T24 - Safe and Secure
Help Mitigate Your Risk through Services and Technology
Agenda

The Problem
Risk Landscape
Cyber Security Approach
People Safety Risk Reduction Methods
Risk Reduction Strategies
What Is Risk?

\[ \text{Risk} = f \{ \text{Vulnerability, Threat, Consequence} \} \]

**Vulnerability** = Attack Vector * Difficulty to Exploit

**Threat** = Intent * Opportunity * Capabilities

**Consequence** = Criticality or Impact to People Safety, Environment etc.
What Is Risk?

\[
\text{Risk} = f \left\{ \text{Vulnerability, Threat, Consequence} \right\}
\]
\[\text{countermeasures}\]

**Vulnerability** = Attack Vector * Difficulty to Exploit
VULNERABILITIES

Skills Gap
- Dearth of qualified personnel 1
- Achieving productivity goals
- Lack of staffing to expand operations 2

Assets
- Security is an afterthought
- Aging industrial control systems and protocols
- Lack of proper policies and procedures
- Evolving industrial security standards

Inflexibility
- Low adoption of risk management processes
- Shadow/stealth IT
- Lack of tools to manage infrastructure
- Too much data, lack of actionable information

IT/OT Convergence
- Lack of comprehensive asset inventory
- Integration of new technologies
- Integrate: customer demand, supply chain and industrial processes

(1) ARC Supplier Provided Automation Services
(2) Aberdeen Group
ICS ATTACK VECTORS

IT Network
- SIEM/SOC
- Servers
- www
- Email, Intranet, Business Planning & Logistics Network

OT Network
- Engineering Station
- Operator Workstation
- HMI
- SCADA Server
- Historian
- Pump
- Actuator
- Sensor
- Valve

ICS Supply Chain
- Remote Maintenance (Compromised VPN)
- On-site Maintenance (Compromised Device)

Direct Attack via IT Network
Direct Attack on Plant Network
Indirect Attack
External Adversaries

Insider Threat
What Is Risk?

\[
\text{Risk} = f \{ \text{Vulnerability, Threat, Consequence} \} \\
\text{countermeasures}
\]

\text{Threat} = \text{Intent} \times \text{Opportunity} \times \text{Capabilities}
THREAT LANDSCAPE

- Nation States
- Insiders
- Terrorists
- Hacktivists
- Cyber Criminals
THREAT LANDSCAPE

2010
- STUXNET: Worm Targeting SCADA and Modifying PLCs
- OPERATION AURORA: APT Cyber Attack on 20+ High Tech, Security & Defense Companies

2011
- NIGHT DRAGON: Advanced Persistent Threat Targeting Global Energy
- DUQU: Worm Targeting ICS Information Gathering and Stealing

2012
- SHAMOON: Virus Targeting Energy Sector Largest Wipe Attack
- FLAME: Virus use for Targeted Cyber Espionage in the Middle East
- GAUSS: Information Stealer Malware

2013
- RED OCTOBER: Cyber-Espionage Malware Targeting Government and Research Organizations

2014
- HAVEX: Industrial Control System Remote Access Trojan & Information Stealer
- HEARTBLEED: Security Bug and Vulnerability Exploited by Attackers

2015
- BLACKENERGY: Malware Injected into Ukrainian Power Company Network, Cut Power to the Affected Region

2016
- BLACKENERGY: Malware Injected into Power Company Network, Attackers Cut Power to the Affected Region
- OP GHOUL: Spear-phishing Campaign Targeting Middle East Industrial Organizations

2017
- NOTPETYA: Ransomware Malware Based On Stolen NSA Exploits that Impacted ICS Systems
- WANNACRY: Ransomware Malware Based On Stolen NSA Exploits that Impacted ICS Systems

ICS CERT INCIDENT COUNT
**Only Reported Incidents in U.S.

- 2010: 140
- 2011: 197
- 2012: 257
- 2013: 245
- 2014: 295
- 2015: 290
- 2016: TBD

Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved.
What Is Risk?

Consequence = Criticality or Impact to People Safety, Environment etc.
Consequences

Robert M. Lee and Michael Assante, SANS Institute, The Industrial Control System Cyber Kill Chain
INDUSTRIAL CYBER RISK EQUATION

Vulnerabilities

Unknown asset inventory
Out of date, unpatched infrastructure
Lack of skilled resources

Threats

Spillover from Nation State Campaigns
Wiper/Ransomware

Consequences

Impact to:
Achieving Business Objectives
Unplanned Production Loss
Environmental Impact
Human Health & Safety

Countermeasures

Basic Industrial Cyber Hygiene + Advanced Countermeasures
Risk Management

Notional Information and Decision Flow within an Organization: NIST Cybersecurity Framework

Implementation
ICS Security Methodology: Strategic vs. Tactical

Securing your operations networks with a risk-based approach
THE APPROACH

Strategic
- Help develop an OT cyber security program
- Adopt an industry framework
- Understand customer 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
Attack Continuum

BEFORE

DURING

AFTER
INDUSTRIAL CYBER RISK EQUATION

Vulnerabilities

Threats

Consequences

Countermeasures

Impact to:
Achieving Business Objectives
Unplanned Production Loss
Environmental Impact
Human Health & Safety

Spillover from Nation State Campaigns
Wiper/Ransomware

Basic Industrial Cyber Hygiene + Advanced Countermeasures

Unknown asset inventory
Out of date, unpatched infrastructure
Lack of skilled resources
ASSET INVENTORY SERVICES: How Does It Work?

With context built from other inventory methods, a disciplined **Active Approach** can be used to fill gaps in attributes collected.

A continuous **Passive Approach** collects asset inventory by using Deep Packet Inspection technology that understands both IT and OT protocols to enumerate asset identifiers, including communication flow maps.

A Rockwell Automation® **Installed Base Evaluation™ (IBE)** collects both connected and non-routable, isolated, or disconnected assets through a manual walkthrough approach.

A Rockwell Automation **Software Inventory Evaluation** acquires Windows-based attributes to understand vulnerability footprint and remediation steps required.
How Does It Work?

**Release Patch Rollups:**
- Security fix
- Quality fix

**PatchQual Lab Tests**
- Qualification levels (fully, partially, etc)

**Stage Patches in an Azure-based WSUS:**
- Fully qualified patches to match customer's OS/applications revision

**Self Service:** You have the patches you need specifically for your environment and may update them as you see fit.

**Managed:** Using vSphere HA and WSUS, we work with your team to remotely test, verify and apply patches based on standard/best practice procedures that meet your production workflows.

**Fully Patched and secure ICS infrastructure**

**Microsoft**
**Rockwell Automation**
**Your Infrastructure**
INDUSTRIAL CYBER RISK EQUATION

Unknown
Out of Date, unpatched Infrastructure
Lack of skilled resources

Vulnerabilities

Spillover from Nation State Campaigns
Wiper/Ransomware

Threats

Impact to:
Achieving Business Objectives
Unplanned Production Loss
Environmental Impact
Human Health & Safety

Consequences

Countermeasures

Basic Industrial Cyber Hygiene

Advanced Countermeasures
Plan, Design, and Implement

- Review infrastructure and documentation
- Appliance implementation
- Definition of asset criticality
- Review and sterilization of baseline results for immediate remediation

Manage, Monitor and Detect

OT Assets

Individually Managed Site Appliance

IT Assets

Deep Packet Inspection (DPI) on IT and OT Data Streams

Managed Service Provider with OT Knowledge

Centralized Self Management (IT SOC)

Respond, Recover

- Response and recovery plan development and review
- Containment, eradication and recovery workflows
- Characterize and scope potential impact
- Set course of action and incident reporting
## THREAT DETECTION SERVICES

<table>
<thead>
<tr>
<th>CAPABILITIES</th>
<th>BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Continuous passive and vendor agnostic asset discovery and identification</td>
<td>▪ Improve visibility of ALL connected plant floor assets</td>
</tr>
<tr>
<td>▪ Automated detection of operational and security anomalies</td>
<td>▪ Improve cyber defense capabilities for the OT environment across the</td>
</tr>
<tr>
<td>▪ Self managed or managed by Rockwell Automation</td>
<td>cyber attack continuum</td>
</tr>
</tbody>
</table>

**Powered by** CLARITY
INDUSTRIAL CYBER RISK EQUATION

Unknown Asset Inventory  Out of date, unpatched infrastructure Lack of skilled resources

Vulnerabilities

Spillover from Nation State Campaigns Wiper/Ransomware

Threats

Impact to:
Human Health & Safety

Consequences

Countermeasures

Basic Industrial Cyber Hygiene + Advanced Countermeasures
Focus on Consequence to Improve People Safety

Vulnerability = Attack Vector * Difficulty to Exploit

Threat = Intent * Opportunity * Capabilities

Consequence = Criticality or Impact to People Safety, Environment etc.
How Do We Define Impact to People Safety?

- Industry Standards: OSHA, ISO, IEC, ANSI, NFPA
- Common Industry Practice is to follow Hazard Risk Number (HRN)
  - Degree of Possible Harm (DPH)
  - Likelihood of Occurrence (LO)
  - Frequency of Exposure (FE)
  - Number of People at Risk (NP)

\[ HRN = f \{ \text{DPH, LO, FE, NP} \} \]
Target Ways to Reduce the Impact

- **Degree of Possible Harm (DPH)**
- **Likelihood of Occurrence (LO)**

- **Frequency of Exposure (FE)**
- **Number of People at Risk (NP)**
Analogy: Bicycle Helmet Safety

**Past**
- Functionally Safe!
- Uncomfortable
- Heavy
- Hot

**Present**
- Functionally Safe!
- Comfortable (pads)
- Light (foam or composite)
- Cool (ventilation)

**Performance enhancing!**
- Functionally Safe!
- Comfortable
- Light
- Cool
Technological Safety Components

- **Past**
  - Functionally Safe!
  - Cumbersome
  - Difficult to apply
  - Difficult to use
  - Often Bypassed

- **Present**
  - Functionally Safe!
  - Easy to apply
  - Safety Rated Products
  - Local Diagnostics

- **Performance Enhancing**
  - Functionally Safe!
  - Flexible
  - Task Oriented
Go from Risk to Results

SAFETY LIFECYCLE
Evaluate Hazards. Prioritize Improvements.

1. ASSESSMENT
2. SAFETY FUNCTIONAL REQUIREMENTS SPECIFICATION (SFRS)
3. DESIGN & VERIFICATION
4. INSTALLATION & VALIDATION
5. MAINTAIN & IMPROVE

Comply with Standards
Reduce Risk
Optimize Production
Task and Team Based Risk Assessment

Team

Task

Hazard

Solution
Technology to Help Reduce Risk

- Software for Task Based Design
- QR Code Instant Access to Safety
- Safety Lifecycle Progression Tools
- Machine Interaction Tracking
Services to Help Reduce Risk

- **Risk Assessments with Production Focus**
  - Recommended Actions
    - **Guarding**
      - Reduce gap by repositioning
      - Add fixed guard under access
    - **Control Logic**
      - Add key lockout
      - WARNING: Ensure lockout is used
    - **Other**
      - 1. Overhead arm and feed mechanism motion
        - Likelihood of Occurrence (LO)
        - Potential protective measures included in full report

- **Site Safety Prioritization Planning**

- **Safety Program Development & Management**
Thank You!