T46 - Integrated Architecture® Tools for Securing Your Control System
The Connected Enterprise

Over 50% of internet connections in the PLANT are THINGS

2011: 15+ billion permanent, 50+ billion intermittent
2020: 30+ billion permanent, >200 billion intermittent

Source: Gartner, February 2013

- Remote sensing of objects and environment
- Cameras and microphones widely deployed
- Content and services via connected products
- Everything has a URL
- 7100 kWh of energy used today
- Subscribe to my news feed
- My yield will meet today's production needs
- Clean me next shift
Risks and Threats to Control Systems

- Application of Security patches
- Natural or Man-made disasters
- Worms and viruses
- Sabotage
- Unauthorized access
- Theft
- Unauthorized actions by employees
- Unintended employee actions
- Unauthorized remote access
- Denial of Service
- Application of Security patches
- Natural or Man-made disasters
- Worms and viruses
- Sabotage
- Unauthorized access
- Theft
- Unauthorized actions by employees
- Unintended employee actions
- Unauthorized remote access
- Denial of Service

Security risks increase potential for disruption to System uptime, improve safety operation, and a loss of IP
October 17, 2014

Sandworm vulnerability seen targeting SCADA-based systems

Hard on the heels of the `Sandworm' spy group revealed by iSIGHT Partners earlier in the week, Trend Micro says its has spotted the zero-day vulnerability of the same name being used to target SCADA-based systems.
Pharmaceuticals, Not Energy, May Have Been True Target Of Dragonfly, Energetic Bear

New research says the compromised companies were suppliers for OEMs that served pharma and biotech.

One of the biggest attack campaigns against critical infrastructure since Stuxnet might not actually have been aimed at critical infrastructure. New research on the Dragonfly, a.k.a. Energetic Bear, attacks that were first reported by F-Secure in June poses the theory that the group's true target was the pharmaceutical and biotechnology industry, not the energy sector.

In a report released today by the signal transmission solution company Belden, Joel Langill, an industrial control systems security expert at RedHat Cyber, explains why he thinks Dragonfly was attacking small companies that supply original equipment manufacturers, which in turn supply the pharma-biotech sector.
What is Industrial Security?

- Seeks to reduce risks associated with unintended or malicious actions
- Seeks to improve ability to be free from danger, injury or loss
- Seeks to help protect key assets from disruption, loss or damage
Innovative Approach to Industrial Security

1. Build in Security Quality

2. Create Security Value
Security Quality
Product Design Approach

- Design for security
  - Develop Specifications
  - Audit and Identify Gaps
  - Enhance & Improve

- ISA
- NIST
Security Quality
Product Resiliency & Robustness (R&R) Testing

- Key part of our Industrial Security Team
  - Help reduce customer risk
- Critical to our Industrial Security Goals
  - Identify weaknesses and vulnerabilities
  - Improve product resiliency & robustness
  - Evaluation of all company products
- Leveraging ISA Security Compliance Institute (ISCI) approved tools and test suites
  - Achilles test tool & “Level-2” test suite fulfills technical aspects of ISA99 and IEC-62443 standard for ICS cyber security
  - Evaluates resiliency of Ethernet protocol suite
  - Results provide concrete facts about product resiliency to simplistic attacks driving continuous improvement.
Security Quality
Incident Response Process

- Product Vulnerabilities:
  - We expect them.
  - We plan for them.
  - We work to avoid them.
  - We support our customers.

- See Rockwell Automation®
  *Knowledgebase article 54102*
  for up to date information on product vulnerabilities
Security Value
Core Tenets

Secure Network Infrastructure
Control access to the network, and detect unwanted access or activity

Tamper Detection
Detect and record unwanted activity & modifications to the application

Content Protection
Help protect viewing, editing, and use of specific pieces of control system content

Access Control & Policy Management
Control who, what, where & when access is allowed to which application or device
Security Value: Secure Network Infrastructure

Secure Network Infrastructure helps enable secure enterprise connectivity, remote manufacturing and remote engineering

- Rockwell Automation® solutions available today include:
  - Stratix™ Portfolio of Routers & Switches
  - Stratix 5900™ Services Router
  - Architectural Guidelines
  - Network and Security Services
## The Stratix™ Portfolio
Securing the Infrastructure

<table>
<thead>
<tr>
<th>Products that offer:</th>
<th>Technology that offers:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Layer 2 and Layer 3 switching for simple to complex networks applications</td>
<td>✓ Advanced switching, routing and security features</td>
</tr>
<tr>
<td>✓ Advanced security services</td>
<td>✓ Common tools for Controls &amp; IT</td>
</tr>
<tr>
<td>✓ Plant-floor and Enterprise integration</td>
<td>✓ Improved Maintainability</td>
</tr>
<tr>
<td>✓ “On-Machine™” Connectivity</td>
<td>✓ Flexible design</td>
</tr>
<tr>
<td>✓ Wireless integration in hard-to-wire and remote areas</td>
<td>✓ Customization based on your plant’s needs</td>
</tr>
</tbody>
</table>

### Addressing the needs of Automation...

- **Stratix 8000™/Stratix 8300™** Layer 2, Layer 3
- **Stratix 5900™ Services Router**
- **ArmorStratix™ 5700**
- **Stratix™ 5100 Wireless Access Point/Workgroup Bridge**
- **Stratix™ 5700** Layer 2
- **Stratix 2000™ Unmanaged**
- **Stratix 6000™ Layer 2**
- **Stratix™ ETAPs**

...as well as Operations and IT
The Stratix™ Engine

- Cisco IOS Software is the most widely leveraged network infrastructure software in the world
- Currently operating on millions of active systems, ranging from the small home office router to the core systems of the world's largest service provider networks

Cisco's leadership in switching, routing and security now in Rockwell Automation® industrial Ethernet products and solutions
The Stratix™ Value

**Designed & developed for Industrial EtherNet/IP applications**

**Optimize network performance**

- **QoS – Quality of Service** - default configurations are set to ODVA standards for EtherNet/IP industrial applications for discrete, motion, safety and process applications
- **IEEE1588 (CIP Sync)** - ODVA implementation of the IEEE 1588 precision time protocol helps ensure performance when connecting EtherNet/IP devices

**Simplify design, deployment and maintainability**

- **DHCP per port** - assign a specific IP address to each port, helping ensure that the device attached to a given port will get the same IP address
- **Broken Wire Detection** - detect cabling problems like, open, broken, cut or shorted twisted-pair wires, with status availability in Logix
- **Network Address Translation – NAT** – A 1:1 IP address translation to help segment machine level network devices from the plant network, translate only the devices that need to be visible to the plant network
The Stratix™ Value

- **Helping protect the assets**
  - Application/Project (CIP) based port access
    - Controller based port control (on/off)
    - Port access based on controller mode (idle/fault)
    - Unauthorized device identification (tags) per port
  - Configurable port security
    - Preconfigured port security set-up via Smartports
    - Configure number of devices allowed per port
    - Configurable device MAC ID authentication

- **Helping protect the plant**
  - Encrypted administrative traffic
    - VPN, SSHv2, SNMPv3, and HTTPS
  - Advanced security features
    - 802.1x for user authentication
    - Multiple layers of password protection
    - Access Control Lists (ACLs) to apply security policies per port
    - TACACS+ and Radius for centralized authentication

**Simplified tools to help protect assets.**
**Advanced feature set to help meet IT standards and policy**
Stratix 8000™ and Stratix 8300™
Layer 2 and Layer 3 Modular Managed

- Configurable up to 26 ports
  - Base unit - 6 or 10 port
  - Expansion Modules
    - Copper, Fiber, SFP & PoE extensions
- SFP for multi and single mode fiber
  - Wide variety of SFPs available
- Power over Ethernet (PoE) - New
  - PoE & PoE+ port configurable
- CompactFlash card
  - Stores configuration and IOS for easy device replacement
- Advanced feature set to address:
  - EtherNet/IP applications
  - Security
  - Resiliency & Redundancy
- Operating Temp: -40°C to 60°C

Ideal for connecting into a higher level of the network infrastructure architecture
Stratix 5700™ Family
Layer 2 Managed Fixed Port

- 3 base platforms offering 20 configurations
  - 6, 10 & 20 port base units
  - 2 Gig port option
- SFP slots support multi and single mode fiber
  - Wide variety of SFPs available
- SecureDigital flash card (optional)
  - Stores configuration and IOS of switch
- Two software packages
  - Lite & Full software versions
- Advanced feature set
  - Same feature set as the Stratix 8000™
  - Integrated NAT functionality
  - Simple static routing
- Power over Ethernet (PoE)
  - PoE & PoE+ port configurable

*Combo ports can be either copper or SFP

Ideal for connecting machines into the plant networks – Converged Networks
Stratix 5900
Layer 2 and Layer 3 Services Router

- Premiere routing and security services for Layer 2 or Layer 3
  - Router + Firewall
  - Virtual Private Network (VPN)
  - Network Address Translation (NAT)
  - Access Control Lists (ACL)
  - Intrusion Prevention Systems (IPS)

- Connections:
  - 1 Gigabit WAN
  - 4 Fast Ethernet

- Industrially hardened, DIN rail mountable
- Ideal for Site to Site Connections, Cell/Zone Area Firewall and OEM Integration

Ideal for helping protect communications through secure channels & restricting unwanted communications by policy and inspection
Stratix 5900™ Services Router
Network Security Framework

Enterprise-wide Business Systems

Plant-wide Site-wide Operation Systems

Stratix 5900™
1) Site-to-Site Connection

Stratix 5900™
2) Cell/Area Zone Firewall

Levels 4 & 5 – Data Center
Enterprise Zone

Level 3 - Site Operations
Industrial Zone

Level 3.5 - IDMZ

Levels 0-2
Cell/Area Zones

Remote Site #1

Local Cell/Area Zone #1

Local OEM Skid / Machine #1

Site-to-Site Connection

Physical or Virtualized Servers
- FactoryTalk® Application Servers & Services Platform
- Network Services – for example DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

Stratix 5900™
3) OEM Integration
Converged Plant-wide Ethernet (CPwE)

Reference Architectures

- Structured and Hardened IACS Network Infrastructure
- Industrial security policy
- Pervasive security, not a bolt-on component
- Security framework using defense-in-depth approach
- Industrial DMZ implementation
- Remote partner access policy, with robust & secure implementation

Network Security Services Must Not Compromise Operations of the IACS
Network & Security Services: Lifecycle Approach to Services and Solutions

Reducing Risk and Creating Value Throughout Your Production Lifecycle

ASSESS
DESIGN
IMPLEMENT
VALIDATE
MANAGE
Tamper Detection allows customers to quickly detect if something in their system has been modified

- Rockwell Automation® solutions available today include:
  - Firmware Digital Signatures
  - FactoryTalk® AssetCentre Auditing
  - Controller Change Detection and Logging
  - High Integrity AOIs
Tamper Detection
Firmware Digital Signatures

- Purpose of digital signature
  - Help protect firmware from accidental and malicious corruption
  - Help ensure firmware was generated by Rockwell Automation®

- How they’re being introduced...
  - New products have their firmware digitally signed from day 1 (L7x, Micro800®…)
  - Digitally signed versions of existing products released as feasible (EN2T, DNB…)

- How they work...
  - Rockwell Automation® digitally signs firmware kits with a private key when they are released
  - Devices locally check the signature with a corresponding public key
  - Any change to the firmware kit will cause the signature check to fail in device
Tamper Detection:
FactoryTalk® AssetCentre Auditing

- Centrally collect records of all interactions with the control system
Tamper Detection:
Controller Change Detection

- Every Logix Controller exposes a Change Detection Audit Value
- When something happens that can impact the behavior of the controller, the value changes
- Audit Value is available in RSLogix 5000, in other software applications and in other controllers via Message instruction
- The set of events that causes the Audit Value to change can be configured
Tamper Detection:
Controller Change Detection

- The Audit Value is stored in every Controller Log entry
- FactoryTalk® AssetCentre (in version 4.1), can monitor the Audit Value and read in the Controller Log

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>remark</td>
<td>TSV-Controller-Log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>remark</td>
<td>Date = Jun-02-2011 15:21:20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>remark</td>
<td>Controller = 1756-L71/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>remark</td>
<td>Serial-Number = 16#0067_D1CF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>remark</td>
<td>Revision = 20.02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Record Number</td>
<td>Time</td>
<td>Entry Description</td>
<td>User Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Change State Value</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>1 Jun-02-2011 15:21:07</td>
<td>Project download</td>
<td>NA\clark [ Daniel W. Clark ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16#FD60_C889_029F_3500</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>2 Jun-02-2011 15:21:07</td>
<td>Change Log entry added</td>
<td>NA\clark [ Daniel W. Clark ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16#FD60_C889_029F_3521</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>3 Jun-02-2011 15:21:38</td>
<td>CCUID Configuration update</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16#FD60_C889_029F_3566</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>4 Jun-02-2011 15:21:38</td>
<td>Change Log entry added</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16#FD60_C889_029F_35BF</td>
</tr>
</tbody>
</table>

FactoryTalk® AssetCentre
Tamper Detection:
High Integrity Add-on Instructions (AOIs)

- High Integrity AOIs allows you to generate a signature for an AOI definition
- Use High Integrity AOIs to:
  - Address the needs of regulated industries for auditing purposes
  - Maintain consistency and revision control in libraries
Security Value: Content Protection

Content Protection allows customers to control access to specific objects within their controllers and other assets.

- Rockwell Automation® solutions available today include:
  - Logix Source Protection
Content Protection:

Source Protection

- Assign a password to any Routine or Add-On Instruction
Application Access Control allows you to control who can do what from where in your automation system

- Rockwell Automation® solutions available today include:
  - Data Access Control
  - FactoryTalk® Security
Application Access Control:

Data Access Control

- External Access Attribute – Read/Write, Read Only, or None
  - Controls which tags can be modified from an HMI or other external application

- Constant Attribute
  - Controls which tags can be modified by controller logic
  - Changes to Constants bump the Audit Value
  - FactoryTalk® Security can control permission to change Constants
Application Access Control
FactoryTalk® Security

Use FactoryTalk® Security to…

- Manage the insider threat by authenticating the user and authorizing the use of Rockwell Automation® software applications to access automation devices

How does it work?

- Provides a centralized authority to verify identity of each user and grants or deny user's requests to perform a particular set of actions on resources within the system.

FactoryTalk® Directory

- Authenticate the User
- Authorize Use of Applications
- Authorize Access to Specific Devices

(All FactoryTalk® Security enabled software)
Application Access Control:
FactoryTalk® Security

- Administrators can manage
  - User Accounts
    - Windows
    - FactoryTalk®
  - User Groups
    - Custom group or role
    - Windows Group
- Computers
  - Computer Groups
- System Policies
- Product Policies
- Product Actions
Application Access Control:
FactoryTalk® Security

PC #1: Logix5000™ Project
ID = 795D5EF-12...
ID= 795D5EF-12...
Security Authority
Security Administration

PC #2: Logix5000™ Project
ID = A73R5CG – 89...
Security Authority
Security Administration

EtherNet/IP

ID’s Match
ID’s Don’t Match

Controller Properties
- Security Authority: FactoryTalk Security (RACORE)
- Require Matching Security Authority ID for Authentication and Authorization
Summary

Rockwell Automation®: Industrial Security Resources

- **Security-enhanced Products and Technologies**
  - Rockwell Automation® product and technologies with security capabilities that help increase overall control system system-level security.
  - [http://www.rockwellautomation.com/security](http://www.rockwellautomation.com/security)

- **EtherNet/IP Plantwide Reference Architectures**
  - Control system validated designs and security best-practices that complement recommended layered security/defense-in-depth measures.
  - [http://www.ab.com/networks/architectures.html](http://www.ab.com/networks/architectures.html)

- **Network & Security Services (NSS)**
  - RA consulting specialists that conduct security risk assessments and make recommendations for how to avert risk and mitigate vulnerabilities.
  - [http://www.rockwellautomation.com/services/security](http://www.rockwellautomation.com/services/security)
Summary
Industrial Security Landing Pad

Assessment Services
Security Technology
Security FAQ
Security Services
Leadership & Standards

Security Resources
Security Advisory Index
MS Patch Qualification
Reference Architectures
Assessment Services

http://rockwellautomation.com/security

secure@ra.rockwell.com
Pretty Good Privacy (PGP) Public Key
Thank you