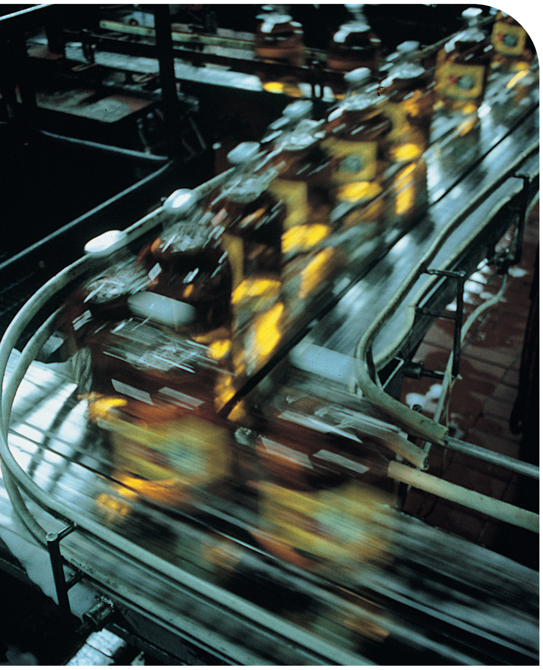


Securing Manufacturing Computing and Controller Assets

Synopsis

Industry adoption of EtherNet/IP™ for control and information solutions has led to the wide deployment of standard Ethernet within manufacturing. With this deployment as the enabler for the convergence of manufacturing and enterprise networks, manufacturers have benefited through increased access to production Key Performance Indicators (KPIs). Receiving KPIs at the right levels and at the right time helps manufacturers make better business decisions. Convergence also calls for evolved security policies for industrial networks, which no longer remain isolated within a manufacturing area. Manufacturing computing and controller assets have become susceptible to the same security vulnerabilities as their enterprise counterparts. A security policy needs to protect manufacturing assets, while balancing requirements such as 24x7 operations, low Mean-Time-To-Repair (MTTR) and high Overall Equipment Effectiveness (OEE).

Securing manufacturing 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. This whitepaper outlines general recommendations for deploying a holistic policy to help secure manufacturing assets. A listing of additional reference materials is available at the end of this whitepaper. Although the white paper references some of these materials with notation such as "see note," the list includes other resources not specifically identified within this whitepaper.

Holistic Security

Protecting manufacturing assets requires a "defense-in-depth" security approach, as depicted in Figure 1, that addresses internal and external security threats. This approach utilizes multiple layers of defense (physical and electronic) at separate manufacturing levels by applying policies and procedures that address different types of threats. For example, multiple layers of network security protect networked assets, data, and end points, and multiple layers of physical security to help protect high value assets. No single technology or methodology can fully secure industrial control systems.

Rockwell Automation and Cisco Four Key Initiatives:

- **Common Technology View:** A single system architecture, using open, industry standard networking technologies, such as Ethernet, is paramount for achieving the flexibility, visibility, and efficiency required in a competitive manufacturing environment.
- **Converged Plantwide Ethernet Architectures:** These manufacturing focused reference architectures, comprised of the Rockwell Automation Integrated Architecture™ and Cisco's Ethernet to the Factory, provide users with the foundation for success to deploy the latest technology by addressing topics relevant to both engineering and IT professionals.
- **Joint Product and Solution Collaboration:** Stratix 8000™ Industrial Ethernet switch incorporating the best of Cisco and the best of Rockwell Automation.
- **People and Process Optimization:** Education and services to facilitate Manufacturing and IT convergence and allow successful architecture deployment and efficient operations allowing critical resources to focus on increasing innovation and productivity.

In achieving a "defense-in-depth" approach, an operational process is required to establish and maintain the security capability. A security operational process includes:

1) Identify priorities (e.g. Availability, Integrity, Confidentiality)
2) Establish requirements (e.g. remote access must not impact control traffic, etc.)
3) Identify assets
4) Identify potential internal and external threats and risks
5) Understand capabilities required
6) Develop architecture
7) Develop and implement policies

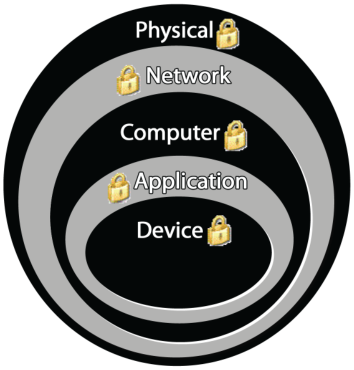
Designing and implementing a comprehensive manufacturing security model should serve as a natural extension to the manufacturing process. Users should not implement security as a bolt-on component to the manufacturing process.

For the purposes of this whitepaper, "defense-in-depth" layers for securing manufacturing assets include:

- Physical Security: This limits physical access of areas, control panels, devices, cabling, the control rooms and other locations to authorized personnel as well as escorts, and tracks visitors.
- Network Security: This includes the network infrastructure, such as firewalls with intrusion detection and intrusion prevention systems (IDS/IPS), and integrated protection of networking equipment such as switches and routers.
- Computer Hardening: This includes patch management and antivirus software as well as removal of unused applications, protocols and services.
- Application Security: This contains authentication, authorization and audit software.
- Device Hardening: This handles change management and restrictive access.
- For additional information on "defense-in-depth", see note 8.

Figure 1

Defense-in-Depth Multiple Layers



Manufacturing Framework for Network Security

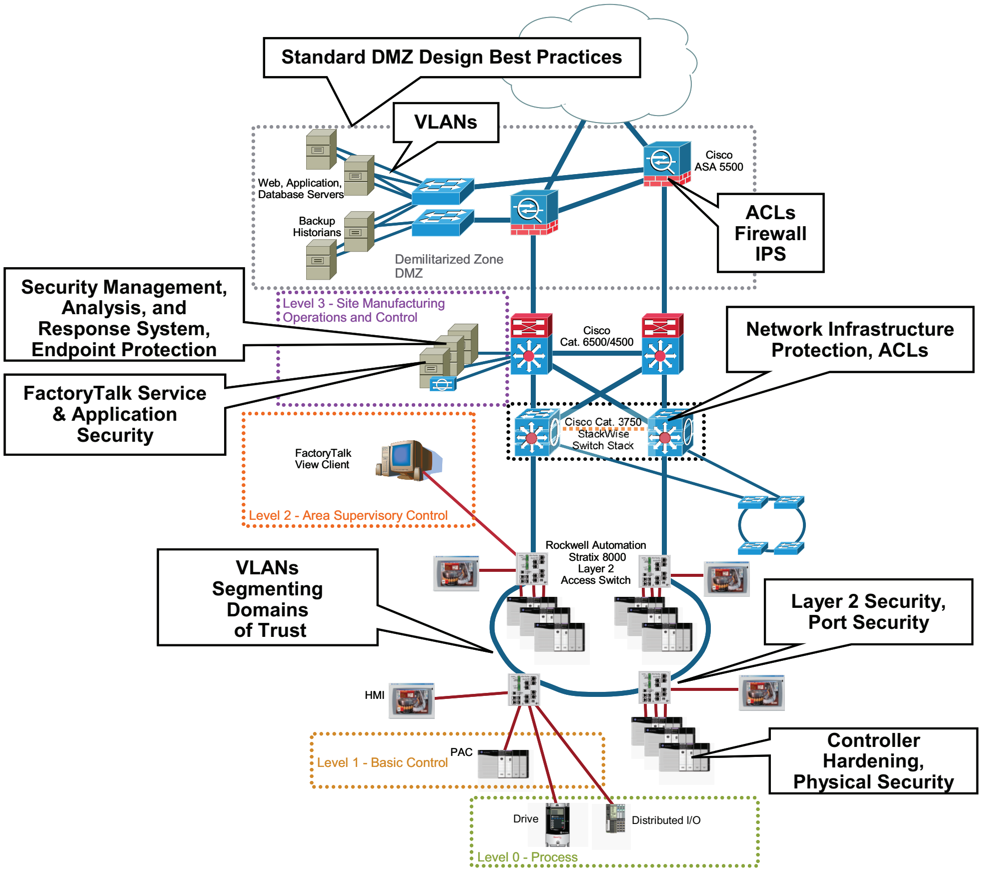
Rockwell Automation and Cisco collaborated to develop Converged Plantwide Ethernet Architectures (see notes 1, 2, and 3) to support and accelerate convergence of manufacturing and enterprise networks. To help users establish robust and secure network infrastructures, Converged Plantwide Ethernet Architectures provide design guidance, recommendations and best practices.

These manufacturing focused reference architectures are built on technology and manufacturing standards common between IT and manufacturing. These include technology standards such as the IEEE 802.3 standard, unmodified Ethernet, Internet Engineer Task Force (IETF) Internet Protocol (IP), and the ODVA Common Industrial Protocol (CIP^{TM}). For additional information about ODVA, see note 5.

Additionally, Converged Plantwide Ethernet Architectures use manufacturing standards to establish a Manufacturing Network Security Framework as shown in Figure 2. This framework establishes a foundation for network segmentation for traffic management and policy enforcement, such as security, remote access, and Quality of Service (QoS). The framework is aligned to industry standards and guidelines such as the ISA-95 Enterprise-Control System Integration, ISA-99 Manufacturing and Control Systems Security, and the Purdue Reference Model for Control Hierarchy.

Both ISA-95 and the Purdue Reference Model for Control Hierarchy segment industrial control devices into hierarchical "levels" of operations within a manufacturing facility. Using "levels" as common terminology breaks down and determines plant-wide information flow. For enhanced security and traffic management, ISA-99 segments levels into "zones." Zones establish domains of trust for security access and smaller LANs to shape and manage network traffic. For additional information about ISA, see note 6. The framework also utilizes the Campus Network Reference Model. Common with enterprise networks, this multitier model naturally segments traffic into three main tiers: core, distribution and access. This three-layer design provides a clear segmentation key to the network security approach and is the basis upon which a highly available and scalable network can be established.

Figure 2 Manufacturing Network Security Framework



Standard DMZ Design Best Practices
VLANs
Web, Application, Database Servers
Backup Historians
Demilitarized Zone DMZ
Cisco ASA 5500
ACLs Firewall IPS
Level 3 - Site Manufacturing Operations and Control
Security Management, Analysis, and Response System, Endpoint Protection
FactoryTalk Service & Application Security
Cisco Cat. 6500/4500
Network Infrastructure Protection, ACLs
Cisco Cat. 3750 StackWise Switch Stack
FactoryTalk View Client
Level 2 - Area Supervisory Control
Rockwell Automation Stratix 8000 Layer 2 Access Switch
VLANs Segmenting Domains of Trust
Layer 2 Security, Port Security
HMI
PAC
Level 1 - Basic Control
Controller Hardening, Physical Security
Drive
Distributed I/O
Level 0 - Process

The Manufacturing Framework groups level into the following zones for specific functions:

- Enterprise Zone: Levels 4 and 5 include traditional enterprise IT networks, business applications, such as email and enterprise resource planning (ERP), and wide area networks (WAN).
- Demilitarized Zone (DMZ) – This buffer zone provides a barrier between the Manufacturing and Enterprise Zones, but allows for data and services to be shared securely. All network traffic from either side of the DMZ terminates in the DMZ. No traffic traverses the DMZ. That is, no traffic directly travels between the Enterprise and Manufacturing Zones.
- Manufacturing Zone: Level 3 Site Manufacturing Operations and Control addresses plantwide applications such as historian, asset management and manufacturing execution systems (MES), and consists of multiple Cell/Area Zones.
- Cell/Area Zone: Levels 0, 1 and 2 include industrial control devices such as controllers, drives, I/O and HMI, and multi-disciplined control applications such as drive, batch, continuous process and discrete.

The recommended Manufacturing Network Security Framework utilizing “defense-in- depth” includes:

- Manufacturing Security Policy: This security policy roadmap identifies vulnerability mitigation. A multidiscipline team of operations, engineering, IT and safety should develop this manufacturing security policy.
- Demilitarized Zone (DMZ): This buffer zone provides a barrier between the Manufacturing and Enterprise Zones, while allowing users to securely share data and services. All network traffic from either side of the DMZ terminates in the DMZ. No traffic traverses the DMZ, which means that traffic does not directly travel between the enterprise and manufacturing zones.
- Defending the manufacturing edge: Users should deploy stateful packet inspection (SPI) firewalls (barriers) with intrusion detection/prevention systems (IDS/IPS) around and within the industrial network.
- Protecting the Interior: Users should implement access control lists (ACLs) and port security on network infrastructure devices such as switches and routers.
- Endpoint Hardening: This restricts access, prevents “walk up, plug in” access and uses change management to track access and changes.
- Domains of Trust: Users should segment the network into smaller areas based on function or access requirements.
- Physical Security: This restricts physical access to manufacturing assets and network infrastructure devices.
- Security, Management, Analysis and Response System: This monitors, identifies, isolates and counters network security threats.
- Remote Access Policy: For employee and partner remote access, implement policies, procedures and infrastructure. For additional information on remote access, see note 9.

Manufacturing Security Policies

The key to a successful security strategy is understanding the potential problems that need to be solved, such as what to protect and how. Establishing a security policy focused on manufacturing needs provides a roadmap for applying security technologies and best practices to protect manufacturing assets, while avoiding unnecessary expenses and excessive restrictive access. Security services should not inhibit nor compromise the manufacturing operation.

As defined by ISA-99, a security policy "enables an organization to follow a consistent program for maintaining an acceptable level of security." The security policy consists of both physical and electronic procedures that define and constrain behaviors by both personnel and components within the manufacturing system. A team consisting of IT, operations and engineering professionals should work together to define manufacturing security needs. Security policy development starts with evaluating potential risks. Conducted by either an internal or external team, the risk assessment process identifies potential vulnerabilities and determines mitigation techniques through procedures and/or technology. For example, a procedure could restrict physical manufacturing systems access to authorized personnel. Technology mitigation techniques could involve change management software to authorize and authenticate user credentials.

Since security policies traditionally remained in the IT domain, IT has developed best practices to help identify and mitigate security vulnerabilities. Users can apply many of these policies and best practices to manufacturing as long as they account for differences between the needs of manufacturing applications and enterprise applications.

Developing a robust and secure network infrastructure requires protecting the integrity, availability and confidentiality of control and information data. Users should address the following when developing a network:

- Is the network infrastructure resilient enough to provide data availability?
- How consistent is the data? Is it reliable?
- How is data used? Is it secure from manipulation?

IT responsibilities include protecting company assets and intellectual property (IP). IT accomplishes this by implementing an enterprise security policy enforcement to protect data Confidentiality, Integrity and Availability (CIA) – typically in that order of priority. Although similarities exist, the manufacturing security policy must place continuous manufacturing operation (Availability) as top priority. Manufacturing security policy enforcement protects data Availability, Integrity, then Confidentiality (AIC) – in that order. For additional information on CIA vs. AIC, refer to ISA-99 and see note 6. Enterprise and manufacturing security policies differ in terms of how they handle upgrades. Users conduct upgrades as soon as possible for enterprise applications, like operating systems and application software patching, as well as antivirus definition updates. However, applying upgrades to a running manufacturing server could disrupt operations, resulting in a production loss. Manufacturing security policies should define upgrades as a scheduled activity during manufacturing downtime.

Computer Hardening

IT best practices applied to enterprise computers should also apply to manufacturing computers. Some best practices and general recommendations include:

- Keep computers up-to-date on service packs and hot fixes, but disable automatic updates. Additionally, users should test patches before implementing them as well as schedule patching and regular network maintenance during manufacturing downtime.

- Deploy and maintain antivirus software, but disable automatic updates and automatic scanning. Other recommendations include testing definition updates before implementing them and scheduling manually initiated scanning during manufacturing downtime because antivirus scanning can disrupt real-time operations.
- Deploy and maintain antispyware software, but disable automatic updates and automatic scanning. Users should test definition updates before implementing them as well as schedule manually initiated scanning during manufacturing downtime since antispyware scanning can disrupt real-time operations. Automatic antivirus and antispyware scanning has caused data loss and downtime at some manufacturing facilities.
- Prohibit direct internet access. Implementing a Demilitarized Zone (DMZ) provides a barrier between the Manufacturing and Enterprise Zones, but allows users to securely share data and services. All network traffic from either side of the DMZ terminates in the DMZ. No traffic traverses the DMZ, meaning that traffic does not directly travel between the Enterprise and Manufacturing Zones.
- Implement a separate Active Directory domain/forest for the Manufacturing Zone. This helps ensure availability to manufacturing assets if connectivity to the Enterprise Zone is disrupted.
- Implement the following password policy settings:

  - Enforce password history

  - Maximum password age

  - Minimum password length

  - Complex password requirements
- Disable the guest account on clients and servers.
- Require that the built-in administrator account uses a complex password, has been renamed and has removed its default account description.
- Develop, and then deploy, backup and disaster recovery policies and procedures. Users should test backups on a regular schedule.
- Implement a change management system to archive network, controller and computer assets (e.g. clients, servers and applications).
- Use Control+Alt+Delete, along with a unique user name and password to log in.
- Protect unnecessary or infrequently used USB ports, parallel and serial interfaces to prevent unauthorized hardware additions (modems, printers, USB devices, etc.).
- Develop and implement a policy for guest access within the Enterprise Zone.
- Develop and implement a policy for partner access within the Manufacturing Zone.
- Uninstall the unused Windows® components, protocols and services not necessary to operate the manufacturing system.

Controller Hardening

Users can secure Rockwell Automation Logix™ Programmable Automation Controllers (PAC) by physical procedure, electronic design, authentication and authorization software as well as change management with disaster recovery software. Best practices and general recommendations include:

- Physical procedure: This restricts control panel access only to authorized personnel. Users can accomplish this by implementing access procedures or locking the panels. Switching the PAC key to "RUN" helps prevent remote programming, including remote firmware flash that could corrupt the PAC. To allow program configuration changes, this requires a physical key change at the PAC. Unauthorized access (intentional or unintentional) could not alter the PAC until the key switch is changed from "RUN."
- Electronic design: Implementing the PAC CPU Lock feature denies front port access to the PAC, which prevents configuration changes.
- Authentication, authorization and audit by implementing FactoryTalk® Security: Authentication verifies a user's identity and whether service requests originate with that user. Authorization verifies a user's request to access a feature or PAC against a set of defined access permissions. For additional information on FactoryTalk Security, see notes 7 and 8.
- Change Management with disaster recovery: FactoryTalk® AssetCentre software continuously monitors PAC assets with automatic version control, disaster recovery and backup, device configuration verification and real-time auditing of user actions.

Software Patch Management

Studies show that more production outages on manufacturing assets have occurred due to poor or missing patch management processes than by exploiting the vulnerability being patched. Users should establish a rigorous and well-documented patch management process.

Microsoft® implements service packs, security updates, hot fixes and patches as necessary to fix vulnerabilities in its operating systems. Users should disable the automatic updates from the Microsoft website for manufacturing assets as well as test all operating system updates and patches prior to implementation.

The automation software vendor, such as Rockwell Automation, should test and support updates and patches. Manufacturing and IT professionals should also extensively test updates and patches on their operating system templates before applying them to manufacturing assets. After testing, users should log all operating system patches and upgrades into an appropriate change management system. Only critical patches and upgrades should be applied to manufacturing assets during scheduled manufacturing downtime.

Rockwell Automation tests and validates its software products to run with specific operating system service packs with each scheduled software release.

Rockwell Automation only supports service packs that have been tested to run with a specific software release. Users should not apply service packs from Microsoft to manufacturing assets running Rockwell Automation software until Rockwell Automation validates the service packs for compatibility and stability.

As soon as Microsoft releases updates, Rockwell Automation qualifies the updates with its software products. The Rockwell Automation Knowledgebase lists operating system, service packs, patches and security updates for each software product release that Rockwell Automation supports and validates. To access this list, search for article "Microsoft (MS) Patch Qualification for 2007-08, ID 35530." For additional information, refer to note 10.

Rockwell Automation publishes updates for its software products as needed between scheduled product releases to address urgent issues with a released software version. Once a month, released patches are combined into a single roll-up. Patches can be applied individually or as part of the monthly roll-up. Users can find patches and rollups on Rockwell Automation Knowledgebase by searching for the article, "Rockwell Automation Software Product Compatibility Matrix, ID 42682." For additional information, refer to note 10.

Summary

The convergence of manufacturing and enterprise networks increases access to manufacturing data, which allows manufacturers to make better business decisions. This business agility provides a competitive edge for manufacturers that embrace convergence.

With these opportunities, come challenges. Network convergence exposes manufacturing assets to security threats traditionally found in the enterprise. Users also face an unclear demarcation line of network ownership and cultural differences between deploying enterprise and manufacturing assets. To address these obstacles, manufacturers should form a multidiscipline team of operations, engineering and IT professionals to jointly develop a manufacturing security policy based on:

- Manufacturing operation requirements.
- Enterprise security policy best practices.
- Risk assessment.
- A holistic security policy based on the "defense-in-depth" approach.
- Industry standards such as ISA-99 (see note 6).
- Manufacturers' corporate standards.
- Segmented Manufacturing Network Security Framework.
- A rigorous and well-documented patch management process.
- Utilization of external network and security services (see note 12).

Additional Reference Material

Notes:

1) Converged Plantwide Ethernet Architectures Website
http://www.ab.com/networks/architectures.html

2) Converged Plantwide Ethernet Architectures Whitepaper
http://www.ab.com/networks/architectures.html

3) Design and Implementation Guide (DIG)1.2
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf

4) Ethernet Design Considerations for Control System Networks – (ENET-SO001)
http://literature.rockwellautomation.com/idc/groups/literature/documents/so/enet-so001_-en-e.pdf

5) Network Infrastructure for EtherNet/IP: Introduction and Considerations
http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00035R0_Infrastructure_Guide.pdf

6) ISA99, Industrial Automation and Control System Security
http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

7) FactoryTalk Website
http://www.rockwellautomation.com/rockwellsoftware/factorytalk/

8) FactoryTalk Security Quick Start Guide
http://literature.rockwellautomation.com/idc/groups/literature/documents/qs/ftsec-qs001_-en-p.pdf

9) Secure, Remote Access to Plant Floor Applications and Data
http://www.ab.com/networks/architectures.html

10) Rockwell Automation Knowledgebase -
http://www.rockwellautomation.com/knowledgebase/

11) Microsoft Security -
http://www.microsoft.com/technet/security/current.aspx

12) Rockwell Automation Network and Security Services
http://www.rockwellautomation.com/services/security/

13) Securing Today's Global Networks in Industrial Environments
http://www.cisco.com/web/strategy/docs/manufacturing_self-defending_networks.pdf

Cisco is the worldwide leader in networking that transforms how people connect, communicate and collaborate. Information about Cisco can be found at www.cisco.com. For ongoing news, please go to http://newsroom.cisco.com. Cisco equipment in Europe is supplied by Cisco Systems International BV, a wholly owned subsidiary of Cisco Systems, Inc.

www.cisco.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Rockwell Automation is a leading provider of power, control and information solutions that enable customers to get products to market faster, reduce their total cost of ownership, better utilize plant assets, and minimize risks in their manufacturing environments.

www.rockwellautomation.com

Americas:
Rockwell Automation
1201 South Second Street
Milwaukee, WI 53204-2496 USA
Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Asia Pacific:
Rockwell Automation
Level 14, Core F, Cyberport 3
100 Cyberport Road, Hong Kong
Tel: (852) 2887 4788, Fax: (852) 2508 1846

Europe/Middle East/Africa:
Rockwell Automation
Vorstlaan/Boulevard du Souverain 36
1170 Brussels, Belgium
Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Publication ENET-WP005A-EN-E — May 2009