



ITS

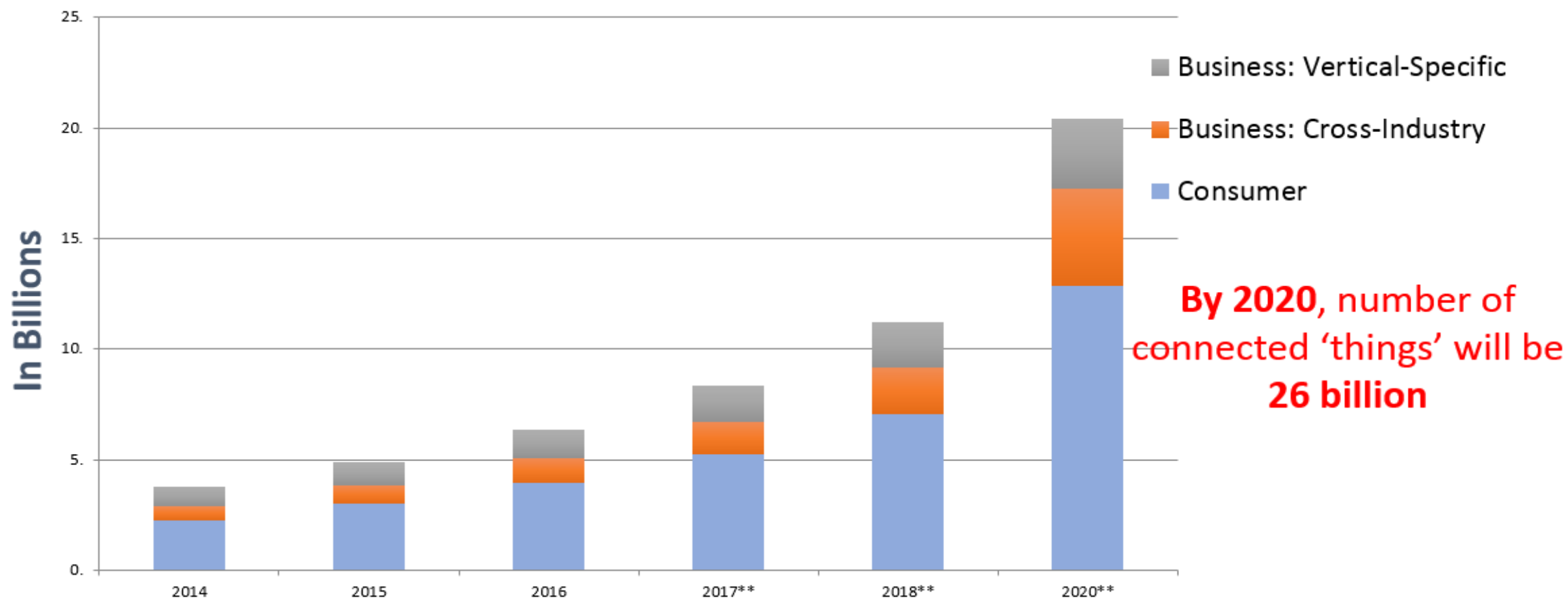
Cybersecurity Technology Seminar SMART Transportation

Presented by:
Michael Cochrane
Moxa Americas
May 2019

Agenda

- 1 Cybersecurity Trends & Overview**
- 2 Global Cybersecurity Standards**
- 3 IEC 62443 - Industrial Cybersecurity Overview**
- 4 Industrial Cybersecurity Best Practices and Solutions**

Connected IoT Devices by category 2014-2020



Source: Gartner



Cybersecurity Hack Attack! How Secure is Your Traffic Network?

Ready or Not, Here it Comes!!

- Connected & Autonomous Vehicles rapidly advancing the recognition of the need for more comprehensive CyberSecurity
- Smart Cities? Smart Regions!
- Coherent Framework, Strategic Transportation Technology Plan for County-wide smart region
- 5 Recommended implementation strategies
 - *Improve overall regional communications infrastructure*
 - *“Develop comprehensive cybersecurity management plan to ensure trusted communications and protect vehicles and roadside equipment against potential cyber-security attacks”*

Autonomous Vehicle

INTERNATIONAL

April 2019

“In 2015, while a Jeep was driving down the highway, its windshield wipers, infotainment system, air conditioning, and even the brakes began to operate by themselves – ultimately sending it into a ditch!”

“Thankfully, it was a controlled experiment where cybersecurity researchers were demonstrating the worrying vulnerabilities that hackers could exploit in today's vehicles”

“The result prompted Fiat Chrysler to patch over 1.4 million cars with an update to stop this weakness from being exposed again, but it did little to quell fears that as cars introduce more technologies, they present more opportunities for nefarious cyber bandits”

Industrial Cybersecurity

- What impact in ITS

1. **“Nobody wants to attack us.”** Other sectors are more likely targets for cyber-incidents than transportation, it won’t happen in transportation.
2. **“It can’t happen to us”.** Our systems are “air gapped” or “firewalled”.
3. **“It’s all about IT”.** Most of the cybersecurity investment will be in technology.
4. **“It’s possible to eliminate all vulnerabilities in systems”.** Cybersecurity incidents can be completely prevented

- **11%** of incidents reported to ICS-CERT (Industrial Control Systems) in 2012 were in Transportation Sector

Some incidents may not have been recognized as “hacking” and so are not thought of as a cybersecurity issue. In 2006 a disgruntled employee hacked into a traffic control computer in Los Angeles and shut down signals at key points causing delays for four days. Equipment

ing and they plan to profit from it. Transportation
Smart parking meters were first hacked in 2009. T

2011 BART website assault by the hacker advocacy group “Anonymous” t
company’s temporary shutdown of underground cell phone service. De

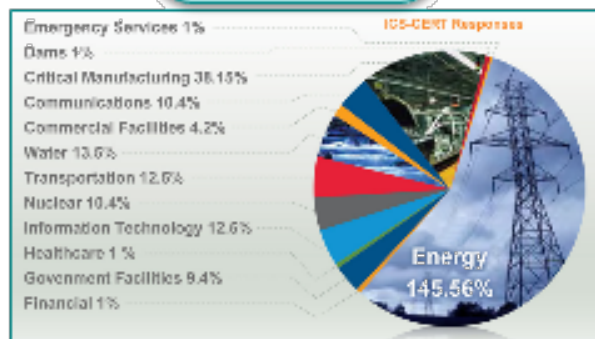
The increasing dependence on connected systems and networks with inherent vulnerabilities **Will**

- Expand Opportunities for cyber incidents (positive train control, ITS, V2V, V2I, V2X)
- Present unique challenges with regard to connectivity of safety-critical control systems in ATMS (Advanced Traffic Management Systems)

Industrial Cybersecurity

- Increasing Security Incidents

2013
257

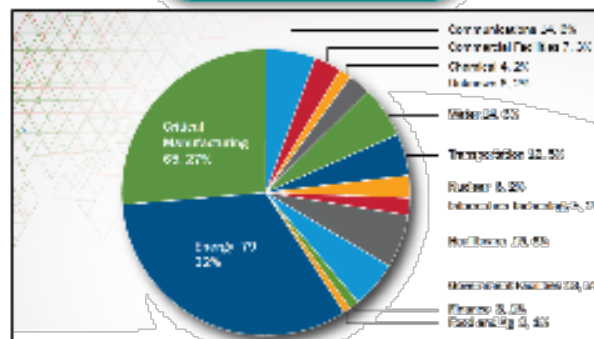


2013-2014

Energy Sector ↓ 46%

Critical Manufacturing ↑ 71%

2014
245



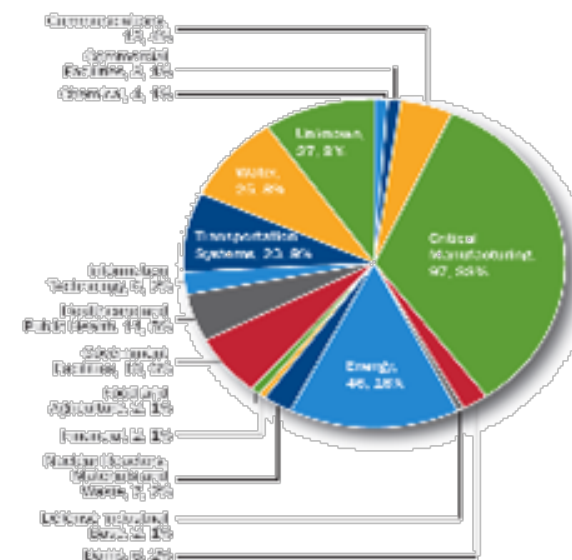
2014-2015

Energy Sector ↓ 42%

Critical Manufacturing ↑ 49%

New: Water, Transportation ↑ 50%

2015
295

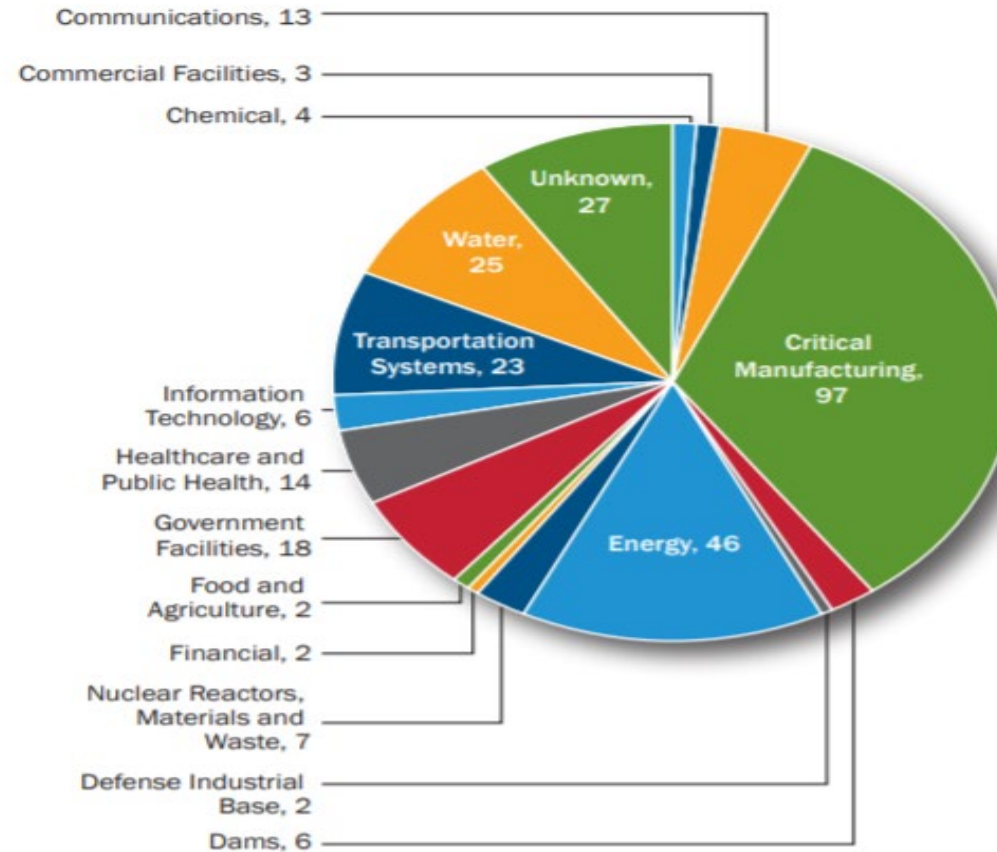


Source: ICS-CERT 2015 Report

Increasing Security Incidents

Incident Response FY 2015 Metrics

FY 2015 Incidents by Sector (295 total)



Industrial Cybersecurity

- The Trend in Recent Attacks

New Ransomware

Will Continue Wreaking Havoc On Industrial Organizations

- In 2017, global ransomware outbreaks such as



- Widespread disruptions among organizations in all industries, from Energy, Manufacturing, to Transportation and Healthcare
- Expect this trend to continue in 2019.

Industrial Cybersecurity

Ransomware



Date	12 May 2017 – 15 May 2017 (initial outbreak) ^[1]
Duration	4 days
Location	Worldwide
Also known as	Transformations: Wanna → Wana Cryptor → Crypt0r Cryptor → Decryptor Cryptor → Crypt → Cry Addition of "2.0" Short names: Wanna → WN → W Cry → CRY
Type	Cyberattack
Theme	Ransomware encrypting files with \$300 – \$600 demand (via bitcoin)
Cause	WannaCry worm
Outcome	Over 200,000 victims and more than 300,000 computers infected ^{[2][3][4]}

Put a firewall in your ICS against Ransomware!

The vulnerability the attackers are exploiting is in the SMB component in Windows. Server Message Block (SMB) is a network protocol that provides file and printer sharing services in Windows systems. SMB may be used inside the corporate network for sharing files and printers; however, it should *never* be allowed beyond the corporate network.

This is so strongly recommended, in fact, that an advisory posted in January 2017 by the United States Computer Emergency Readiness Team (US-CERT) recommends blocking “all versions of Server Message Block (SMB) at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.” This measure prevents the WannaCry attack and should be implemented on business and home firewalls.

Reference: US-CERT Advisory, <https://www.us-cert.gov/security-publications/Ransomware>



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Cybersecurity Standards – What is IEEE 1609? Is it Enough?

IEEE 1609.2-2016 (Revision of IEEE Std 1609.2-2013)

- A Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages

ITS Security Architecture

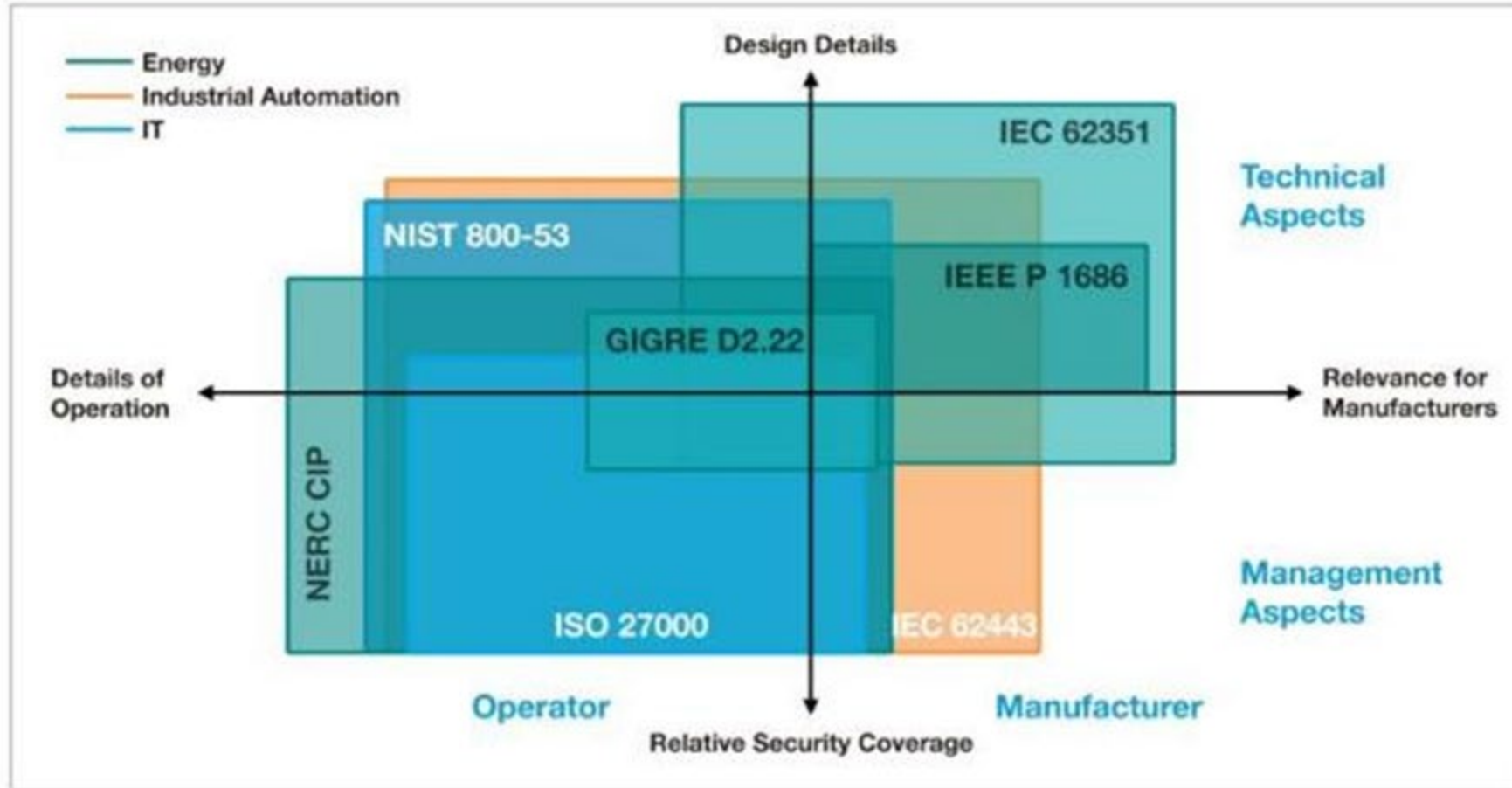
The security features of ITS, both **WAVE** and ETSI standards have defined the security architecture.

- The main security components, including the security headers, certificate format and security profiles.
- Based on a slightly modified IEEE 802.11p at the access layer, and enables new networking features based on geographical addressing at the network layer, and new facilities layer on top that enables a set of rich messages that support different types of applications.

Table 1. Security attacks, compromised security requirements and countermeasures.

Security Attack	Compromised Security Requirement	Countermeasure
Denial of Service (DoS)	Availability	Digital Signature
Jamming, Flooding	Availability	Digital Signature
Sybil	Availability, Authentication	Digital Signature
Malware, Spamming, Black hole, Grey hole, Sink hole, Warm hole	Availability, Authentication	Digital Signature
Eavesdropping	Confidentiality	Encryption
Data Interception	Confidentiality	Encryption
Falsified Entities	Authentication, Authorization	Digital Signature and Encryption
Cryptographic Replication	Authentication, Authorization	Digital Signature and Encryption
GNSS Spoofing	Authentication, Authorization	Digital Signature and Encryption
Timing	Authentication, Authorization	Digital Signature and Encryption
Masquerading	Data Integrity	Digital Signature with Certificate
Data Playback	Data Integrity	Digital Signature with Certificate
Data Alteration	Data Integrity	Digital Signature with Certificate

Cybersecurity Standards



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



General Industrial Automation:
ISA 99 / IEC 62443

Cybersecurity Standards: What Is IEC-62443?

Introduction

The 62443 series of standards have been developed jointly by the ISA99 committee and IEC Technical Committee 65 Working Group 10 (TC65WG10) **to address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS).**

Series Goal

The goal in applying the 62443 series is to **improve the safety, availability, integrity and confidentiality of components or systems** used for industrial automation and control, and **to provide criteria for procuring and implementing** secure industrial automation and control systems.

The Content

of the series is directed towards those responsible for designing, implementing, or managing industrial automation and control systems. This information also applies to users, system integrators, security practitioners, and control systems manufacturers and vendors.

What Is IEC-62443 - Continued

Approach

The 62443 series builds on established standards (e.g., the ISO/IEC 27000 series), to specifically identify and address the important differences present in Industrial Automation and Control Systems (IACS).

Many of these differences are based on the reality that cyber security risks with IACS may have Health, Safety or Environment (HSE) implications and the response should be integrated with other existing risk management practices addressing these risks.

All ISA-62443 standards and technical reports are organized into four general categories called *General, Policies and Procedures, System, and Component*

IEC-62443 Industrial Automation and Control Systems Security

Organization

The elements of the 62443 series are shown in Figure 1.

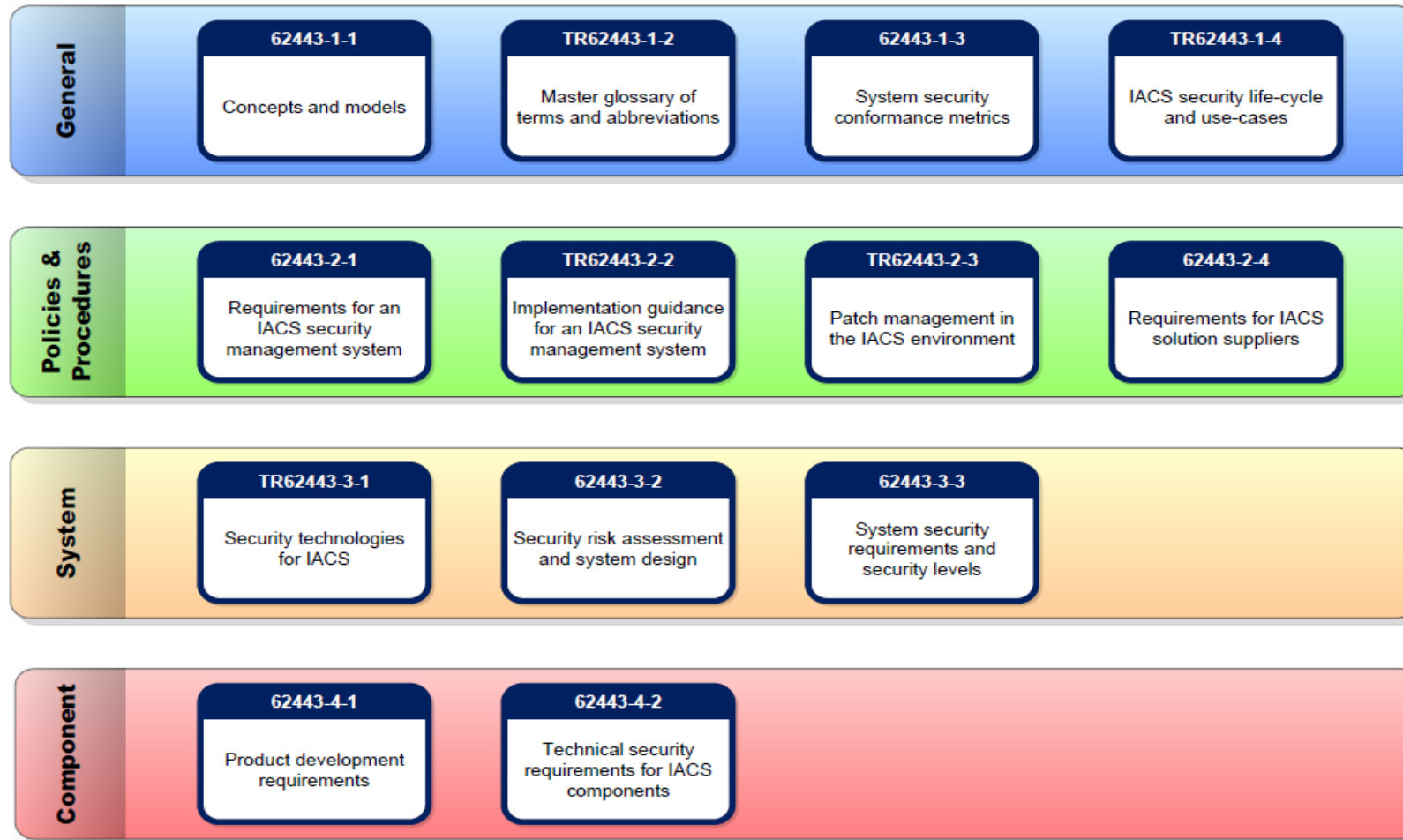


Figure 1 – 62443 Elements

The 7 Foundational Requirements

Functional Requirements: IEC-62443-4-2

Functional Requirement	Description
FR1	Identification and Authentication Control
FR2	Use Control
FR3	Data Integrity
FR4	Data confidentiality
FR5	Restrict Data Flow
FR6	Timely Response to Event
FR7	Network Resource Availability



Cybersecurity: Network Product Portfolio

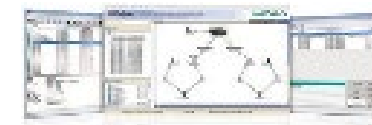
**Enhance Edge Devices
security features for
IEC 62443-4-2**



**Enhance Network Devices
Security features for
IEC 62443-4-2**



**Develop Cybersecurity
Management NMS for
IEC 62443-2-1**



**Enhance Secure Routers
Cybersecurity features for
IEC 62443-3-2/-3-3**



**IIoT Gateway
Enhance Secure Remote
Connect**



Industrial Cybersecurity Best Practice

- Stage 1 – End Devices Security

1. Entry

- To protect specific assets
- Wants simple solutions



2. Engaged

- Starting to take a systemic approach
- Looking for guidance/best practices



3. Advanced

- Policy established (often by IT)
- Looking for IT like solutions



End Device Security - Common Challenges

These are common challenges faced when having to secure an industrial network.

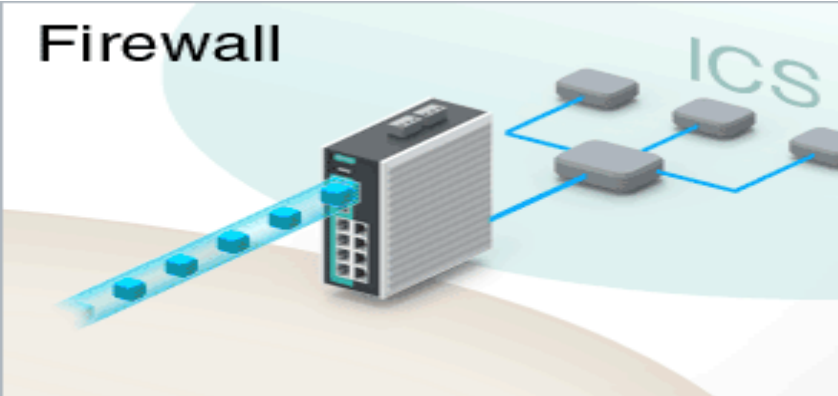
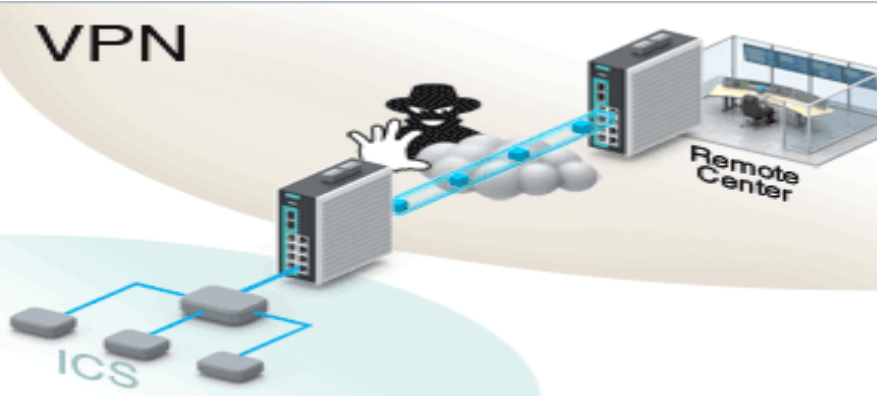
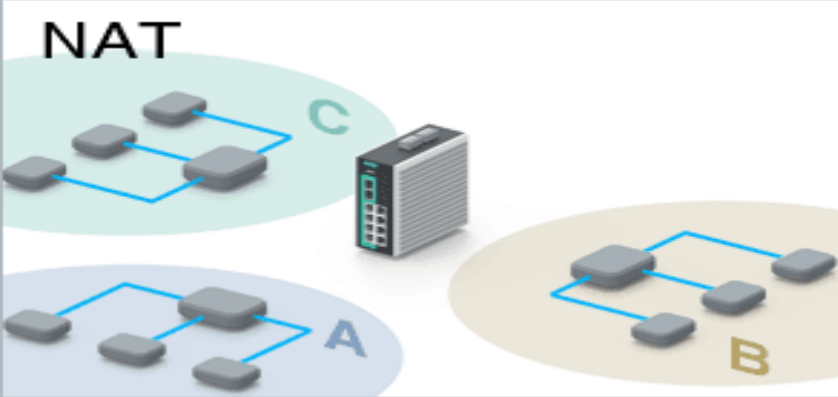
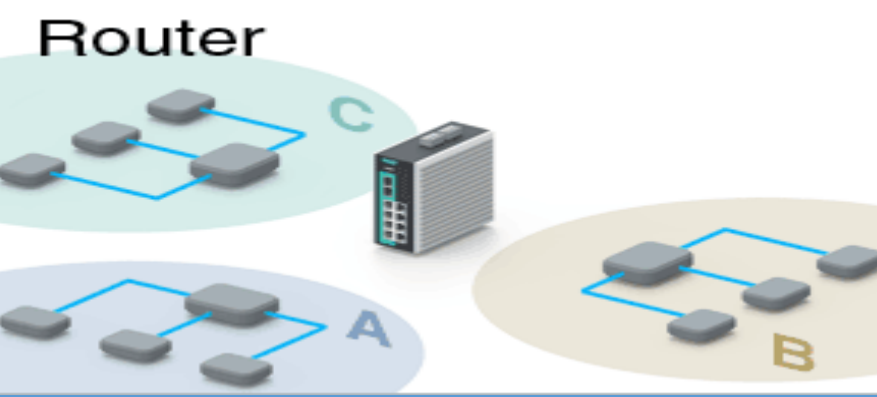
- Securing existing systems
 - To secure previously unsecured networks?
 - To prevent unauthorized use inside of the facility?
- Providing secure remote access
 - To provide a secure way to connect to a remote network?
 - To ensure data transmission is not modified in transit?
 - To protect my confidential information?



Industrial End Devices Security

Industrial Secure Router Solutions

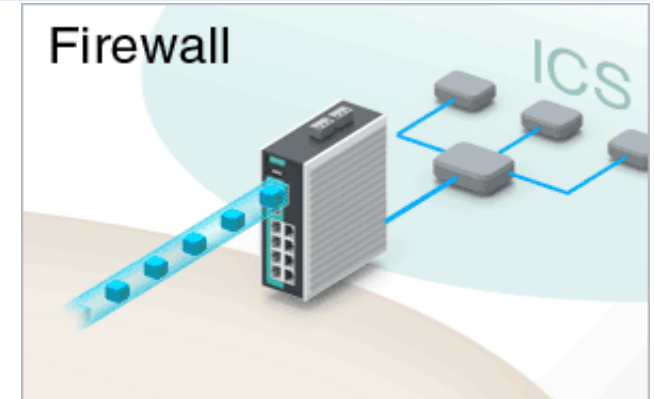
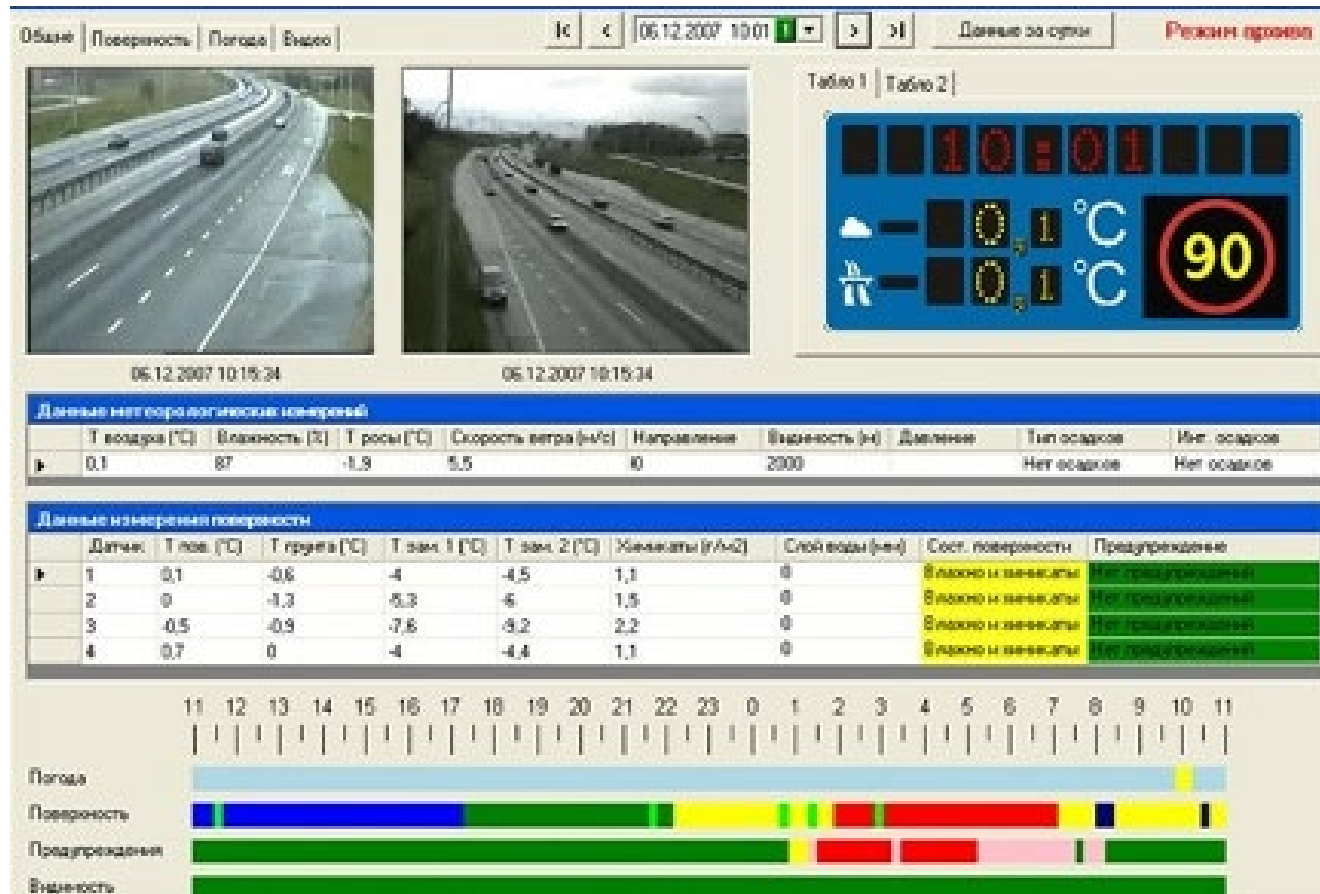
Firewall / VPN / NAT / Router & Layer 2 & 3 Managed Switches

Filtering unauthorized traffic	Providing encrypted network tunnel
Firewall 	VPN 
NAT 	Router 
Remapping one IP address into another	Routing unicast or multicast traffic among subnets



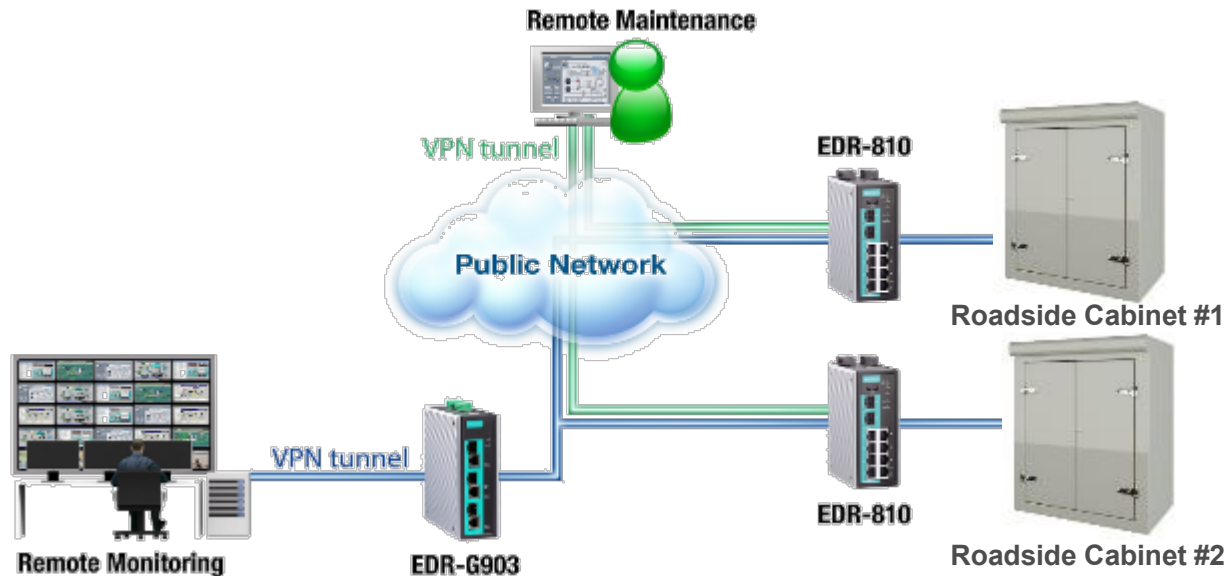
Securing Interconnected Traffic Signal Communications via Public Network

Filtering unauthorized traffic

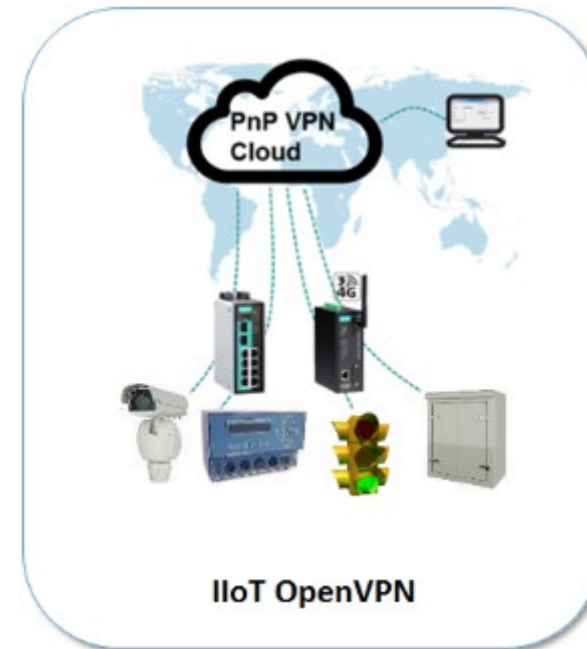
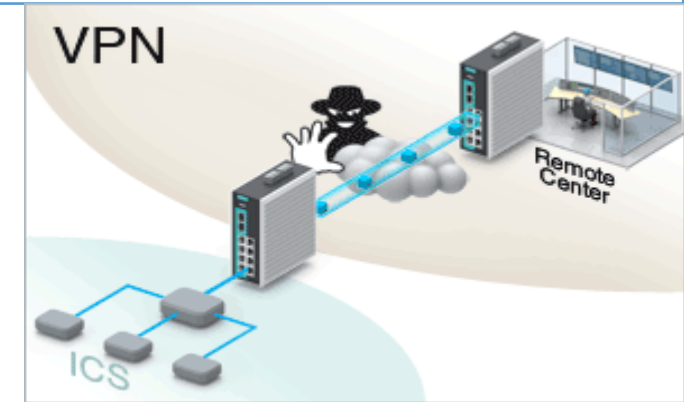


Secure VPN Tunnel with Public Network

- Secure VPN tunnel between two sites LAN to LAN
 - IPSec site-to-site VPN
- Secure VPN tunnel for Remote User Access
 - L2TP (Layer 2 Tunnel Protocol)
 - OpenVPN

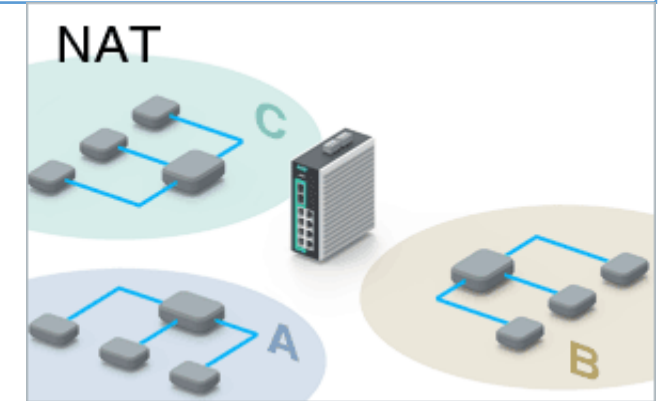
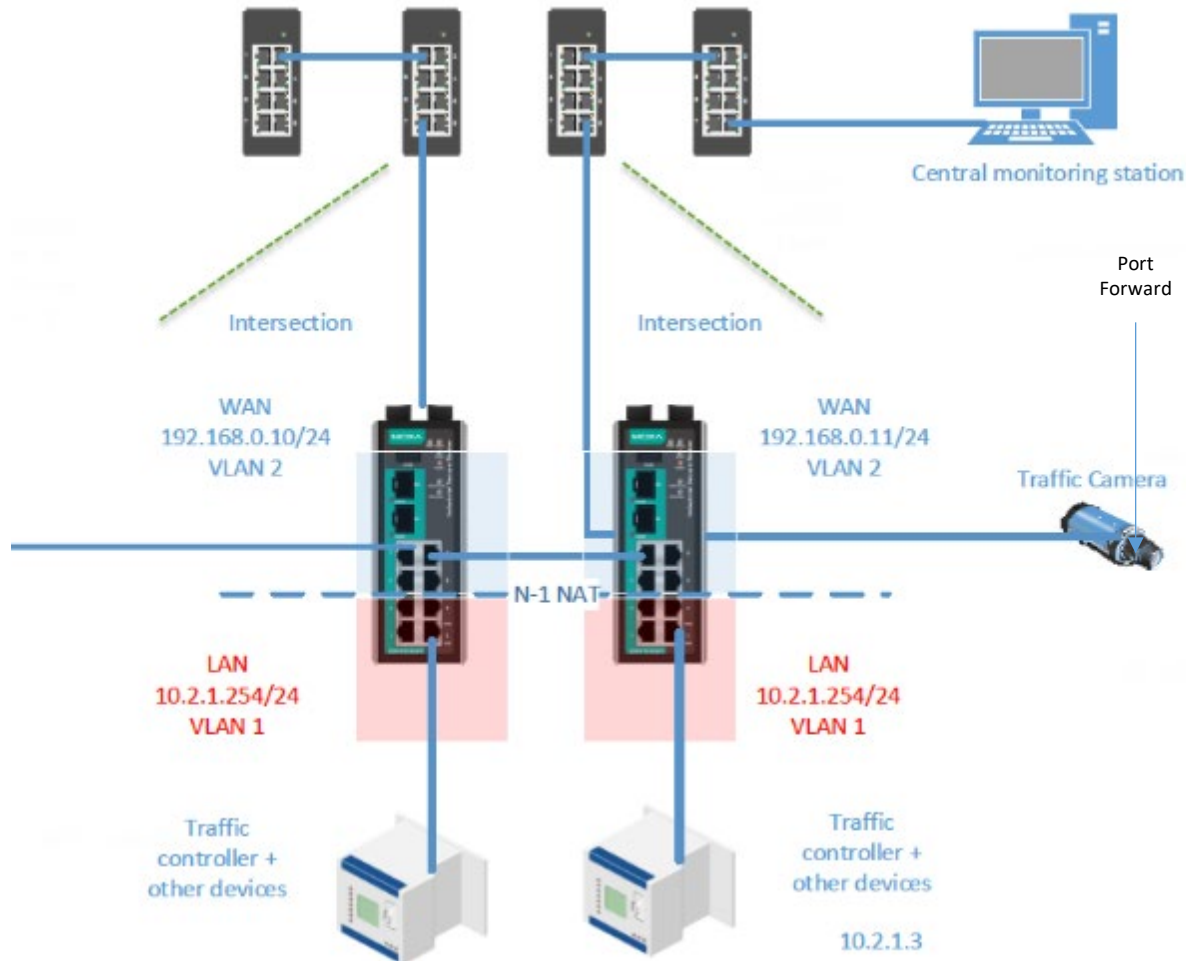


Providing encrypted network tunnel



NAT Benefit in ITS Network

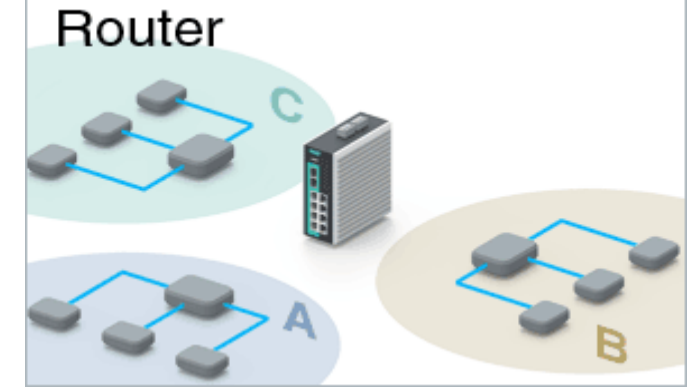
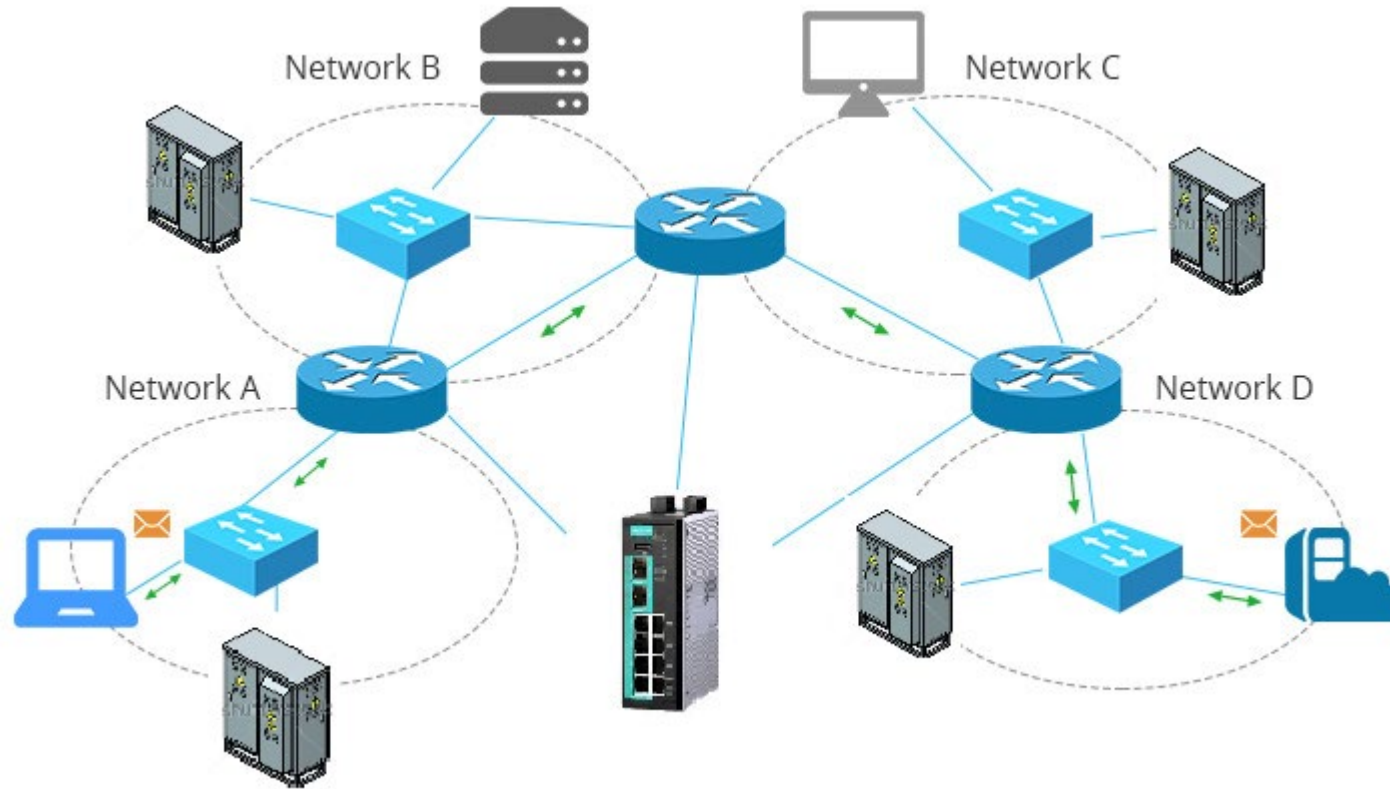
Remapping one IP address into another



- Each Cell/Zone can use the same IP addressing Scheme
- N-1 NAT allows same IP scheme at each intersection
- Port forwarding allows the traffic controllers and Serial to Ethernet devices to be accessed from traffic management center
- Flexible number of WAN/LAN ports
 - Support more devices
 - Support traffic Camera Application

Subnet Management

Routing unicast or multicast traffic among subnets



Industrial Cybersecurity Best Practice

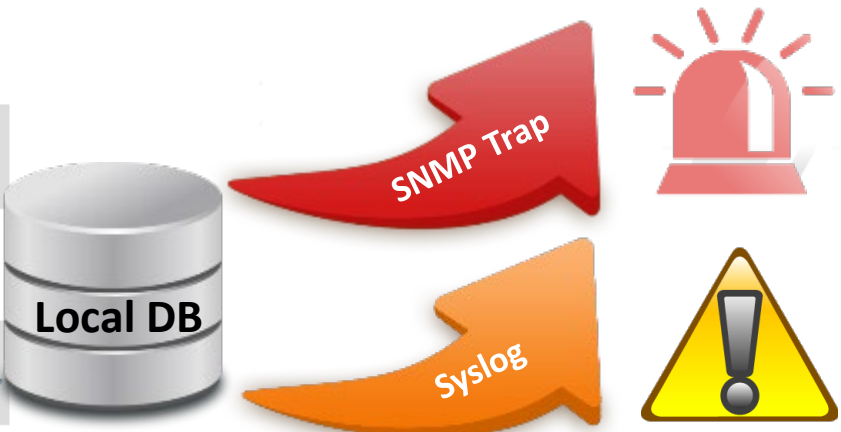
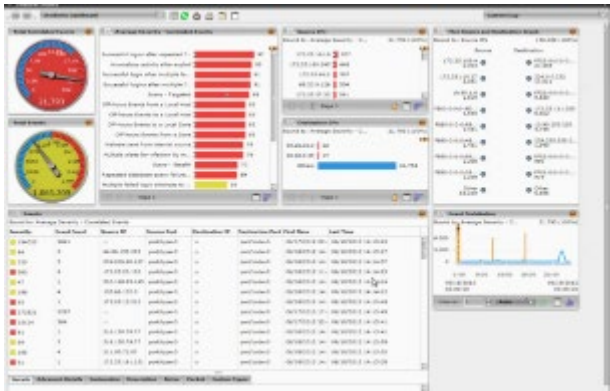
- Stage 1 – End Devices Security

Real-time event alarm made security management easier!

Event Log Table

All <=> <7> Debug Page 1/4

Index	Date	Time	Functions	Severity	Event
1	2015/02/04	13:36:51	Firewall	<0> Emergency	[TCP-Without-SYN Scan] DROP PROTO=TCP, SRC_IP=192.168.126.1, SRC_PORT=15591, IN=BRG, DST_IP=192.168.28.231, DST_PORT=14963, OUT=WAN
2	2015/02/04	13:36:47	Firewall	<0> Emergency	[R3] ACCEPT PROTO=UDP, SRC_IP=192.168.126.1, SRC_PORT=52231, IN=BRG, DST_IP=157.56.106.184, DST_PORT=3544, OUT=WAN
3	2015/02/04	13:36:47	Firewall	<0> Emergency	[TCP-Without-SYN Scan] DROP PROTO=TCP, SRC_IP=192.168.127.2, SRC_PORT=1482, IN=LAN, DST_IP=217.146.26.210, DST_PORT=443, OUT=WAN
4	2015/02/04	13:36:47	Firewall	<0> Emergency	[TCP-Without-SYN Scan] DROP PROTO=TCP, SRC_IP=192.168.127.2, SRC_PORT=5900, IN=LAN, DST_IP=192.168.126.1, DST_PORT=36796, OUT=BRG
5	2015/02/04	13:36:47	Firewall	<0> Emergency	[TCP-Without-SYN Scan] DROP PROTO=TCP, SRC_IP=192.168.126.1, SRC_PORT=15591, IN=BRG, DST_IP=192.168.28.231, DST_PORT=14963, OUT=WAN has repeated 1 times in past 10 seconds



Industrial Cybersecurity Best Practice

- Stage 2 – Engaged Security

1. Entry

- Looking to protect specific assets
- Wants simple solutions



2. Engaged

- Starting to take a systemic approach
- Looking for guidance/best practices



3. Advanced

- Policy established (often by IT)
- Looking for IT like solutions



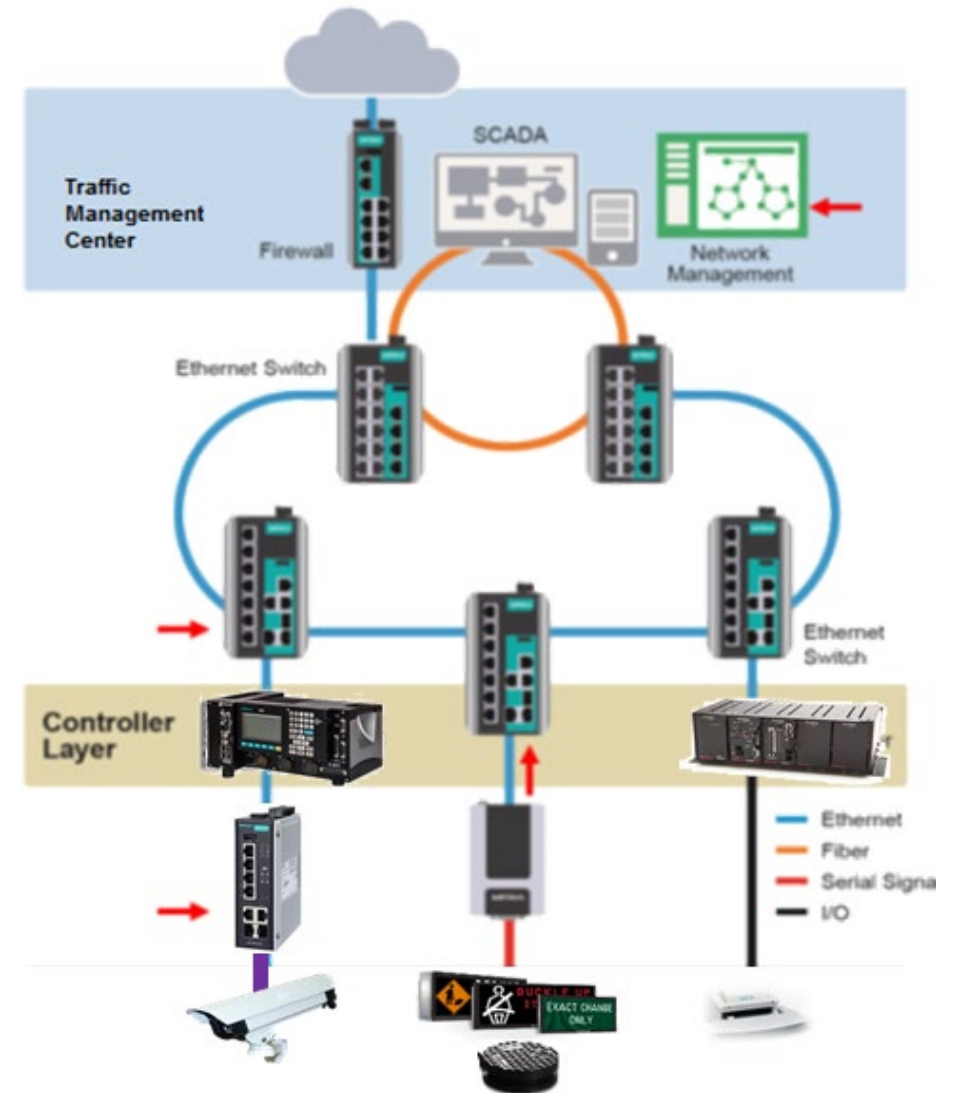
Industrial Cybersecurity Best Practice

- Stage 2 – Engaged Security

To Ramp Up

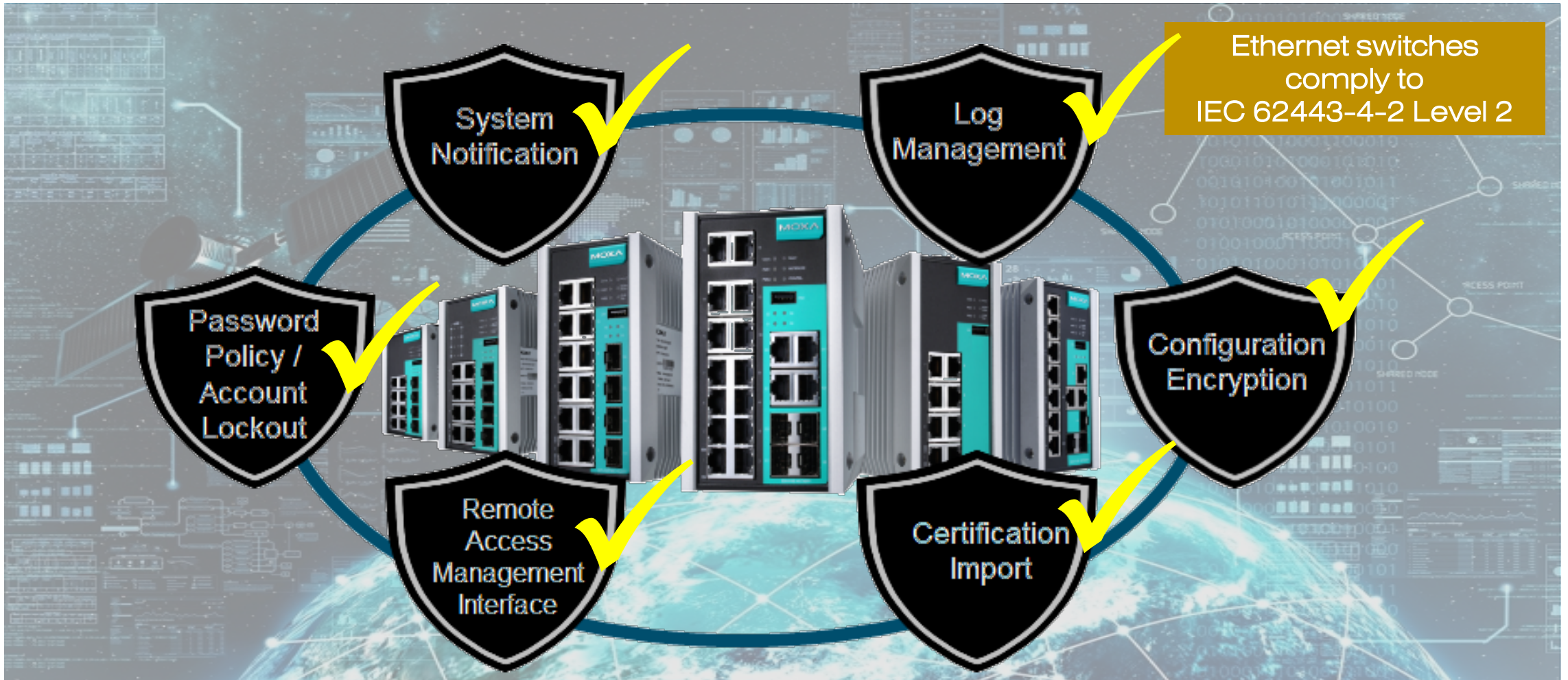
Roadside Cabinet Network Security

- Prevent Intrusions and Attacks
- Protect Sensitive Data
- Ability to Audit Security Events
- Visualize the Security Status of the Network
- Correct Configuration



Industrial Cybersecurity Best Practice

- Stage 2 – Engaged Security



Industrial Cybersecurity Best Practice

- Stage 2 – Engaged Security

Setup Different User Account Levels
Remote Access Interface Management

User Account

Active ☒

Authority

User Name

Password

Confirm Password

Account List

Active	User Name	Authority
<input checked="" type="checkbox"/>	admin	admin
<input checked="" type="checkbox"/>	user	user

Management Interface

☐ Enable HTTP TCP Port

☒ Enable HTTPS TCP Port

☐ Enable Telnet TCP Port

☒ Enable SSH TCP Port

☒ Enable SNMP TCP Port

☐ Enable Moxa Service TCP Port UDP Port

☒ Enable Moxa Service(Encrypted) TCP Port UDP Port

Maximum Login Users For HTTP+HTTPS (1~10)

Maximum Login Users For Telnet+SSH (1~5)

Auto Logout Setting (min) (0~1440; 0 for Disable)

Industrial Cybersecurity Best Practice

- Stage 2 – Engaged Security

Password Policy & Strength Options

Trusted Access for Authorized Devices

Account Password and Login Management

Account Password Policy

Minimum Length
(4~16)

- ☒ Enable password complexity strength check
 - ☐ At least one digit (0~9)
 - ☒ Mixed upper and lower case letters (A~Z, a~z)
 - ☐ At least one special character (~!@#\$\$%^&*-_!;:.,<>[]{}())

Account Login Failure Lockout

☒ Enable

Retry Failure Threshold
(1~10)

Lockout Time (min)
(1~60)

Trusted Access

☒ Enable trusted access

Please add your local IP address first, otherwise, your PC will not be able to connect the device again

<input type="checkbox"/> All	IP Address	Subnet Mask
<input checked="" type="checkbox"/>	192.168.127.10	24(255.255.255.0) ▼
<input type="checkbox"/>	<input type="text"/>	0(0.0.0.0) ▼
<input type="checkbox"/>	<input type="text"/>	0(0.0.0.0) ▼
<input type="checkbox"/>	<input type="text"/>	0(0.0.0.0) ▼
<input type="checkbox"/>	<input type="text"/>	0(0.0.0.0) ▼
<input type="checkbox"/>	<input type="text"/>	0(0.0.0.0) ▼
<input type="checkbox"/>	<input type="text"/>	0(0.0.0.0) ▼
<input type="checkbox"/>	<input type="text"/>	0(0.0.0.0) ▼
<input type="checkbox"/>	<input type="text"/>	0(0.0.0.0) ▼

Industrial Cybersecurity Best Practice

- Stage 2 – Engaged Security

Configuration File Encryption
SNMP Trap and Syslog for Remote Server

Configuration Backup and Restore

☒ Local ☐ TFTP Server ☐ Auto Backup Configurator (ABC-02)

Backup Configuration File to Local Computer Backup

Restore Configuration From Browse Restore

Configuration File Encryption Setting

☒ Enable Password Apply

☒ Auto load configuration from ABC-02 to system when boot up

☐ Auto backup to ABC-02 when configuration change Apply

SNMP

SNMP Versions

Admin Auth. Type

☒ Enable Admin Data Encryption Data Encryption Key

User Auth. Type

☒ Enable User Data Encryption Data Encryption Key

Community

V1,V2c Read Community

V1,V2c Write/Read Community

Trap/Inform Recipient

Mode

Host IP Address 1

1st Trap Community

Host IP Address 2

2nd Trap Community

Syslog Settings

Syslog 1 ☒

Server

UDP Port (1~65535)

Syslog 2 ☐

Server

UDP Port (1~65535)

Syslog 3 ☐

Server

UDP Port (1~65535)

Industrial Cybersecurity Best Practice

- Stage 3 – Advanced Security

1. Entry

- Looking to protect specific assets
- Wants simple solutions



2. Engaged

- Starting to take a systemic approach
- Looking for guidance/best practices

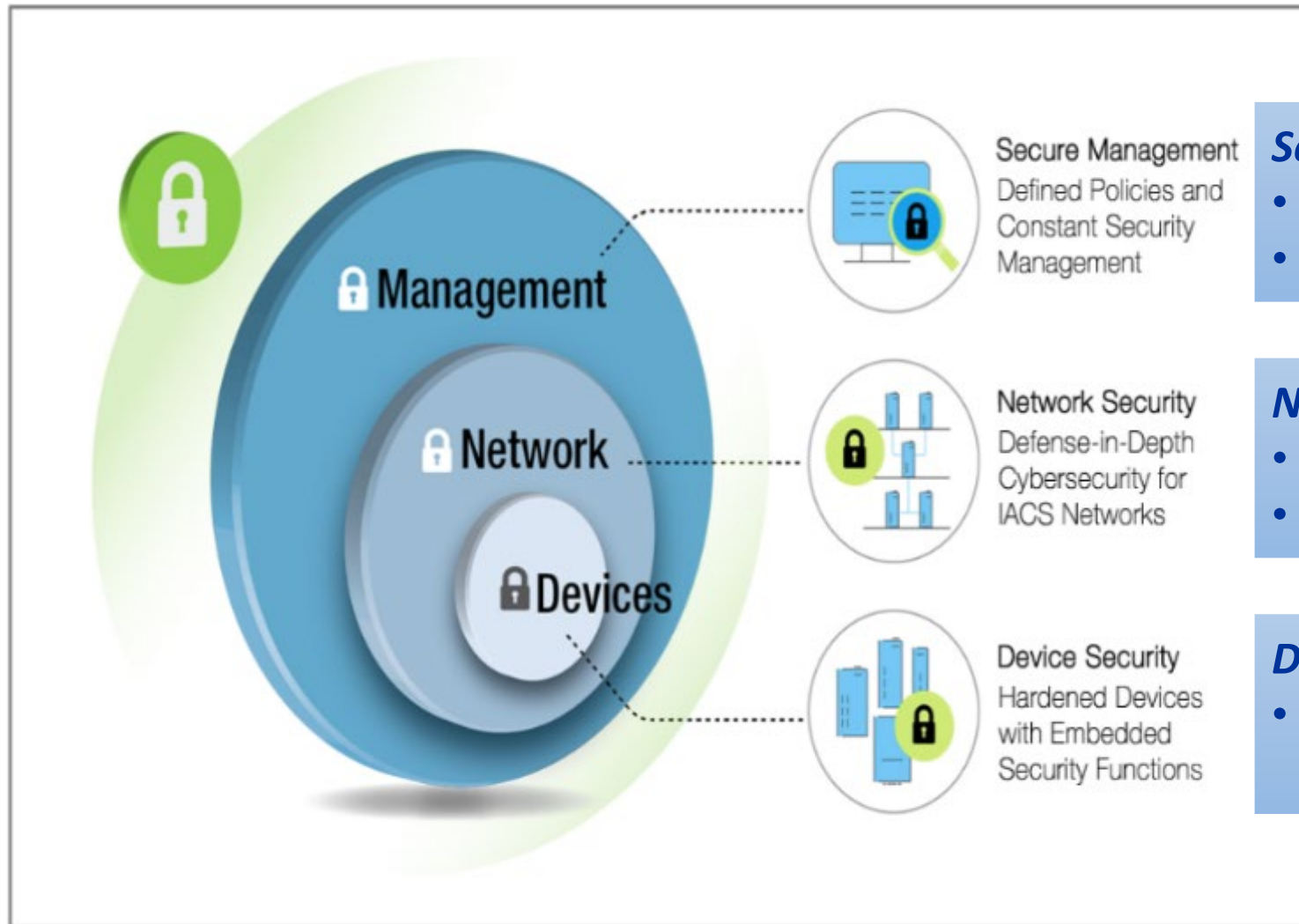


3. Advanced

- Policy established (often by IT)
- Looking for IT like solutions



Industrial Network Cybersecurity - Management



Security Management

- Security View
- Security Wizard

Network Security

- Industrial Firewall / VPN
- Secure Remote Connect

Device Security

- Reinforced features based on IEC 62443 requirements

Industrial Cybersecurity Best Practice

- Stage 3 – Advanced Security

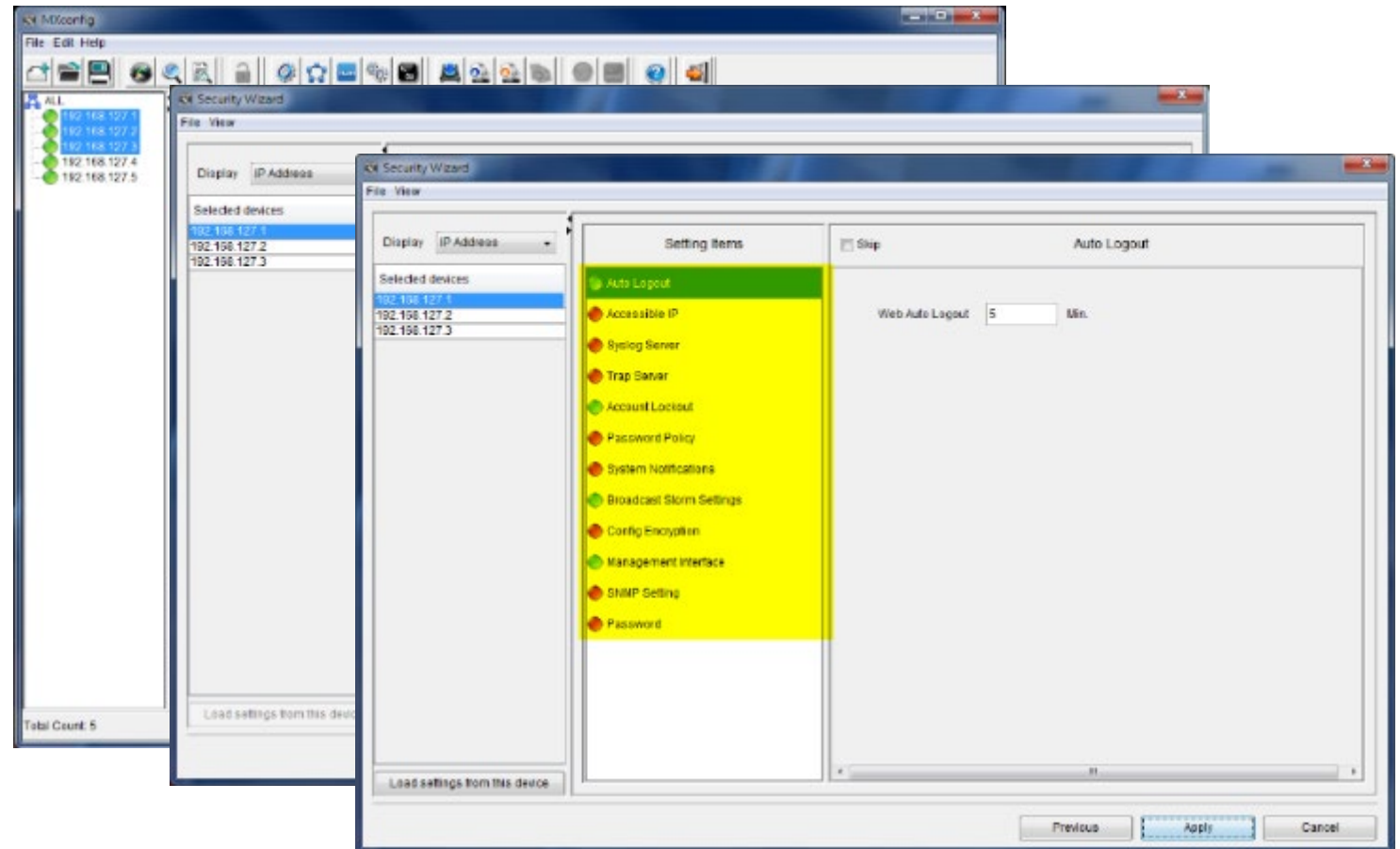
Check Items of Built-in Industrial Security Profiles

Security Level	High	Medium	Basic	Open	Unknown
Built-in Profiles	<i>IEC 62443-4-2 Level 2</i>	<i>IEC 62443-4-2 Level 1</i>	<i>General Baseline*</i>		
Check Items					
• Enable Auto Logout	Enabled	Enabled	Enabled	-	N/A
• Set Login Message	Set	Set	-	-	N/A
• Disable Non-encrypted TCP/UDP Ports	Disabled	Disabled	-	-	N/A
• Enable Account Login Failure Lockout	Enabled	Enabled	-	-	N/A
• Enable Trusted Access	Enabled	Enabled	Enabled	-	N/A
• Enable Password Complexity Strength Check	Enabled	Enabled	-	-	N/A
• Enable Configuration File Encryption	Enabled	-	-	-	N/A
• Enable Broadcast Storm Protection	Enabled	Enabled	-	-	N/A
• Set SNMP Trap/Inform or Syslog Server	Set	Set	Set	-	N/A
• Change Default Password / SNMP Community String	Changed	Changed	Changed	-	N/A

Industrial Cybersecurity Best Practice

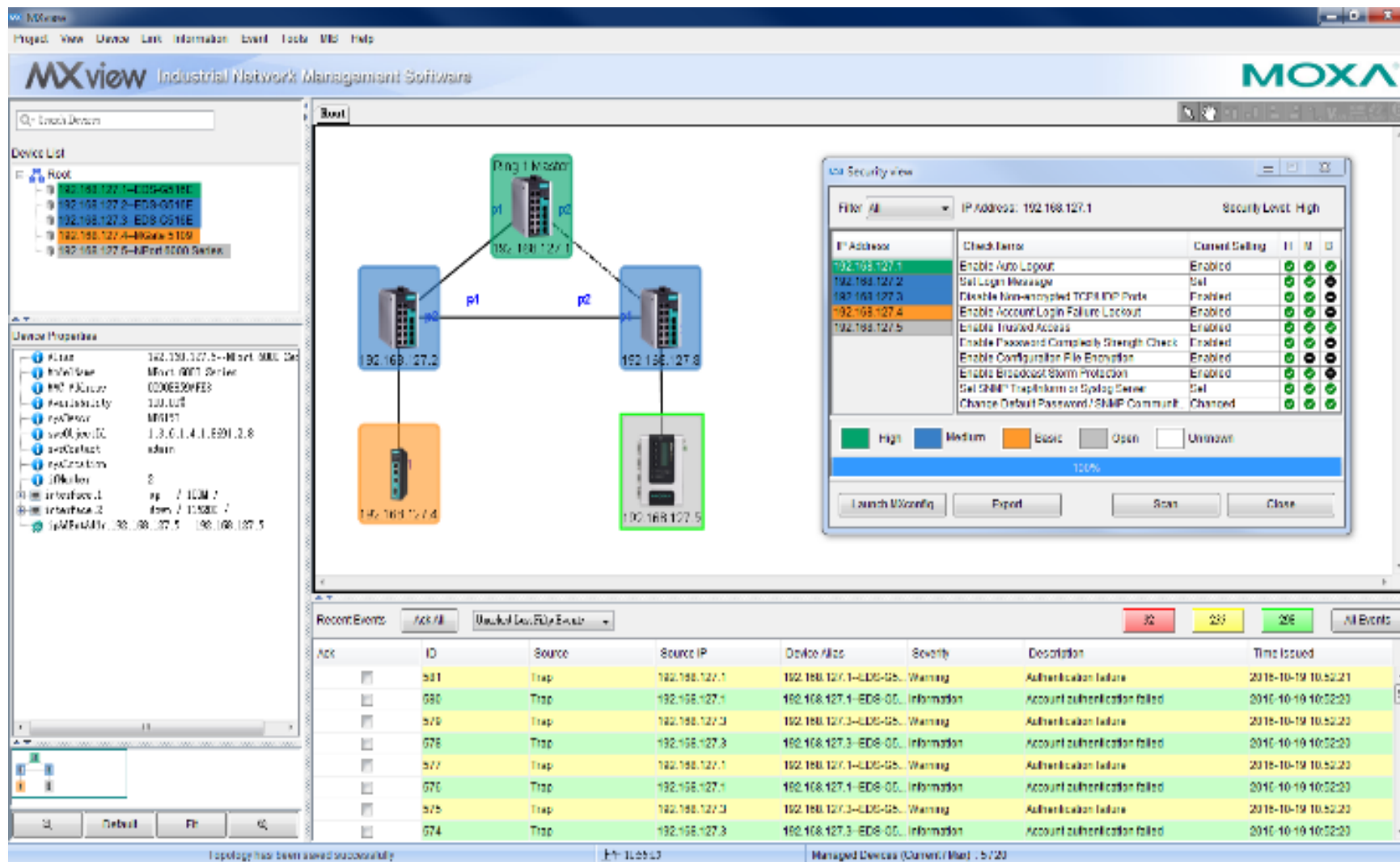
- Stage 3 – Advanced Security

Security Wizard



Industrial Cybersecurity Best Practice

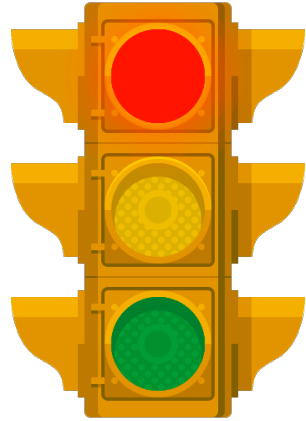
- Stage 3 – Advanced Security - Address Security & Get Visualization



Summary

Connected and Autonomous Vehicles means Increased Automation. Increased Automation means Increased Connectivity. Increased Connectivity means Increased Complexity. Plus Increased Hacker Sophistication = Increased RISK

- The Threat is Real. The Need for a Comprehensive Solution is Real.
- Implement an Infrastructure that Supports Industry Standards
- IEC-62443 Foundational Requirements Address CyberSecurity at the Vendor, Integrator, and Operator level.
- IEC-62443 can be implemented, managed, and viewed simply and efficiently
- There is no “Finish Line” But now there’s a solid foundation to build upon.....



**THANK
YOU!**