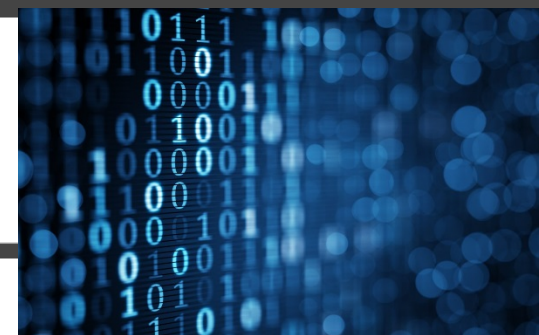




Italy
Section



Cyber security - why and how

Frankfurt, 14 June 2018

ACHEMA

Cyber Attack Continuum

Prevent, Detect and Respond



Allen-Bradley • Rockwell Software

Rockwell
Automation

Pierre Paterni
Rockwell Automation, Connected Services
EMEA Business Development Manager

The Threat is real!



There are two types of companies: those who **have been hacked**, and those who **don't yet know** they have been hacked.

John Chambers



IACS Security Myths



Common IACS Security Myths

- Cyber Threats are not Real
- Security by Obscurity
- Everything is under control (by CIO, CISO)
- High barriers to entry for attackers
- Hackers do not understand OT
- I am a ... (Food & Bev) manufacturer, I am not a target
- You can't do X, Y or Z in IACS because ...
- Management won't pay to secure the IACS

Reality

- 175,632 ICS accessible from the Web
- USB, modems, rogue WiFi...
- Cross disciplinary task force
- Hacking as a Service **HaaS**
- wiki/forums on SCADA ports
- Wannacry wake up call!
- Wannacry wake up call!
- Accepting the risk not an option anymore

Hacking: low barriers to entry



New Tool Automatically Finds and Hacks Vulnerable Internet-Connected Devices

Hacking just got fully automated for script kiddies.

FeaturesBusinessExploreMarketplacePricing

This repositorySearch

Sign in or Sign up

ITI / ICS-Security-Tools

Watch68Star220Fork72

CodeIssues0Pull requests0Projects0WikiInsights

Branch: master

ICS-Security-Tools / protocols / PORTS.md

Find fileCopy path

timyardley Update PORTS.md

9c7a730 on Apr 27, 2017

1 contributor

136 lines (122 sloc)5.01 KB

RawBlameHistory

Control Systems Ports

Standard Protocol Ports

The standard protocol ports table lists the ports for protocols that are considered industry standards and are used by multiple vendors.

Protocol	Ports
BACnet/IP	UDP/47808
DNP3	TCP/20000, UDP/20000
EtherCAT	UDP/34980
Ethernet/IP	TCP/44818, UDP/2222, UDP/44818
FL-net	UDP/55000 to 55003
Foundation Fieldbus HSE	TCP/1089 to 1091, UDP/1089 to 1091
ICCP	TCP/102
Modbus TCP	TCP/502
OPC UA Binary	Vendor Application Specific
OPC UA Discovery Server	TCP/4840
OPC UA XML	TCP/80, TCP/443



[Submit answers for another facility](#)

Welcome back, ppatern1@ra.rockwell.com!

[Manage Account](#)[Log Out](#)

Detailed Comparison

Below is your facility's Detailed Comparison to other manufacturing facilities.

You can download your report to either PDF  or Excel 

Select your criteria

Apply as many criteria as you'd like, but please note that the tool will not display data for fewer than five facilities for any search.

[Return to Quick Evaluation chart](#)

Number of Responses Matching Search Criteria : 171

▼ Type of manufacturer

▼ Industry

▼ Region

▼ Use of custom-built AOIs

Run report

Reset

ISA/IEC 62443

Certified Products, Systems and System Delivery



Series of standards that define procedures for implementing electronically secure industrial automation and control systems (IACS).



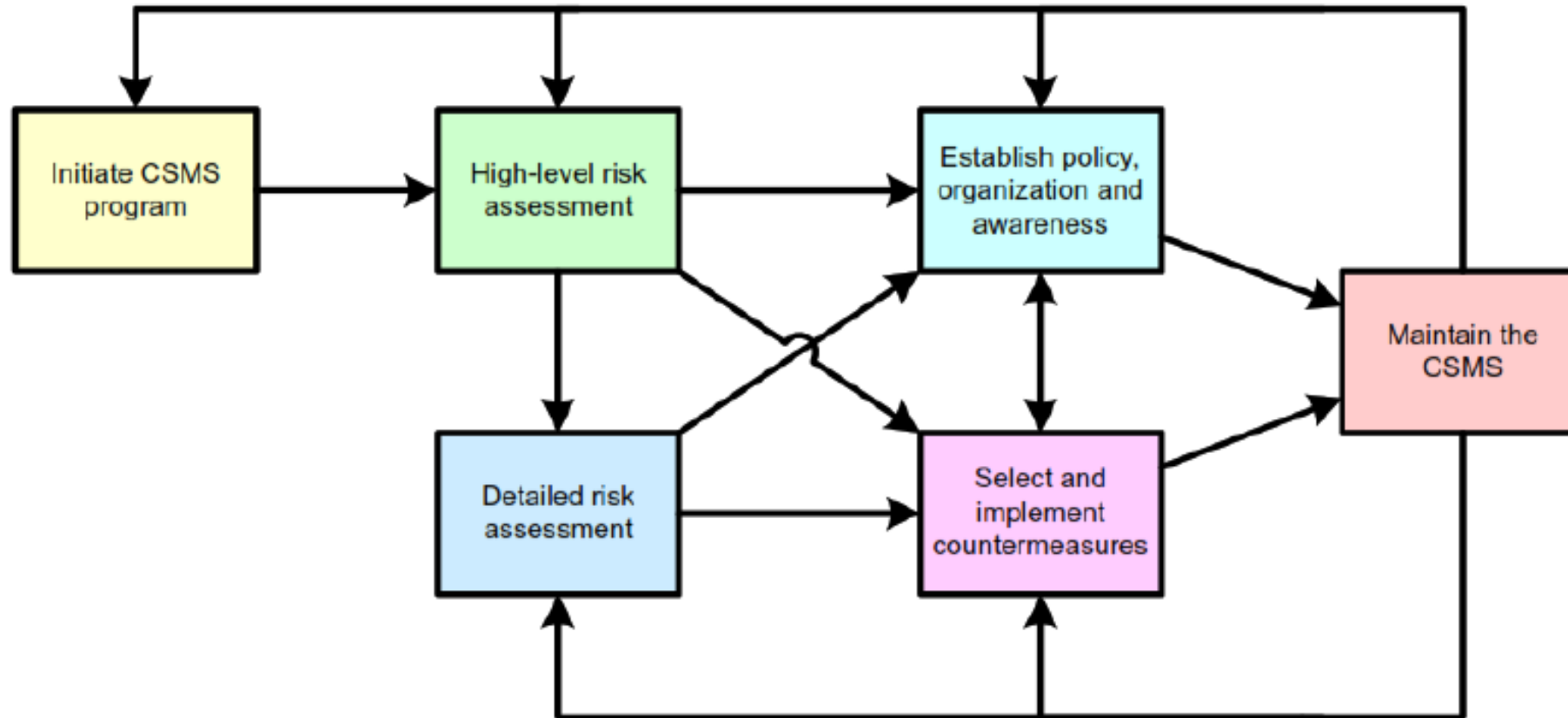
Applies to those responsible for *designing, manufacturing, implementing, or managing* industrial control systems:

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



ISA/IEC 62443 establishing a CSMS

Cyber Security Management System – 6 top level activities



Source: IEC62443-2-1 Establishing an Industrial Automation and Control Systems Security Program

NIST Cybersecurity Framework



Functions	Categories
IDENTIFY (ID)	Asset Management (AM)
	Business Environment (BE)
	Governance (GV)
	Risk Assessment (RA)
	Risk Management Strategy (RM)
PROTECT (PR)	Access Control (AC)
	Awareness and Training (AT)
	Data Security (DS)
	Information Protection Processes and Procedures (IP)
	Maintenance (MA)
	Protective Technology (PT)
DETECT (DE)	Anomalies and Events (AE)
	Security Continuous Monitoring (CM)
	Detection Processes (DP)
RESPOND (RS)	Incident Response Planning (RP)
	Communications (CO)
	Analysis (AN)
	Mitigation (MI)
	Improvements (IM)
RECOVER (RC)	Recovery Planning (RP)
	Improvements/Gap Remediation (IM)
	Communications (CO)

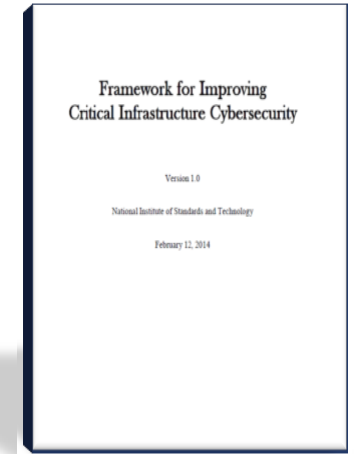
◀ Know what you have

◀ Secure what you have

◀ Spot threats quickly

◀ Take action immediately

◀ Restore operations





ICS Security Consulting Services

What is it?

A security assessment helps understand the risk posture of your ICS environment to identify vulnerabilities and areas of improvement against established ICS Cyber Security Standards such as ISA/IEC 62443, NIST 800-82 and NIST CSF.

What are the best practices?

A thorough security assessment strategy for ICS requires the following:

- Identification of an organization's risk tolerance
- Measuring the environment against an ICS Security Standard or Framework
- Building an asset inventory, understanding of "what you have"
- A list of vulnerabilities for those assets
- A review of how those assets being protected from cyber attack
- A review of current security policies and procedures
- Finally recommendations of how to address the current vulnerabilities associated with assets, policies, procedures and methods to defend against cyber risk

Why Rockwell Automation?

Network and Security Services (NSS)



Differentiation

- Converged skill set of operational technology (OT) and information technology (IT)
- Experience across industrial control applications and networks
- Breadth of industry standard committee (ISA, NIST, INL, DHS...) participation
- Ability to address security risks without sacrificing productivity
- Full lifecycle service offering with global delivery capability
 - For plant personnel, who need secure industrial infrastructure, NSS is a team of industrial automation and IT experts that assess, implement and support plant-wide network infrastructure
 - Unlike large IT vendors and resellers, we offer a comprehensive and tailored solution that balances both strategic and tactical needs of your company



Network &
Security Services

Example Counter Measures



Secure Infrastructure

1. Establish the perimeter (Zones & Conduit)
2. Harden the interior
3. Prevent & contain

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

Harden the Endpoints

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





Qualified Patch Management

What is it?

Patch Management in Industrial Control System (ICS) environments is required to maintain a secure application infrastructure, protecting assets from being compromised by malware and viruses.

What are the best practices?

A thorough patch/anti-virus (a/v) management strategy for ICS requires maintaining current knowledge of:

- Operating Systems and applications installed
- Currently installed and available patches and a/v updates.
- Deciding what updates are appropriate for particular systems
- Scheduling patching and a/v updates around production schedules
- Testing systems before and after installation
- Ensuring that patches are installed properly

How can we help?

Rockwell
Automation



**INDUSTRIAL
CYBER SECURITY
SERVICES**



Validated Windows Patch Subscription

Delivery of customer system specific validated Windows patches to your local Windows Server Update Services (WSUS) server from our managed cloud based WSUS.



Remote Patch and Antivirus Management

If needed, Rockwell Automations skilled IT/OT professionals can remotely conduct patch/anti-virus management services to verify a proper patching and anti-virus cadence is developed, robust testing procedures are implemented and executed, and compliance needs are met.

Key Takeaways!

Strategic

- Adopt a Cyber Security industry framework
- Initiate the cyber security program
 - Senior management support – business imperative
 - Define scope
 - IT & OT Alignment
- Understand business drivers and risk tolerances
- Conduct assessments to develop an understanding of gaps
- Work with trusted partners knowledgeable in **IACS + Security**



Thank You!



PUBLIC



Connect with us.

www.rockwellautomation.com

 *Allen-Bradley • Rockwell Software*

Rockwell
Automation