T22 - Industrial Control System Security
A secure application depends on multiple layers of protection and industrial security must be implemented as a system.

- **Defense in Depth**
  Shield targets behind multiple levels of security countermeasures to reduce risk

- **Openness**
  Consideration for participation of a variety of vendors in our security solutions

- **Flexibility**
  Able to accommodate a customer’s needs, including policies & procedures

- **Consistency**
  Solutions that align with Government directives and Standards Bodies
The Approach

**Strategic**
- Develop an OT cyber security program
- Adopt an industry framework
- Understand business drivers and risk tolerances to drive target profiles
- Conduct assessments to develop an understanding of gaps
- Create an improvement plan to drive the tactical approach

**Tactical**
- Execute on filling gaps as defined and prioritized in the strategic approach
- Use validated designs and architectures
- Implement pre-engineered infrastructure and software solutions to achieve targets
Securing your operations environments with a risk-based approach
Series of standards that define procedures for implementing electronically secure industrial automation and control systems (IACS).

Applies to those responsible for designing, manufacturing, implementing, or managing industrial control systems:

- End-users (for example; asset owner)
- System integrators
- Security practitioners
- ICS product/systems vendors
Recent Events

- Frequency of malware attacks are rapidly increasing
- Phishing attacks are the #1 delivery mechanism
- Increasing levels of adaption and scalability
Typical Access Points

- Remote access
- Modems
- Business system connectivity
- USB and portable media
- Mobile PCs and devices

People are the weakest link!
Our Plan of Attack

- Secure the infrastructure
- Harden the endpoints
- Detect and monitor
Secure Infrastructure

1. Establish the perimeter
2. Harden the interior
3. Prevent & contain
Secure Network Infrastructure
Validated Architectures

Help achieve infrastructure security through a common, validated system architecture leveraging the Stratix portfolio and Cisco security solutions.

Design and Implementation Guides:

- Converged Plantwide Ethernet (CPwE) Design and Implementation Guide
- Segmentation Methods within the Cell/Area Zone
- Securely Traversing IACS Data Across the Industrial Demilitarized Zone
- Deploying Identity Services within a Converged Plantwide Ethernet Architecture
- Site-to-site VPN to a Converged Plantwide Ethernet Architecture
- Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture

Download these and more at:

Leverage managed switches to build out robust networks that can manage ACL’s, VLANs, and QoS policies.

Implement industrial firewalls (Stratix® 5950) to isolate critical systems.
Connectivity Considerations

- Data Diodes for more secure one-way data transfer
- Enables data to move out of control system networks without allowing any data in, for:
  - View-only OPC
  - View-only screen sharing
  - Historian replication
  - Backups
- Allow tightly controlled movement of data into control system networks for needed files, patches and software updates
Connectivity Considerations

- Network segmentation using private overlay networks on top of untrusted infrastructure
  - Private networks can be mapped to users and/or devices
  - Requires no changes to existing infrastructure
  - Leverages HIPswitches and a centralized HIPConductor
Harden the Endpoints

1. User access control for endpoints and applications
2. Authorize appropriate software and devices
3. Establish a patching procedure
Hardened PCs and Servers

System Infrastructure Configuration User Manual:

- Infrastructure: domain controller, Active Directory, Windows management and
  - Windows group policies with recommendations (i.e. USB use policies, password complexity, time sync, etc.)
  - WSUS for OS patch management – coming soon!
- Application user authentication with FactoryTalk® Security
  - Prescribed role-based policies (maintenance, operator, admin, etc.)
  - Area-based security models

Download the manual at:

Application Whitelisting

- Symantec embedded security: critical system protection
  - Great for helping to protect PCs that can’t be frequently updated
  - Completely policy driven – no signatures
  - Features include:
    - Application whitelisting
    - Sandboxing
    - Host firewall
    - File protection
    - Monitoring, and more…
User Access Control and Authorization
FactoryTalk® Security

- Provides a **centralized authority** to verify identity of each user
  - Active Directory integration
  -Disconnected environment support
- Grants or deny user's requests to perform a particular set of actions on resources within the system

-Authenticate the user
-Authorize use of applications
-Authorize configuration access to controllers

**New in version 28:**
- Temporary Privilege Escalation
- Guest User Access
- Reusable Permission Sets (Routines, Add-On Instruction, and Tags)
- Secondary Security Authority
Asset Inventory & Patch Management
FactoryTalk® AssetCentre

REDUCE THE TIME IT TAKES TO GET lifecycle INFORMATION

Export the asset inventory to Product Compatibility and Download Center (PCDC)
Disaster Recovery
FactoryTalk® AssetCentre

WHEN A DIFFERENCE IS DETECTED
Disaster Recovery can optionally be configured to create a new archive version

1. Compares image or code to master file in archive
2. Detects differences & generates an event to FactoryTalk® AssetCentre
3. Email containing difference report sent to users
Detection and Monitoring

1. Alert on anomalous behavior
2. Identify known threats
3. Provide an audit trail to support analysis
4. Measure on-going compliance to policy
Network Security Appliances
Stratix® 5950 Security Appliance

Strategic collaboration between Cisco and Rockwell Automation®

- Based on recognized and proven technologies
  - Adaptive security appliance for firewall and VPN
  - SourceFire FirePower for inspection and detection
  - Enhanced with OT context of protocols, behaviors, and features

Key Features:
- Deep Packet Inspection for ICS protocols
- Threat & application update service
- DIN rail mount

- Connectivity Options:
  - (4) 1Gig Copper
  - (2) 1Gig Copper and (2) SFP
- Industrially-hardened
MANAGED ANOMALY DETECTION

Capabilities

Centrally Managed Services

- 24x7 Monitoring and Response by Trained IT/OT Professionals

Individually Managed Site Appliance

- Security and Operational Alerts and Events

Asset Monitoring

- Comprehensive asset inventorying
- Passive network monitoring
- Vendor and protocol agnostic
- Deep network analysis

OT Assets

- Behavioral anomaly detection
- Active change detection
- Alert on operational and security events
- Incident response services

IT Assets

- Validate operational tasks to reduce risk, and maintain process integrity
- Near real-time detection of cyber threats
- Recover from security Incidents with Highly-Trained Professionals
- Reduce risk of downtime with 24x7 response
Compliance and Reporting

- **Tripwire Configuration Compliance Manager (CCM)**
  - Audit industrial automation networks and controllers for more secure and approved configurations
  - Identify unauthorized changes, configuration hardening errors and security vulnerabilities
  - Layer on top of a standard implementation of FactoryTalk® AssetCentre for greater visibility into industrial automation applications
Industrial Security Landing Web Page

http://rockwellautomation.com/security
secure@ra.rockwell.com
Thank You!