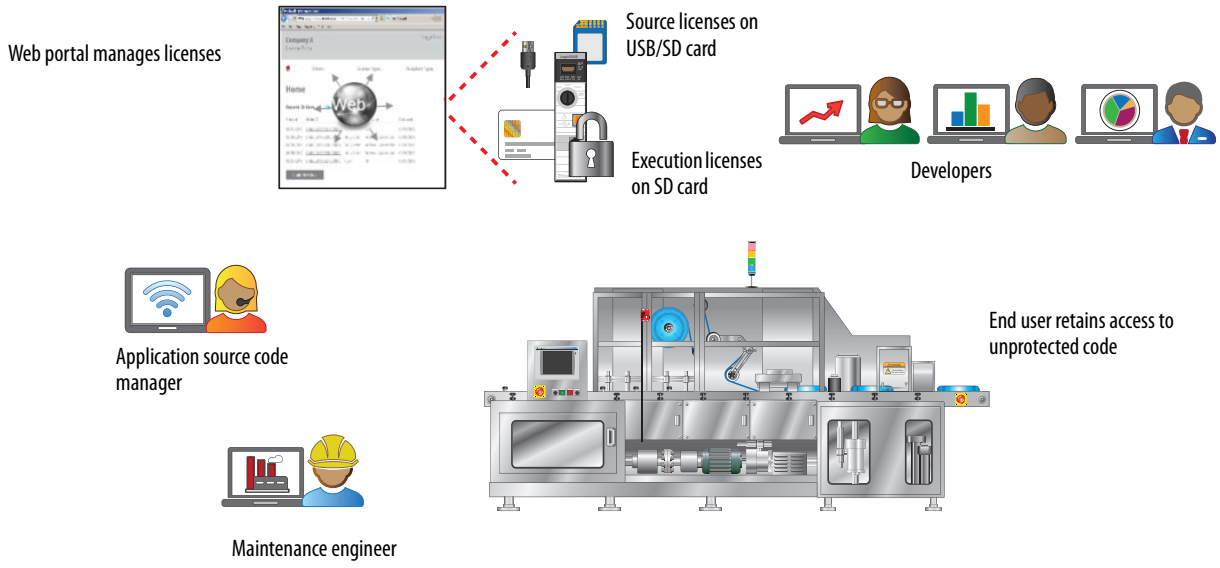
The following solutions can be used individually or together to protect intellectual property in controller applications.

Scenario	Solution	Requirements
I want flexible, manageable policies for who can access my controller content • Many users with different permissions	FactoryTalk Security software	• Central server, similar to Microsoft Windows domain functionality • Restrict users not part of FactoryTalk Security.
I want the most secure protection possible for my intellectual property. Concern over external and internal theft of IP. • Customers with highly sensitive IP • Heavily regulated industries where theft or modification of controller content is a concern	License-based source and execution protection	• Activated secure device • Subscription to License Portal

For more information on license-based protection, see Logix 5000 Controllers Security Programming Manual, publication 1756-PM016.

License-based Source and Execution Protection

You can implement license-based protection on a routine or Add-On Instruction.



Additional Resources

The following publications provide details that are related to manage user access.

Resource	Description
FactoryTalk Security System Configuration Guide, publication FTSEC-QS001	Guidelines on how to integrate, configure, and optimize FactoryTalk Security settings.
FactoryTalk View Site Edition User Manual, publication VIEWSE-UM006	How to develop and implement HMI applications that involve multiple users and servers, which are distributed over a network.
Logix 5000 Controllers Security Programming Manual, publication 1756-PM016	How to configure security options for Logix Designer projects.

Notes:

Monitor and Recover

Monitor the system for suspicious activity.

- Examine logs from workstations, firewalls, switches, and devices for evidence of foreign activity.
- Inspect network traffic and controller memory use for anomalies.

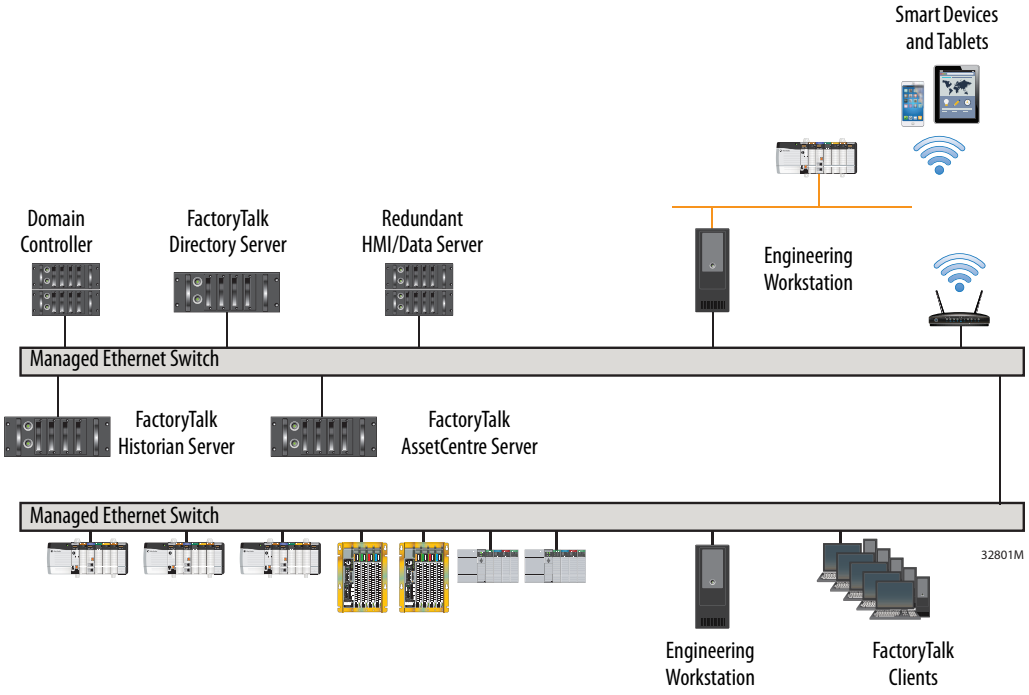
Management, audit, measurement, and detection technologies, such as the following, monitor the IACS:

- Log audit utilities
- Virus and malicious code detection systems
- Intrusion detection systems (IDS)
- Vulnerability scanners
- Forensics and analysis tools (FAT)
- Host configuration management tools (HCM)
- Automated software management tools (ASM)
- Syslog aggregate tools

Audit and Change Management with FactoryTalk AssetCentre Software

The FactoryTalk® AssetCentre server centrally tracks and manages configuration changes and restricts who can make changes. This server functionality assists with diagnostics and troubleshooting and reduces maintenance time for production assets.

Feature	Description
Audit	The audit feature gathers information about user interactions with FactoryTalk-enabled applications. Audits are captured while connected or even disconnected from the network. The audit trail includes Logged Time, Occurred Time, Source, Location, Resource, Username, and Message.
Security	FactoryTalk AssetCentre software internally leverages the security that is provided by the FactoryTalk Services platform. This security model minimizes efforts to administer users and passwords on workstations. Security rights are even enforced while computers hosting FactoryTalk applications are disconnected from the network.
Tamper Detection	FactoryTalk AssetCentre software continuously monitors controllers for changes. The software detects changes, logs activities, and creates a report. For example, the software logs and reports if a contractor walks up to a panel, connects a laptop to a controller, goes online, and modifies logic.



Route individual product events to the FactoryTalk AssetCentre system log. Individual products with rolling audit logs can overwrite event data before you have a chance to react. Configure the log in FactoryTalk AssetCentre software to make sure that the log is large enough to record all events. Also, monitor the log to make sure the log does not overflow.

A typical FactoryTalk AssetCentre system has the following components (roles).

Role	Quantity
Network FactoryTalk Directory server	1
Microsoft® SQL server	1
FactoryTalk AssetCentre server	1
FactoryTalk AssetCentre agent (required for all configurations)	1+ Maximum 10 agent groups Single agent services ~100 assets/12 hrs
FactoryTalk AssetCentre client One of the following required for audit functionality: • Studio 5000 Logix Designer • FactoryTalk View Studio • FactoryTalk View SE client	1+ Maximum 50 concurrent
ProCalV5 server (for calibration management)	0 or 1
ProCalV5 client (for calibration management)	0 or 1+ Maximum 50 concurrent

FactoryTalk AssetCentre Guidelines

- Link a FactoryTalk AssetCentre server with only one FactoryTalk Network Directory server.
- Each FactoryTalk AssetCentre system can use one Microsoft SQL (MSSQL) application, which can be co-located with the server component.
- There is only one agent per host. The agent component can be co-located with the server component.
- Do not use agent hosts as engineering workstations due to resource use.
- Audits and events are not collected automatically. You must install a client on the host to send the diagnostic information to the server.

Backups via FactoryTalk AssetCentre Software

System-level backup is done via FactoryTalk AssetCentre software. You can:

- Centrally manage versions of programs, files, and folders.
- Automate the backup of automation assets.
- Generate detailed difference-detection reports of assets.

ControlLogix® Disaster Recovery supports the automated backup and comparison of program files running in ControlLogix controllers. Once a ControlLogix device is configured as an asset in the FactoryTalk AssetCentre asset tree, it can be added to a Disaster Recovery schedule. The results of the Disaster Recovery schedule are added to the FactoryTalk AssetCentre Event Log, and can also be configured to be emailed.

Component Change Detection and Logging for Controllers

The Logix Designer application, revision 30 and later, supports component change detection. This detection determines whether changes are made to a program offline.

- The tracking group setting tracks changes on tags, I/O modules, and routines within a program
- In the event that changes are made to components within a tracked group, the group signature changes:
  - The tracked state value can be accessed from the Security tab in Controller Properties
  - The list of items tracked is on the View Components page

Disposal Guidelines

Devices contain various types of memory that store device and network settings, information from embedded solutions, and user data. The types of memory—along with the types of data in each—are described as follows.

- Volatile memory—Some devices use random access memory (RAM) to buffer user data temporarily.
- Nonvolatile memory—Some devices use EEPROM or NAND nonvolatile memory to store the operating system, device settings, and network information.
- SD card memory—Some devices support the use of an SD card to store user data.

To dispose of this data:

- If there is a battery, remove the battery and wait for residual power to dissipate.
- Reset the device to the default, factory settings.

See the user documentation for your device for instructions.

In high-security environments, you might need additional steps to verify that confidential data on the controller cannot be accessed once the controller is removed from your premises. Consider one or more of the following actions before disposing of a controller:

- Degaussing—Flushes the device with a magnetic field that erases stored data
- Crush—Physically compresses the device to break component parts and render them unreadable
- Mill—Physically shreds the device into small metal bits

To guarantee that all data is completely erased, physically destroy each memory device on which data was stored.

Notes:

History of Changes

This appendix contains the new or updated information for each revision of this publication. These lists include substantive updates only and are not intended to reflect all changes. Translated versions are not always available for each revision.

SECURE-RM001D-EN-P, March 2020

This revision updated the section on Product Change Management to add more information about product series indicators

SECURE-RM001C-EN-P, December 2019

This revision added a section on Product Change Management.

SECURE-RM001B-EN-P, April 2019

This revision:

- Added a section on Control Device Communication Ports
- Added a section on CIP Security for secure communication
- Updated Workstation Hardening
- Added FactoryTalk Administration Console and Studio 5000 Logix Designer features to Control Data Access.
- Renamed Monitor the Control System to Monitor and Recover
- Added a section on Backups via FactoryTalk AssetCentre Software

Notes:

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Knowledgebase	Access Knowledgebase articles.	rok.auto/knowledgebase
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	rok.auto/pcdc

Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at rok.auto/docfeedback.

Rockwell Automation maintains current product environmental information on its website at rok.auto/pec.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenkÖy, İstanbul, Tel: +90 (216) 5698400 EEE YÖnetmeliğine Uygundur

Connect with us.

rockwellautomation.com — expanding **human possibility**™

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication SECURE-RM001E-EN-P - March 2021
Supersedes Publication SECURE-RM001D-EN-P - March 2020
Supersedes Publication SECUR-LM003A-EN-P - September 2016