Current state of Global Cyber Security
Customer Challenges
Increased Attacks on Power Gen ICS – Unpatched systems still a major threat vector

In the news

In the second half of 2016, about 20 thousand different modifications or malware representing over two thousand different malware families were detected in total in industrial automation systems.

Threat Landscape for Industrial Automation Systems, 2nd half 2016, Kaspersky Lab ICS CERT

67% perceived severe or high levels of threat to control systems, up from 43% in 2015.

SANS 2016 State of ICS Security Survey of 236 companies operating ICS, (utilities = 26% of respondents)

As the WannaCry pandemic has shown once again, the up to date patching of generic systems like Windows OS is a crucial security measure. Currently these are run regularly (at least fortnightly) by six in ten of the sample, with the remainder taking this action more infrequently.

The State of Industrial Cybersecurity 2017
Customer Challenges

Increased Attacks on Power Gen ICS – Unpatched systems still a major threat vector

In The News

In FY 2016, ICS-CERT coordinated 2,272 vulnerabilities. This number is significantly greater than the number of vulnerabilities reported in prior years. The dramatic increase is primarily due to two vulnerability reports containing hundreds of vulnerabilities, identified by using automated scanning tools. The scanning tools expedite the detection process and make it easier to detect out-of-date third-party software.

Customer Challenges
It’s hard to hire and staff security related roles needed to maintain industrial control systems

State of Cybersecurity

- 54% of industrial organization have had more than one cyber incident in the last 12 months.
- 1.2 million per year is the annual price of ineffective security solutions in industrial organizations.
- 50% of respondents find it difficult to hire the ICS cybersecurity employees with the right skills.

Some numbers

- A report from Cisco puts the global figure at one million cybersecurity job openings.
- Demand is expected to rise to six million globally by 2019, with a projected shortfall of 1.5 million, says Michael Brown, CEO at Symantec, the world’s largest software vendor.

Leading to:

- **Greater burdens on plant staff:** These security requirements create more work for plant staff. On average, staff at power generation facilities can spend between 15 to 40 hours per month on basic DCS security maintenance, including system hardening, patch management, patch and AV application and back up.
- **Greater demands on corporate security and IT staff:** Corporate teams are often asked to track and report to auditors and enterprise risk group metrics that reflect patch level, frequency of back ups and status of system hardening. These corporate teams seek more automated reporting tools that can make it easier to report on the security posture of all the plants in their fleet.
Cyber Security Workplace 1.1
A suite of security applications that offers our customers a roadmap to achieve improved reliability and automate efforts to utilize the latest cyber security tools and techniques.
The Play – Cyber Security Workplace

Solution to automate, manage and provide visibility to security controls for Symphony & System 800xA

Features

- Secure & Patch/ Anti-virus deployment (applicable & tested updates)
- Automated Backup and Restore function
- Status reports for Patch Management, Antivirus updates, Backup & Restore, and Group Policy (Hardening)
- System hardening implementation:
  - Identification of unnecessary software components
  - Windows Firewall configuration to close unnecessary communications ports
  - Windows Service configuration to disable unneeded operating system services

Benefits

- **Reduce internal labor** required to maintain and update ICS security by a minimum of 24 hours or more a month
- **Provide greater visibility** to access ICS security status reporting
- **Minimize risk** of updates not being completed on a timely basis or potential operational impacts from manual application (i.e., impact to communication from un approved patch being applied)
The Play - Cyber Security Workplace

Our solution

Why ABB Industrial Automation Energy Industries?

— “ABB recognizes the importance of cyber security in control-based systems and solutions for infrastructure and industry, and is working closely with our customers to address the new challenges.” ABB CEO

— As the designer and service provider of the DCS, ABB is able to assure security updates are made without impacting availability.

— ABB understands the demands of operating plants and has created a system that allows operators to maintain their plants’ security posture while minimizing impacts on labor and processes

Return on Investment

Cyber Security Workplace Return on Investment per power block* assuming monthly patching & reporting:

- 2 hrs/ month: download applicable updates
- 8 hrs/month: complete back-ups before & after patching
- 10 hrs/month: apply patches & create audit reports
- 4 hr/month: reviewing patches applied & aggregating input corporate risk reporting

Total Annual Benefit = $ 43,200
24 hours per month @internal labor cost of $150/hour

*Assuming site has 2 servers + 6 nodes
Cyber Security Workplace

How it works

Getting Started
At installation, ABB Control System is backed up, patched to current levels and systems are hardened through removal of unnecessary software components, ports and services.

Monthly Updates
Each month ABB validates and tests applicable OS security updates and Anti Virus Signatures.

Back Ups
These validated updates delivered to the Cyber Security Workplace through the security update service (ABB WSUS). All HMI, servers, engineering work stations and historians are backed up before patches are applied.

Operator Engagement
Patches are applied serially based on an operator acknowledged command and schedule.

Reporting
The operator can use Cyber Security Workplace to generate a report showing all OS and AV updates were completed. This provides a handy artifact to show compliance to internal standards or national regulations.
Cyber Security Workplace – At a glance

Network topology
Cyber Security Workplace - Supporting foundation security controls
Support for international standards, national regulations and recommended best practices

IEC/ISA

**Solution Hardening:**
- Ongoing support of system hardening, including Identification of unnecessary software, components and unnecessary ports, services and programs are removed or disabled
- Automated identification of missing patches
- Anti-Virus provided for Servers and nodes and capabilities for validating/installing latest definitions

**Patch Management:**
- Centralized service to audit and deploy security patches
- Patches are tested in ABB labs to validate applicability and compatibility
- Procedures or patching and work arounds for unapproved patches
- Patches are developed and delivered to customer via secured supply chain, allowing customer to meet chain of custody requirements

**Backup and Recovery:**
- Best practices, documentation and automation to support backup/recovery
Cyber Security Workplace 1.1 – At a glance

Features

Security Patch Management
- Scans the system and reports patch status and gaps for configured nodes
- ABB validates and creates a monthly approved patch list

Anti-Virus Management (AV)
- Scans the system and reports AV status and gaps
- Updates Malware Definition Files (DAT)

System hardening status and deployment (S+ only)
- Scans and detects variances in the system hardening settings (aligned to the secured-deployment status).
- Removes unused software and OS services
- Set inbound and outbound Windows firewall rules

Group Policies hardening report for Symphony Plus and 800xA systems
- Detects incongruencies in the configuration of the Group Policies of the system, and produce a report.

Backup & Restore
- Configure backup routines and schedule them automatically
- Restore previously backed-up system data

Reporting
- Traffic light dashboards showing details for each node
- Detailed report for each node on user request
Cyber Security Workplace
Reliability - Compliance

Best Practices

Industry best practices for DCS include a critical focus on vulnerability management

1. Obtain structured vulnerability and patch feeds that cover a wide variety of sources.

2. Match the vulnerability disclosures and patch announcements against their asset inventory.

3. Prioritize vulnerability remediation efforts by considering ICS architecture location, simplicity of exploitation and possible impact on the controlled industrial process.
Cyber Security Workplace - Customer Use Case

Customer requirement:
- Reduce compliance work load, simplify/automate increasing compliance and corporate risk reporting
- Improved resiliency, automate backup and restore after a cyber/operational incident
- Automate routine security tasks (increasing cyber work load on small cyber focused team)

ABB solution: Cyber Security Workplace
- Automates and enforces foundational security best practices: automated patching, backup/restore and system hardening

Benefits:
- Significant reduction of monthly manual efforts
- Reduced patch related audit prep hours by 85%
- Technology enforces and automates security best practices, providing greater resiliency
Why ABB?

– Reduce system vulnerability while increasing system reliability
– Solutions to cost-effectively meet corporate/regulatory requirements
– Maintain system data integrity and operational availability
– Meet cyber and regulatory security requirements (NERC-CIP, NIST 800-53, ISA-99, IEC 62443)