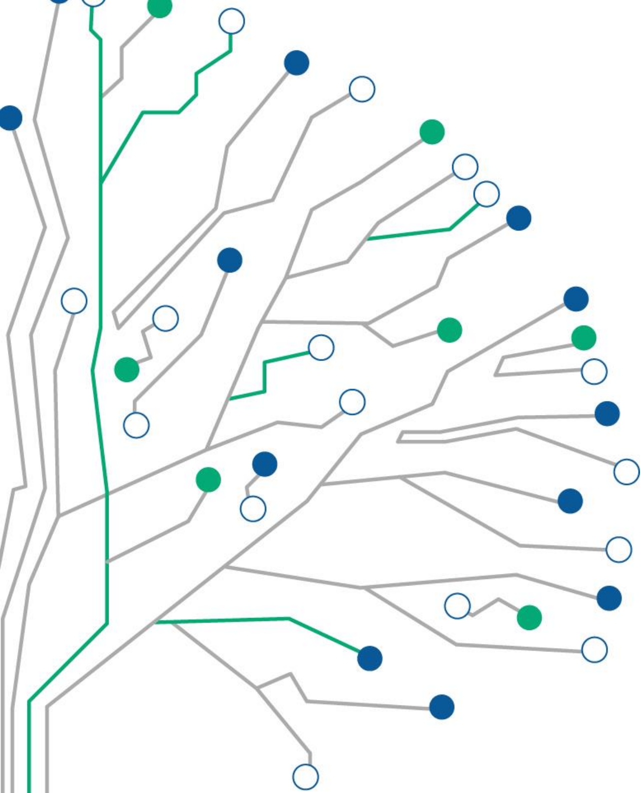


FORUM
TELECONTROLLO
RETI DI PUBBLICA
UTILITÀ 2013

ANIE
AUTOMAZIONE

ANIE FEDERAZIONE

CONFINDUSTRIA

ICS Cybersecurity

SANS Top 20 Critical Controls for ICS

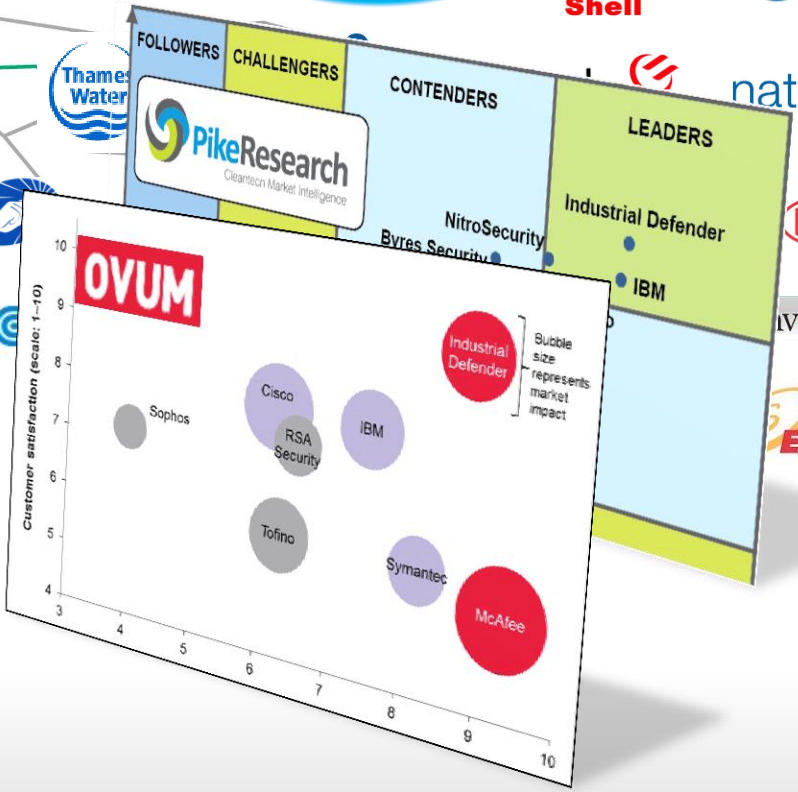
David Van Crout

FORUM TELECONTROLLO
RETI DI PUBBLICA UTILITÀ 2013

ANIE AUTOMAZIONE

ANIE FEDERAZIONE   CONFINDUSTRIA

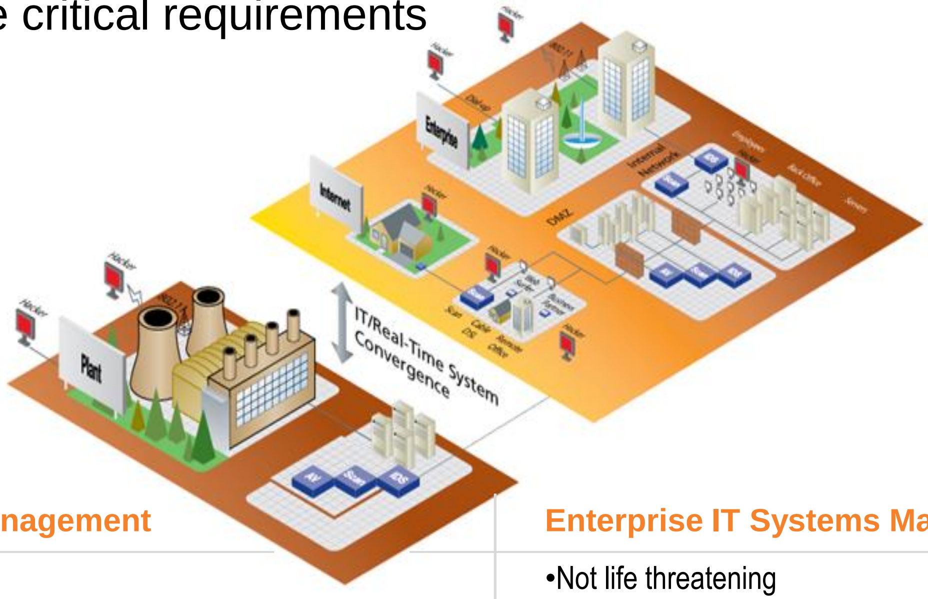
We ranked #**1 two years in a row** by independent analysts



- Security and compliance since 2002
- Exclusively focused on OT
- Pioneering **automation systems management** for security, compliance and change management
- Turnkey technology and service solution
    - Multiple applications, one platform
    - Vendor agnostic
    - Purpose built
- **10,000+ technology deployments**
- **400+ customers**
- **25+ countries**

Automation Systems Management

Understanding the critical requirements



Automation Systems Management	Enterprise IT Systems Management
• Safety first	•Not life threatening
• Zero downtime focus	•Availability important – reboot common
• Real-time focus	•Transactional orientation
• ABB, Siemens, GE, Honeywell, Emerson, etc.	•IBM, SAP, Oracle, etc.
• Few people; many, many devices	•People ~= Devices
• Sensors, Controllers, Servers, Industrial Devices (IED, RTU, PLC)	•PCs and Servers
• Polled process control model	•Web services model is dominant
• Purpose-specific devices	•Many commercial software products installed on each PC
• Industrial Protocols: ICCP, Modbus, DNP3, some over TCP/IP	•Protocol is primarily HTTP/HTTPS over TCP/IP - widely known
• Harsh operating plant environments	•Office environment, plus mobile
• Industry-specific regulations	•Cross-industry regulations (mostly)

Security

- **Vulnerabilities are on the rise: NEW public SCADA/ICS vulnerabilities increased 8x according to Symantec’s 2012 Threat Report**
- **ICS CERT reports dramatic increase in incidents**

“Electrical Grid Woefully Prepared for Cyber Security Threats, Says ABI Research”

ELECTRIC LIGHT&POWER POWERGRID INTERNATIONAL

“Major cyber attack aimed at natural gas pipeline companies”
May 7, 2012

msnbc.com

“Oil Companies Spring a Leak”
July 17, 2012

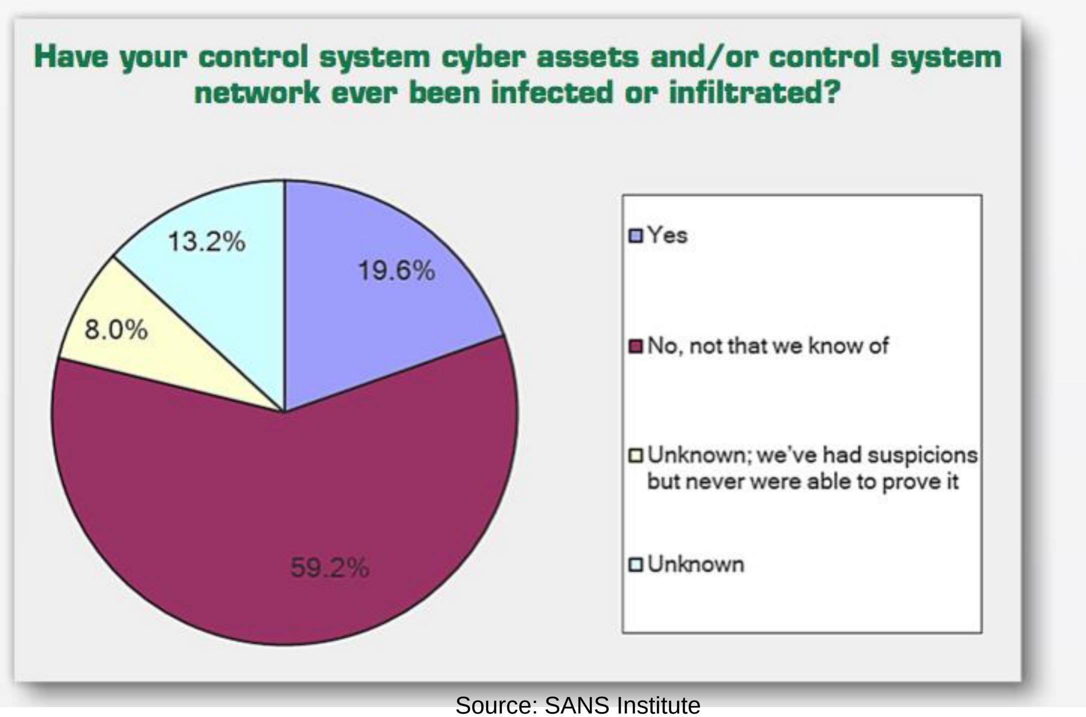
WIRED

“Hackers Lay Claim to Saudi Aramco Cyberattack”
August 24, 2012

The New York Times

Security is now a part of doing business

Not just headlines; ICS compromises are real.



Source: SANS Institute
SCADA Security Survey Feb. 2013

Compliance & Auditability

Governments and critical infrastructure sector companies feeling pressure to ensure cybersecurity.

WALL STREET JOURNAL

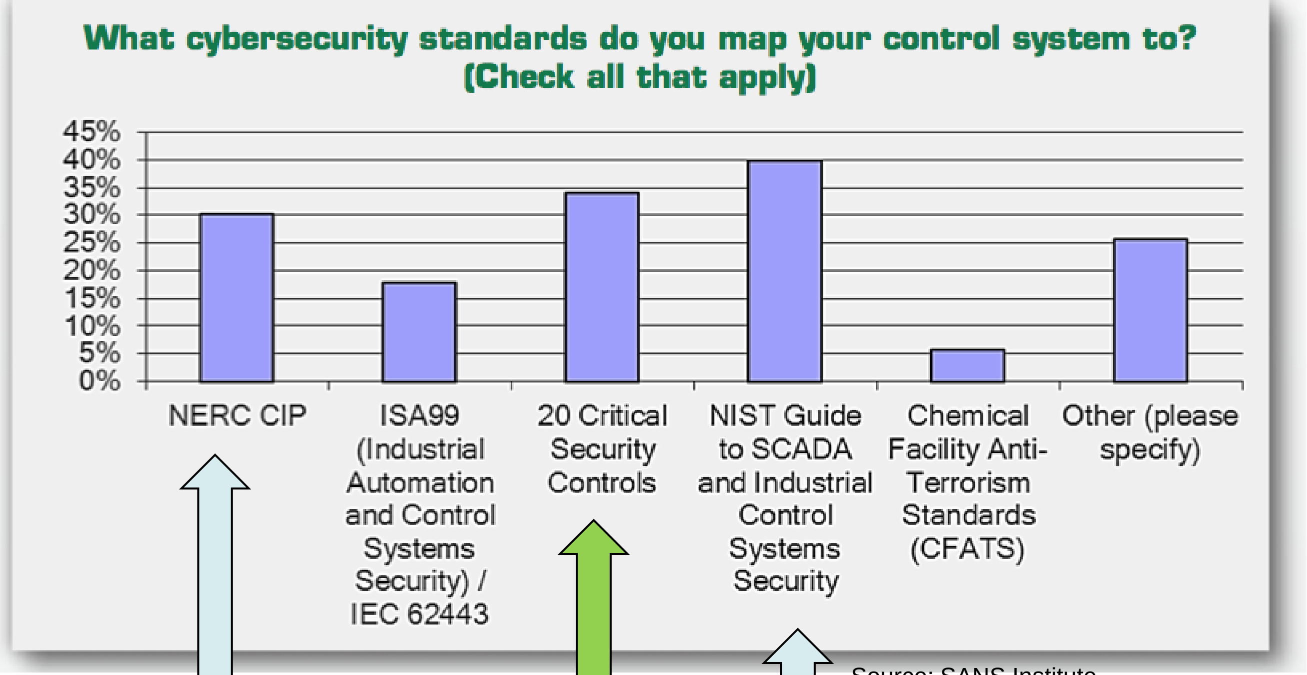
"Oil and Gas Lobby Resists Regulatio
Despite Cyber Risk" May 22, 2013

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Presidential Executive Order
On Cyber Security- Feb 13, 2013

Internal & External Compliance Initiatives are Steadily Increasing

What standards are being used? Survey says….



Source: SANS Institute
SCADA Security Survey Feb. 2013

NERC CIP V5 submitted to FERC: Jan 31, 2013

Exec Order 13636 specifies NIST framework

Change Management

“Cyber security approaches that start with grid reliability and change management appear to have been most successful”

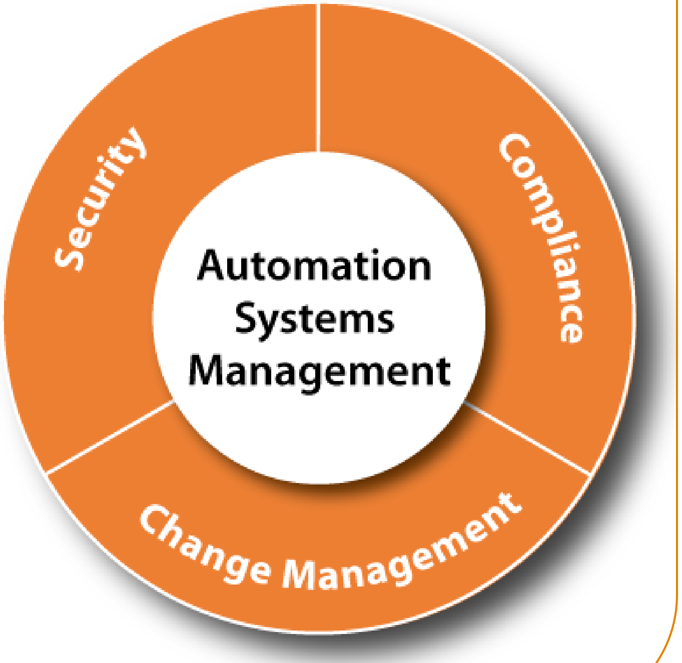
–Navigant Research, March 2013 10 Trends in Smart Grid

How will you manage change across a growing, heterogeneous complex automation environment

The Challenges in Automation Systems Management

- Automation Systems becoming more **complex**
  - Mix of legacy and next generation architectures
  - Heterogeneous Systems
  - Exponential Increase in intelligent devices
    - Smart meters by the millions
  - Unclear responsibility/ownership
- Need for increased **security**
- Increasing **compliance** requirements
- Managing **change** introduces additional business process requirements and labor allocation
- **Fewer** Resources / increasing skill set gaps
- Downward **Budgetary** Pressure

Managing Diverse Requirements of Automation Systems Environments
The convergence of:



Balancing Operational Requirements with Security, Compliance, Change Management requirements

The 20 Controls And Their Priority / Impact

Critical Security Control		Mitigation Ranking
1	Inventory of Authorized and Unauthorized Devices	Very high
2	Inventory of Authorized and Unauthorized Software	Very high
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Very high
4	Continuous Vulnerability Assessment and Remediation	Very high
5	Malware Defenses	High/Medium
6	Application Software Security	High
7	Wireless Device Control	High
8	Data Recovery Capability	Medium
9	Security Skills Assessment and Appropriate Training	Medium
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	High/Medium

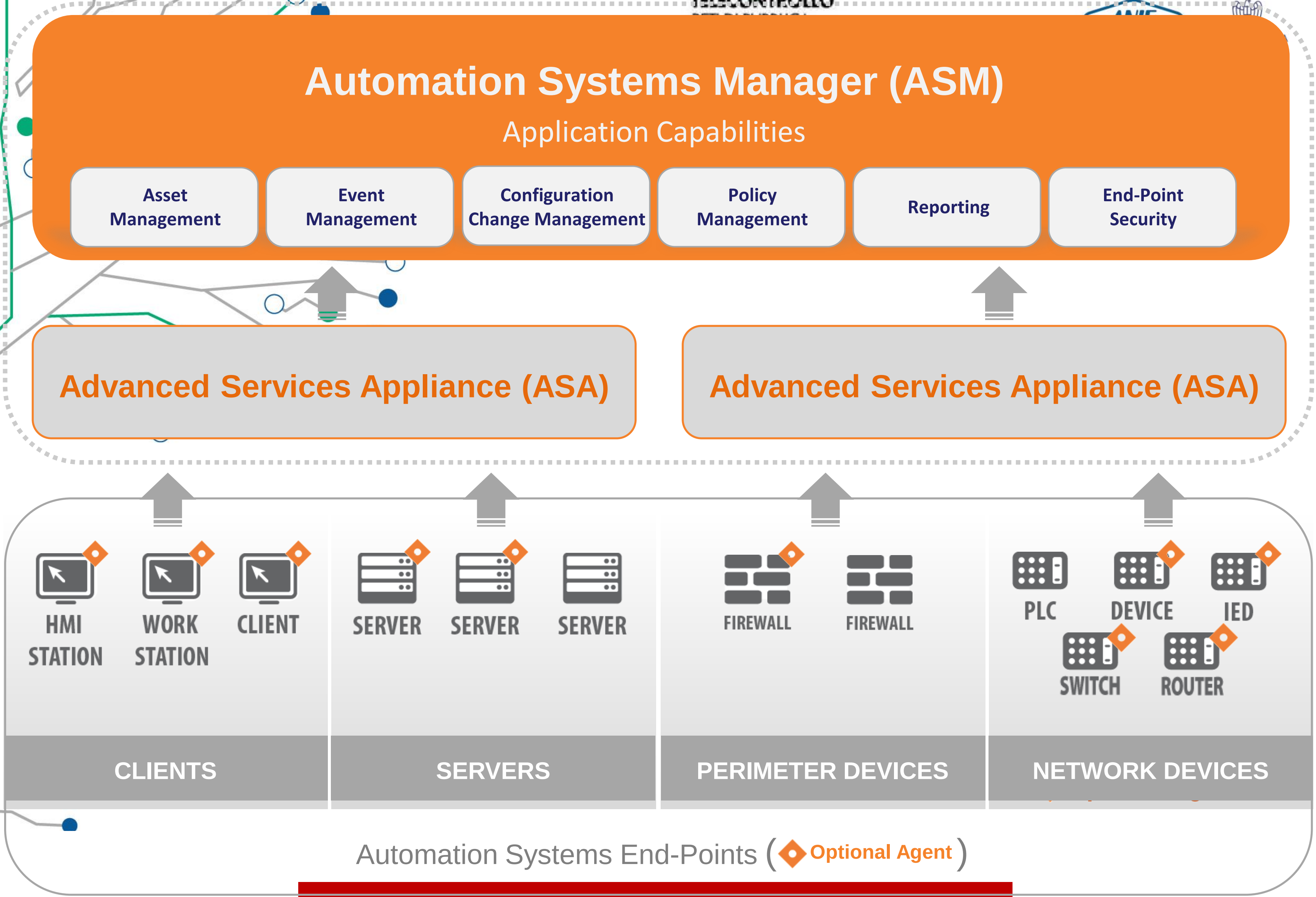
www.sans.org/critical-security-controls/

The 20 Controls And Their Priority / Impact

Critical Security Control		Mitigation Ranking
11	Limitation and Control of Network Ports, Protocols, and Services	High/medium
12	Controlled Use of Administrative Privileges	High/medium
13	Boundary Defense	High/medium
14	Maintenance, Monitoring, and Analysis of Audit Logs	Medium
15	Controlled Access Based on the Need to Know	Medium
16	Account Monitoring and Control	Medium
17	Data Loss Prevention	Medium/low
18	Incident Response and Management	Medium
19	Secure Network Engineering	Low
20	Penetration Tests and Red Team Exercises	Low

www.sans.org/critical-security-controls/

ASM Architecture



Software Applications essential to Security, Compliance and Change Management

Asset Management

A single **unified view of all assets** within the automation system's environment. Enables **onboarding and decommissioning of assets, reports device status, information access** and **state information**.

Event Management

Brings visibility to control system and networks by providing **event log data**. **Receives and consolidates events** from multiple security sources, **centralizes operations** and **reduces expenses**.

Configuration Change Management

Enables operators to **track and audit** device settings, software, firewall rules and user accounts and **view and baseline** the system configurations, ports & services, and software.

Policy Management

Enables operators to **communicate new policies, track acceptance** and **manage conformance**.

Reporting

A comprehensive suite of **standard configurable reports to meet regulatory requirements** (such as NERC CIP) and simplify adherence to **internal requirements**. Enables users to **define, generate and automate reports as needed.**

Integration with:

- ABB 800xA, ABB Symphony/Harmony, ABB Infi90, ABB FACTS and ABB SYS600C & MicroSCADA, Ventyx Network Manager
- Emerson DeltaV and Emerson Ovation
- Emerson/Westinghouse WDPF
- GE XA / 21 & PowerOn FUSION
- Foxboro I/A Series
- Honeywell Experion
- Itron OpenWay System
- Rockwell RSView
- Schneider Electric Momentum, Quantum, OASyS, Citec
- Siemens PCS7
- Yokogawa Centrum CS 3000
- ***and many more!***

Operating Systems

- Windows 7
- Win 2K R2, WinNT, Win 2003
- HP-UX PA-RISC & Itanium
- Linux
- DEC Tru-64
- Sun Solaris
- IBM AIX

Industrial Rules

- DNP3
- Modbus
- ICCP
- IEC
- Siemens S7 Protocol
- TCP/IP

Real World Solutions…..

Power Generation Customer

Case Study

Power Generation

Chemical Manufacture Customer

Case Study

Chemical Manufacture

Tri-State Generation and Transmission Association

Case Study

TRI-STATE

Case studies available for download…
http://www.industrialdefender.com/about/customers.php

Critical Control 1
Inventory of Authorized & Unauthorized Devices

Goal:

Reduce the ability of attackers to find & exploit unauthorized & unprotected systems.

Key Considerations for Control Systems:

Active scanners should never be used in ICS as some systems cannot deal with unexpected traffic & may cause denial of service.

How Automation Systems Manager helps:

ASM maintains a secure database of all IP devices in the target environment. New assets are alerted on, and require an approval process to be listed as a current configuration (aka: baseline) in inventory. Configuration versions are promoted through an approval process and can be downloaded for secure storage.

Critical Control 2
Inventory of Authorized & Unauthorized Software

Goal:

Mitigate or root out attacks by identifying vulnerable or malicious software, protect the good stuff

Key Considerations for Control Systems:

Any patches on ICS systems should be approved by the ICS providers and tested on a QA environment before going live.

How Automation Systems Manager helps:

ASM collects asset software information, including Operating System (OS), software, as well as, patch application and versions from the associated hardware assets in the inventory database.

An approval process is required to control changes to the configuration of the software assets. Policies can be created to alert on changes to a system's reference baseline.

Critical Control 3
Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations & Servers

Goal:

Prevent attackers from exploiting services & settings that allow easy access through networks & browsers

Key Considerations for Control Systems:

Cyber assets in the control system are generally configured by the vendor for maximum performance and reliability yet may not always follow security best practices, such as avoiding administrator accounts with easily guessed passwords. Configuration changes may not be allowed and may affect the availability of the system or might void warranty.

How Automation Systems Manager helps:

ASM performs strict configuration change management. Changes to configurations, including security settings, asset details, software, ports & services are alerted on & require approval to update the configuration baseline in the database. The previous configuration is archived, & the approved changes are included in the new configuration. Policies can be created to alert on pending changes to a system's reference baseline.

Critical Control 4 Continuous Vulnerability Assessment & Remediation

Goal:

Proactively identify & repair software vulnerabilities reported by security researchers or vendors.

Key Considerations for Control Systems:

Due to the resource constraints, performing vulnerability assessments on control systems should be approached with caution as they can cause restarts or denials of service.

How Automation Systems Manager helps:

ASM' change management processes can identify changes to assets in the inventory database, as well as configuration drift outside of organization-defined boundaries. Events are logged & archived at specified intervals.

Critical Control 5
Malware Defenses

Goal:

Block malicious code from adversely affecting reliability & performance standards, tampering with system settings or capturing sensitive data.

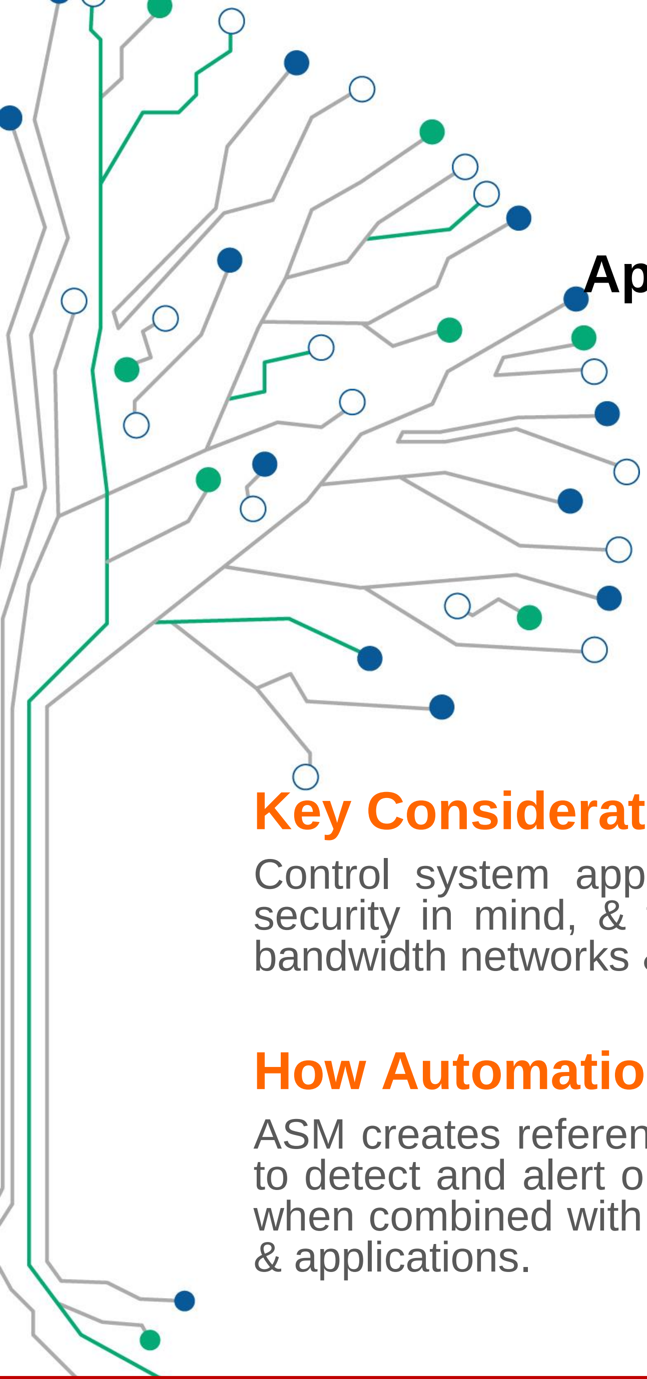
Key Considerations for Control Systems:

Control systems traditionally run on low bandwidth networks. Malware can upload code, run as a service and connect to external command & control servers, potentially causing a denial of service.

How Automation Systems Manager helps:

ASM technologies have the ability to scan traffic for malware & block what appears suspicious.

Integrated intrusion detection system adds further industrial control protocol-specific detection of malware signatures & behavior based anomalies.



Critical Control 6
Application Software Security

Goal:

Neutralize vulnerabilities in web-based and
other application software.

Key Considerations for Control Systems:

Control system applications have not traditionally been designed with security in mind, & traditional security software is not designed for low bandwidth networks & assets.

How Automation Systems Manager helps:

ASM creates reference baseline sets of asset information, & use policies to detect and alert on unnecessary libraries, components or compilers, & when combined with a NIDS will inspect traffic flowing across the network & applications.

Critical Control 7
Wireless Device Control

Goal:

Protect the security perimeter against unauthorized wireless access.

Key Considerations for Control Systems:

Wireless access is relatively uncommon in industrial control systems and implementation must be approached with caution.

How Automation Systems Manager helps:

ASM Policy management enables enforcement of authorized configurations & security profiles.

Configurations are securely stored in the File Repository by date/time stamp. Alerts on changes to configurations can be sent via email at specified intervals.

FORUM TELECONTROLLO RETI DI PUBBLICA UTILITÀ 2013

ANIE AUTOMAZIONE

ANIE FEDERAZIONE CONFINDUSTRIA

Critical Control 8
Data Recovery Capability

Goal:

Minimize the damage from an attack.

Key Considerations for Control Systems:

Backup and recovery process are essential to the prevention of unscheduled downtime. These processes are resource intensive, and require time and training to set up and maintain.

How Automation Systems Manager helps:

ASM has the ability to archive and backup most devices with text-based configuration files that can be used for restoration purposes. In conjunction with Survive™ services ASM provides automatic backup for assets, including OS, applications and data. Backups are verified and tested. Backup data files are encrypted, secured at rest and in transmission.

Critical Control 9
Security Skills Assessment & Appropriate Training to Fill Gaps

Goal:

Find knowledge gaps, & fill
them with exercises & training.

Key Considerations for Control Systems:

The ICS workforce is tasked with keeping the process running safely and reliably. The addition of cyber security awareness to the current training schedule is essential to protecting critical assets. Having current information on those assets is central to security training.

How Automation Systems Manager helps:

ASM provides information on the target assets that can be used as training materials. ASM asset management feature automatically keep the database updated, and has a unified view for better understanding & communication of security information on a wide variety of devices.

Critical Control 10
Secure Configuration for Network Devices such as Firewalls, Routers & Switches

Goal:

Preclude electronic holes from forming at connection points with the Internet, other organizations & network segments.

Key Considerations for Control Systems:

ICS are often connected to corporate networks & data flows between them. The defense of the perimeter is critical to avoid corporate side vulnerabilities that may affect the process control network segments.

How Automation Systems Manager helps:

ASM provides management of change information for software, patches, user accounts, and configurations of network devices, including routers, switches, firewalls, IDS and IPS systems. The ASM has the ability to archive and backup most devices with text-based configuration files that can be used for restoration purposes. In conjunction with NIDS & UTM, ASM will provide ingress and egress filtering, secure network virtual connections, and analyze network traffic for discovery of unauthorized access and signs of malicious activity.

Critical Control 11
Limitation & Control of Network Ports, Protocols & Services

Goal:

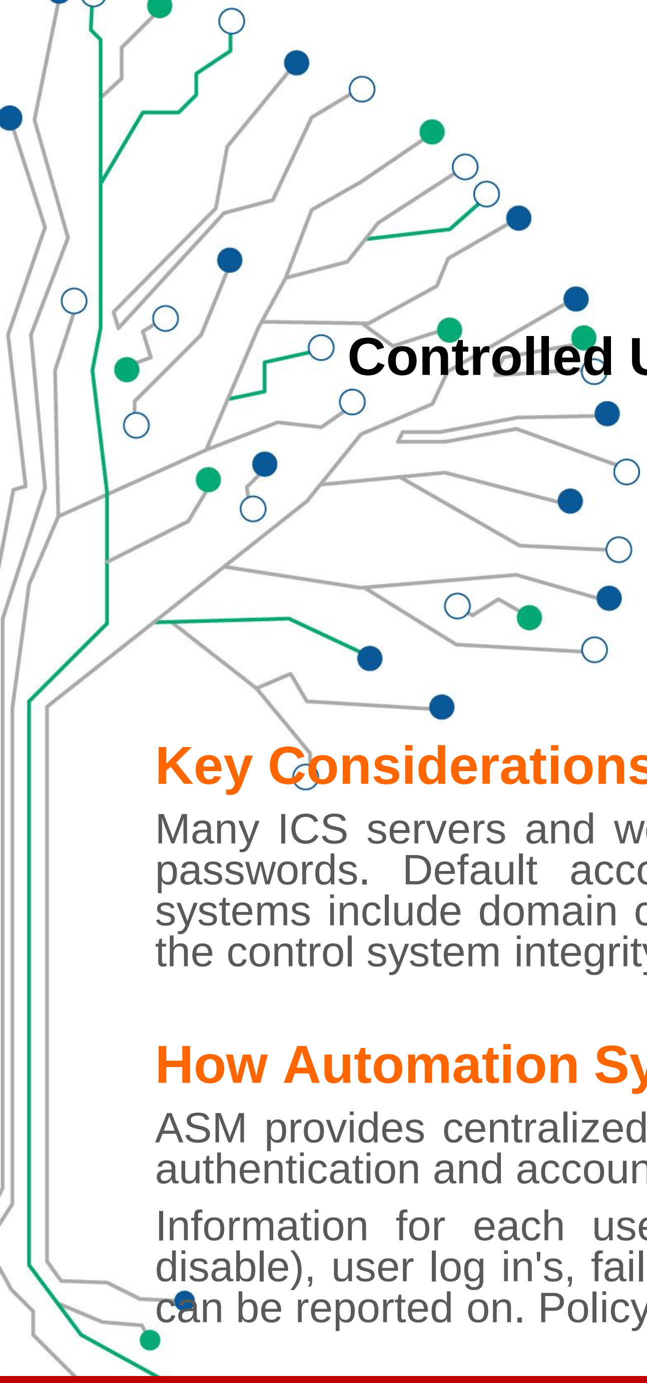
Allow remote access only to legitimate users & services.

Key Considerations for Control Systems:

Control system devices are normally preconfigured by vendors. The pre-configured state may lack robust security configurations and settings.

How Automation Systems Manager helps:

ASM automatically collects information on ports, protocols & services on assets in the control network. Reports can be run on demand or at regular intervals to show the status. Reference baselines can be updated & compared against.



Critical Control 12
Controlled Use of Administrative Privileges

Goal:

Protect & validate administrative accounts on desktops, laptops & servers to prevent common types of attacks.

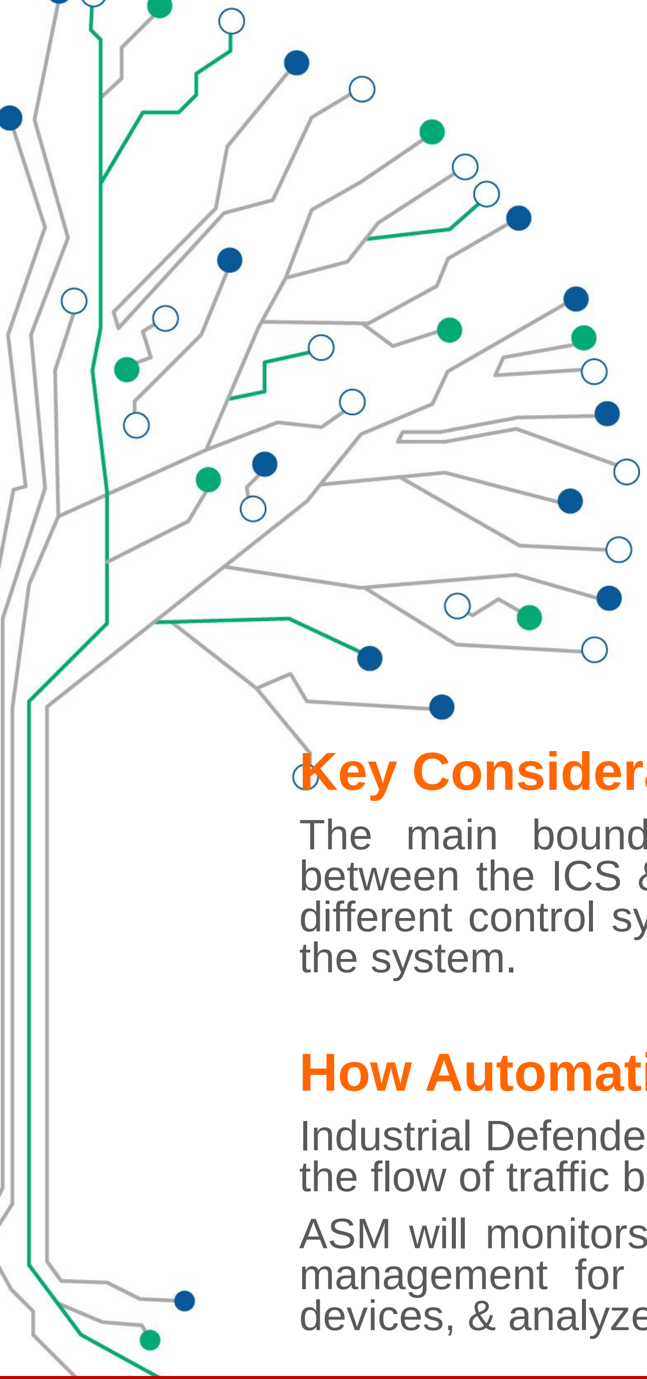
Key Considerations for Control Systems:

Many ICS servers and workstations use a set of standard user names and passwords. Default accounts often have administrator privileges. Many systems include domain controllers which if compromised could compromise the control system integrity.

How Automation Systems Manager helps:

ASM provides centralized monitoring, management and reporting of access, authentication and account management.

Information for each user includes: date/time of status (create, remove, disable), user log in's, failed log in attempts, unauthorized users, all of which can be reported on. Policy management can enforce complex passwords.



Critical Control 13 Boundary Defense

Goal:

Control the flow of traffic through network borders, & monitor for attacks & evidence of compromised machines.

Key Considerations for Control Systems:

The main boundaries in control systems are the interconnection between the ICS & the corporate network, the interconnection between different control systems, & 3rd party remote access points directly into the system.

How Automation Systems Manager helps:

Industrial Defender’s suite of technologies provides layers of defense for the flow of traffic between networks.

ASM will monitors devices, provide change management activities, log management for events that are collected from network monitoring devices, & analyze network traffic.

Critical Control 14
Maintenance, Monitoring & Analysis of Audit Logs

Goal:

Use detailed logs to identify & uncover the details of an attack, including the location, malicious software deployed, & activity on victim machines.

Key Considerations for Control Systems:

Event monitoring across disparate systems is time consuming & resource intensive.

Events that are correlated & aggregated will ensure that crucial information for forensics and preventive maintenance are seen on a timely basis.

How Automation Systems Manager helps:

ASM provides centralized event monitoring and log management from a wide variety of network & host-based devices, as well as remote & perimeter devices.

Log management uses aggregation & consolidation of events for analysis and alerting, & can be archived for years.

Critical Control 15
Controlled Access Based on the Need to Know

Goal:

Prevent attackers from gaining access to highly sensitive data.

Key Considerations for Control Systems:

While reliability and performance are primary drivers of control systems, they must be protected from exfiltration of intellectual property including network diagrams and system configurations.

How Automation Systems Manager helps:

ASM provides centralized logging for access events. Alerts are generated based on consolidation & aggregation of events & may be reported on.

Critical Control 16
Account Monitoring & Control

Goal:

Keep attackers from impersonating legitimate users.

Key Considerations for Control Systems:

Accounts are typically logged in for long durations and often shared between individuals.

How Automation Systems Manager helps:

ASM provides account management with centralized viewing & reporting of user accounts and associated user activities.

Customizable dashboards provide account information including new or modified user accounts, and user metrics such as failed login attempts.

Critical Control 17
Data Loss Prevention

Goal:

Stop unauthorized transfer of sensitive data
through network attacks & physical theft.

Key Considerations for Control Systems:

Data being syphoned through the control system could signal an intrusion & adversely affect network bandwidth and integrity.

How Automation Systems Manager helps:

ASM can provide centralized event logging and reporting while NIDS analyzes network traffic for discovery of unauthorized access and can flag network packages with key words as they traverse the network.

Critical Control 18
Incident Response Management

Goal:

Protect the organization’s reputation, as well as its information.

Key Considerations for Control Systems:

Control systems are more interconnected than ever before & malicious code can propagate in numerous ways including removable media unknowingly brought in by trusted vendors or contracts.

How Automation Systems Manager helps:

The ASM Asset Inventory report can be used for defining & describing protected assets.

Critical Control 19
Secure Network Engineering

Goal:

Keep poor network design from enabling attackers.

Key Considerations for Control Systems:

DMZ separation of the Control System and corporate enterprise layer ensures information flow is allowed only through secure channels.

How Automation Systems Manager helps:

The ASM provides central configuration management for IP based assets in the target environment.

Critical Control 20
Penetration Tests & Red Team Exercises

Goal:

Use simulated attacks to improve organizational readiness.

Key Considerations for Control Systems:

Use of vulnerability scanning and penetration testing tools in the ICS pose risks to the low bandwidth systems and must be approached with caution.

How Automation Systems Manager helps:

ASM continuously updates dashboards and reports of assets & asset configurations that will be used in penetration testing.

Reference baselines can be generated from the asset inventory, & policies can be written to produce reports on differences in assets after the penetration testing.

The log management provided by the ASM can be used to consolidate & aggregate events during the pen testing to simplify analysis.

INDUSTRIAL DEFENDER®

Kim Legelis

klegelis@industrialdefender.com

Web
www.industrialdefender.com

Blog
blog.industrialdefender.com

Twitter
@i_defender