Industrial Security Solutions

Building More Secure Environments – From Enterprise to End Devices

You have assets to protect. Control systems, networks and software can all help defend against security threats and risks. It's time to manage potential threats and build a more secure industrial control system that meets your needs.

LISTEN. THINK. SOLVE.®

Allen-Bradley • Rockwell Software

Rockwell Automation

Industrial Security Solutions

As industrial organizations move towards greater visibility within their operations, the need to establish a seamless flow of information by connecting control systems to the enterprise has become a requirement of modern industrial networks. Effectively developing a fully connected enterprise requires a comprehensive approach to industrial security that extends beyond the control system to include policies and procedures that address people, process and technology-related risks. A complex, interconnected system doesn't come without challenges. It's critical to understand the potential risks and start building security into your industrial automation control systems.

Remote Access
Do you need to communicate with a control system over a non-production network (e.g. public or business networks)?

Unauthorized Access
Have you ever lost production because someone made a change they weren't permitted to make (e.g. downloading a program to the wrong controller)?

Intellectual Property Protection
Are you worried that your assets could be duplicated by your competitors?

Outside Hacker
Have you experienced performance issues or suspicious network traffic and suspect malicious activity, such as malware or a virus?

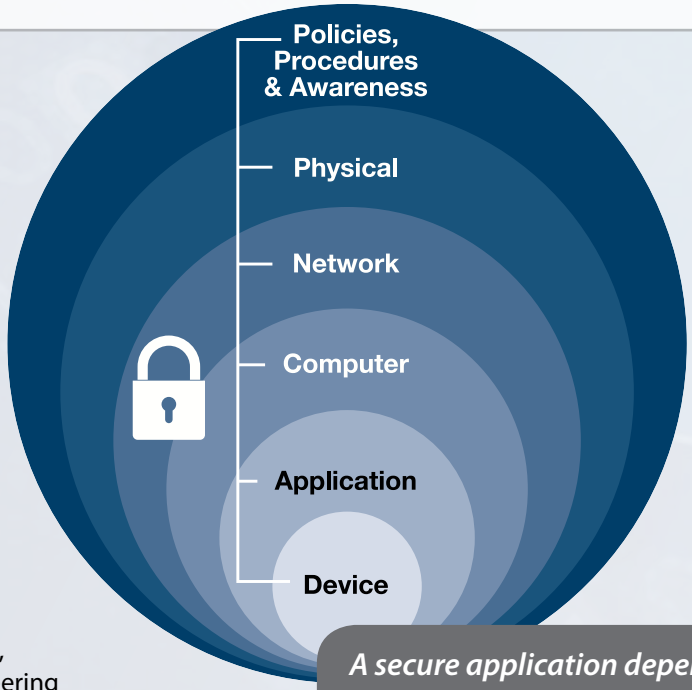
Unauthorized Changes
Have there ever been changes made to your system that went undetected for a long period of time?

Security Approach

With a systems-oriented approach to industrial security, Rockwell Automation can help you proactively assess and address risks in your control systems, and help you establish a common, secure environment for your industrial systems.

Rockwell Automation provides customers with products, solutions and services that enable a defense-in-depth approach using multiple layers of defense at separate industrial levels.

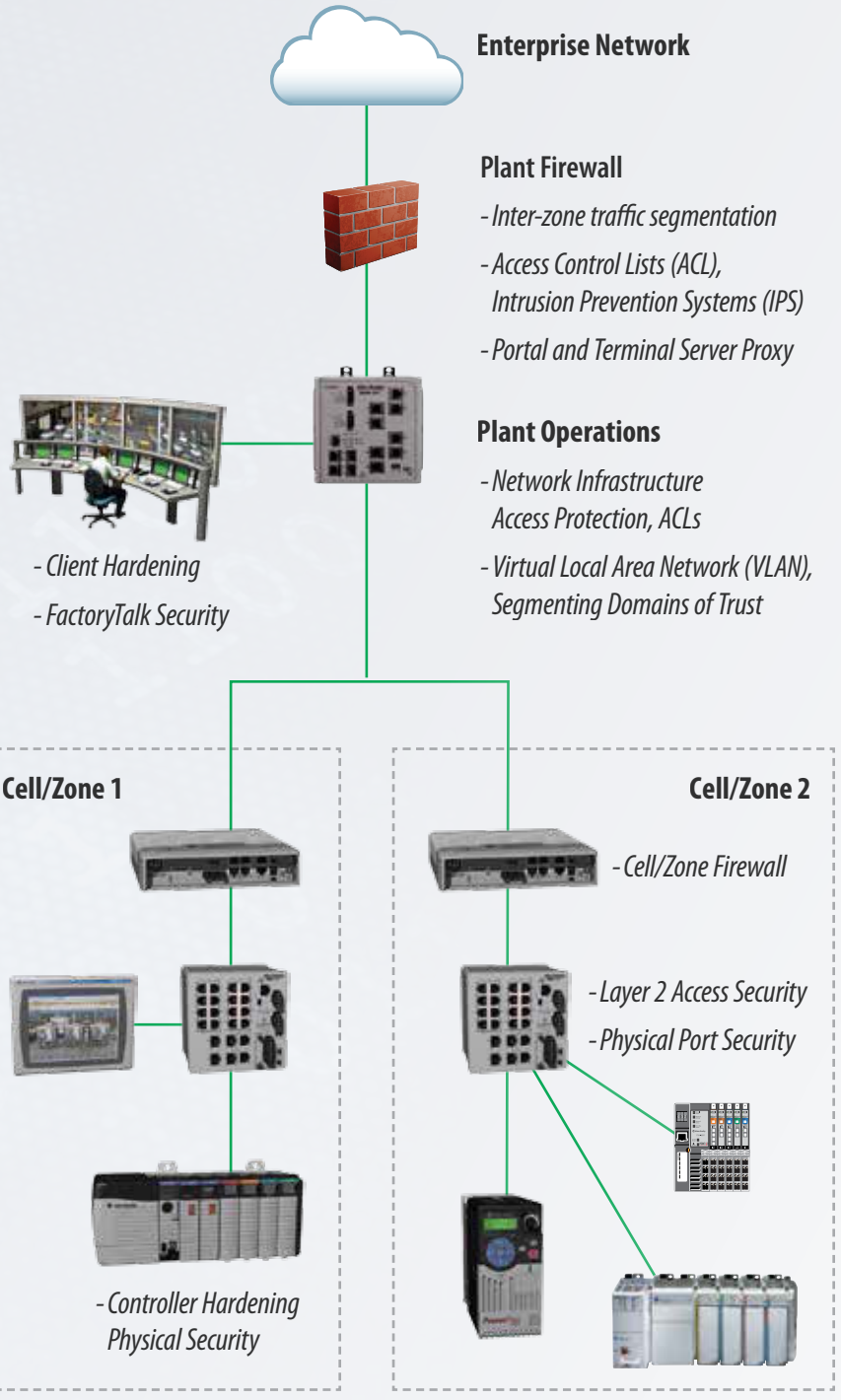
Within this approach, Rockwell Automation builds quality into their products with their design-for-security philosophy which includes, for example, training, architectural and engineering reviews, resiliency and robustness testing, and auditing.



A secure application depends on multiple layers of protection, including physical and logical controls and structured processes and procedures.

Offering and Capabilities

No single product, technology or methodology can fully secure a control system network. By partnering with companies such as Cisco, Microsoft and Panduit, Rockwell Automation solutions extend beyond products and technologies to also include guidance on company-wide security best practice designs, policies and procedures taking into account the unique requirements of each customer and industry.



An Automation Architecture Designed for Security

Securing the Network Infrastructure

Creating a control system network resistant to outside attacks.

- Reference Architectures
- Network and Security Services
- Stratix™ Portfolio of Routers and Switches

Intellectual Property Protection

Protect valuable control system content from unauthorized usage.

- Logix Source Protection

Tamper Prevention and Detection

Detect, document and provide notification for attacks on the control system.

- Firmware Digital Signatures
- Controller Change Detection and Logging

Identity Management and Access Control

Create a trusted system with advanced user control.

- Data Access Control
- FactoryTalk® Security

Our control systems and other intelligent end devices are developed using our design-for-security philosophy; building quality, resiliency and operational integrity into our products.

ControlLogix Programmable
Automation Controller

Designed with Security in Mind

CompactLogix Programmable
Automation Controller

Integrated Architecture®

The Rockwell Automation Integrated Architecture creates a unique opportunity for plant-wide optimization with scalable controllers, open and versatile networks, and a seamlessly integrated control system. It allows you to use a single network technology to accomplish many tasks, streamline multiple disciplines and applications into a single package, and enable secure and easy flow of production data across the enterprise.

Rockwell Automation programmable automation controllers (PACs), human-machine interfaces, drives, software and other intelligent connected devices are being developed using our design-for-security philosophy and include features to facilitate physical and logical access control and intellectual property preservation. In the automation environment, content is protected by secure communications and tamper prevention mechanisms which can help provide an additional layer of end-to-end security.

ControlLogix® Programmable Automation Controller

- Trusted Slot Designation
- Change Detection and Logging (Studio 5000® v20 and later)
- Firmware Digital Signatures

CompactLogix® Programmable Automation Controller

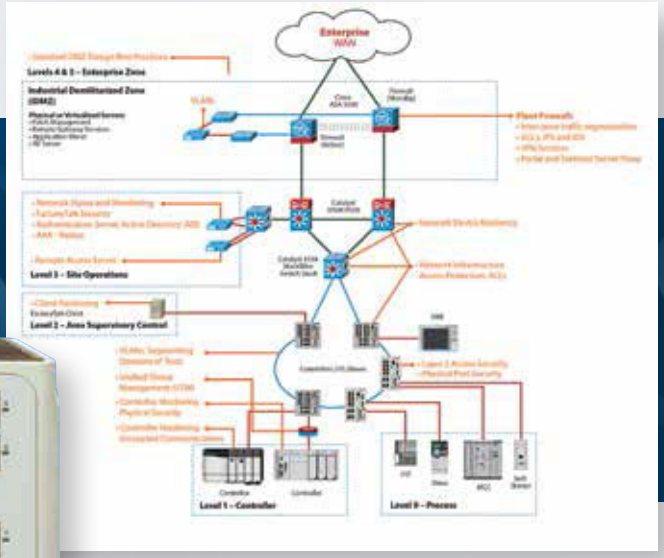
- Change Detection and Logging (Studio 5000 v20 and later)
- Firmware Digital Signatures

Design-for-security development practices are now being embedded within the product development process to help harden products against common attack.

Stratix 5900
Services Router

Stratix 5700 Layer 2 Managed Switch

Stratix 8000 Layer 2 and Layer 3
Modular Managed Switch



Reference Architectures

Network Infrastructure Solutions

In the last few years, we have been entering the era of the Internet of Things (IoT) – a world where billions of smart "things" and machines are connected to the internet.

All devices within a plant need to talk with one another, as well as those at the enterprise level, using a unified networking infrastructure that is Ethernet IP-centric. That's because only the Internet Protocol suite can ensure the scalability and coexistence of the Internet of Things.

Rockwell Automation offers infrastructure solutions designed to meet the unique needs of industrial automation. These solutions are optimized for use in the Rockwell Automation Integrated Architecture and can be used in other industrial applications that use standard Ethernet and TCP/IP to help enable plant and IT integration.

Stratix 5900™ Services Router

- Secure routing and firewall capabilities
- Virtual Private Network (VPN)
- Network Address Translation (NAT)
- Access Control Lists (ACL)
- Intrusion Prevention Systems (IPS)

Stratix Managed Switches

- Access Control Lists
- Device authentication with Learn Mode
- Programmable port control (on/off)
- Unauthorized device identification
- Encrypted administrative traffic

Reference Architectures

- Jointly developed with Cisco and optimized for both IT and industrial controls
- Provides design considerations, guidance and best practices to help you design and deploy secure and future-ready EtherNet/IP network infrastructures
- Security framework utilizing defense-in-depth approach
- Industrial DMZ implementation
- Guidance on remote access policies and approaches providing for a robust and secure solution

Information Software

The Internet of Things provides the potential to share data instantly with everyone and everything – creating a potential security threat.

Large amounts of industrial data are being delivered using contemporary technologies. It's imperative you protect that data and information. By integrating control and information, you can collect, manage and create actionable data securely to help drive productivity in your plant.

Information software manages information, including the collection, storage, analysis and/or visualization of data. The data can be used to better execute or understand the process.

FactoryTalk® VantagePoint EMI

This software connects to data sources, associates the data with other disparate sources across the enterprise and organizes it in a way to provide meaning to individuals ranging from engineering, maintenance, operations and executives.

- Creates a wide range of web-enabled dashboards and reports, enabling informed decision-making leading to improved productivity
- Tightly integrates with the Microsoft Active Directory and grants role-based access only to those individuals

FactoryTalk® Security

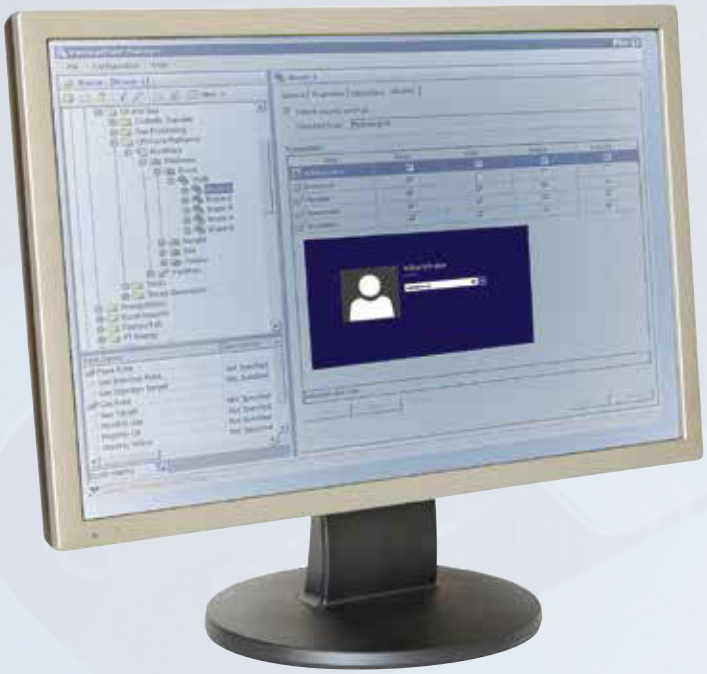
It's important to control who is permitted to do what from where. FactoryTalk Security provides centralized authentication and access control by verifying the identity of each user who attempts to access the automation system.

- Controls access to specific controllers with FactoryTalk Security with Security Authority Binding
- Provides user access controls and role-based security to Controllers, HMI and Software
- Communicates with FactoryTalk® Directory to determine what the user is and isn't permitted to do

FactoryTalk® AssetCentre

A set of asset-centric focused tools that help secure access to the control system.

- Tracks users' actions, manages asset-configuration files and provides backup and recovery of operating asset configurations
- Monitors the Audit Value and sends the data to the Controller Log



Studio 5000®

The Studio 5000 Automation Engineering and Design Environment combines engineering and design elements into one standard framework. The security features in the software can help protect your intellectual property and detect changes made to your system.

- Logix Controller Source Protection and Data Access Control
- Controller Change Detection and Logging
- High Integrity Add-on Instructions

Professional Services

Rockwell Automation field consulting services help customers assess, design, implement, validate and manage solutions that enhance industrial security. Our Network and Security Services (NSS) consultants offer a wide range of services to help customers achieve greater operational integrity and security within their control systems, regardless of the equipment employed. NSS capabilities include:

- Asset-based risk and vulnerability assessments
- Definition of security policies, procedures and guidelines
- Development of technical security controls
- Establishment of pragmatic Security Governance Programs
- Security Life-Cycle Management
- Industrial and IT expertise

Guidelines to Protect your Industrial Control System

Securing industrial assets requires a comprehensive security model based on a well-defined set of security policies. Policies should identify both security risks and potential mitigation techniques to address these risks.

The Rockwell Automation Network and Security Services can help you assess, design, implement and audit your security program and architectures against security standards.

- International Society of Automation, ISA/IEC-62443, is a set of standards specifically to help secure Industrial Automation and Control Systems (IACS).
- National Institute of Standards and Technology, NIST 800-82, provides a guide to establishing secure industrial control systems, which includes Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) and control system configurations.
- Department of Homeland Security Presidential Directive 21 – a national policy directive to strengthen and maintain secure, functioning and resilient critical infrastructure.
- Idaho National Lab, DHS INL/EXT-06-11478, is a U.S. Department of Energy National Laboratory that provides guidance on using a Defense-in-Depth approach.

Industrial IP Advantage –
The Resource Center for The Future of Industrial Connectivity

Industrial IP Advantage is a community of like-minded companies – Cisco, Panduit and Rockwell Automation in cooperation with ODVA – to help producers make the most of networking technologies that make integration and the flow of information effortless. The community provides education, technical resources and tools on the advantages of utilizing standard Internet Protocol (IP) in industrial applications. This can help you share and overcome challenges and seize opportunities offered by the Internet of Things. Join the online community at **www.industrial-ip.org** to receive the latest trends, developments, implementation advice and opinions on the use of IP in industrial applications.

Industrial IP ADVANTAGE
CONNECT INFORM TRANSFORM

Ten Actionable Steps

Enhance your industrial reliability and security with these ten actionable steps.

1. Control who has access to various areas of your network using features such as Access Control Lists and port blocking features.
2. Ensure robust and reliable operations by limiting and managing network traffic through the use of firewalls and intrusion detection/prevention systems.
3. Protect computer assets by using anti-virus and application whitelisting.
   Reference material: *Achieving Secure, Remote Access to Plant-Floor Applications and Data*, Publication # ENET-WP009.
4. Establish a system patching policy to keep software up to date.
   Reference material: *Computer System Security Updates*, Publication # SECUR-WP002.
5. Develop security policies to manage the "human factor", for example: managing and protecting passwords, managing removable media and use of personal devices.
6. Implement a level of physical control by putting the key-switch on your Logix Controller in Run Mode, and remove the key.
7. Control who is allowed to do what from where in the application with FactoryTalk Security.
8. Monitor what is going on in your system with Controller Change Detection and FactoryTalk AssetCentre.
9. Protect your intellectual property with Logix Source Protection.
10. Limit access to automation equipment by implementing physical controls such as locking cabinets and doors.

EtherNet/IP Plantwide Reference Architectures
Control system designs that complement recommended layered defense-in-depth measures.
http://www.ab.com/networks/architectures.html

Network and Security Services
Consulting specialists that conduct security risk assessments and make recommendations on how to mitigate risks.
http://www.rockwellautomation.com/services/security

For more information, visit: www.rockwellautomation.com/security

Rockwell Automation, Inc. (NYSE:ROK), the world's largest company dedicated to industrial automation, makes its customers more productive and the world more sustainable. Throughout the world, our flagship Allen-Bradley® and Rockwell Software® product brands are recognized for innovation and excellence.

Follow ROKAutomation on Twitter. Connect with us on Facebook and LinkedIn.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

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 SECUR-BR001A-EN-P – February 2014