Moxa The Technology Communication Industrial Leader

Ing. Felipe Sabino Costa
Líder en Tecnología & Ciberseguridad Industrial Latín América

Presenters

Moxa Americas Inc.

Felipe Sabino Costa

Líder en Tecnología & Ciberseguridad Industrial Latín América

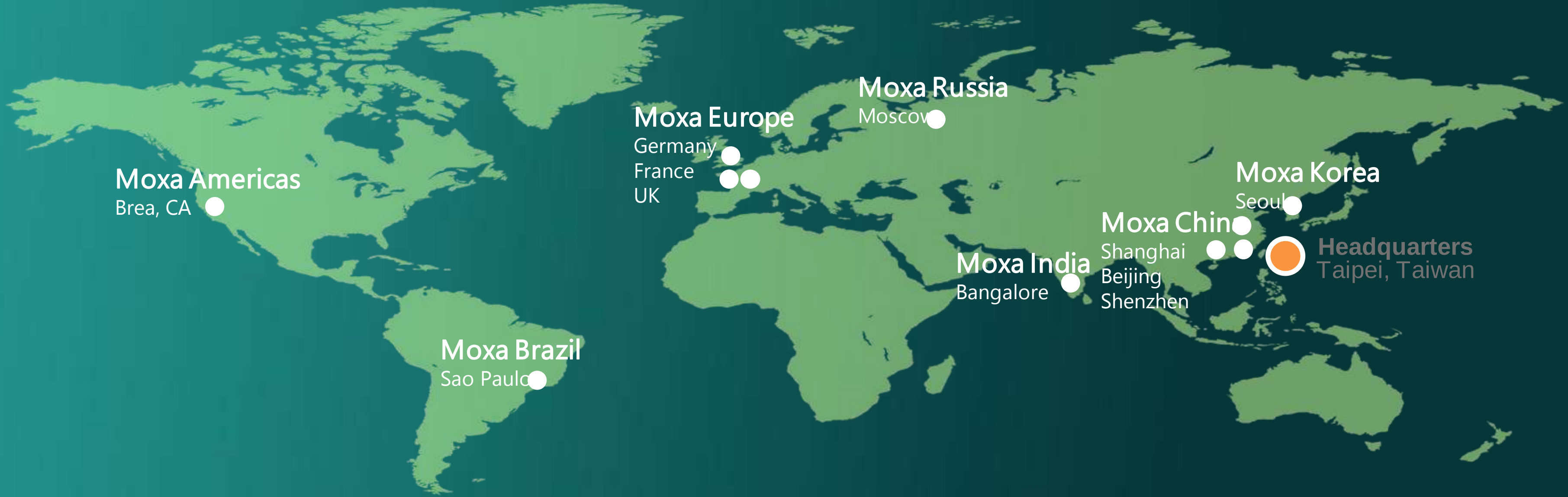
- **+ 15 years** of experience in Automation
- **+ 6 years** Network and Cybersecurity (Moxa, CCNA)
- **International** official I**SA/IEC-62443** ICS instructor
- Different certifications **(US-DHS, MIT, Stanford and currently on Master in ICS)**

MOXA®

CONNECTIVITY, SIMPLIFIED

ICCX & Moxa

Established **Global** Presence



12

Branches on Four Continents

120+

Distributors Worldwide

70+

Countries Covered by Our Dist. & Service Network

57M+

Devices Connected

FROM OUTER SPACE

The International Space Station (ISS)

TO THE OCEAN FLOOR

Ocean Power Generation in the UK

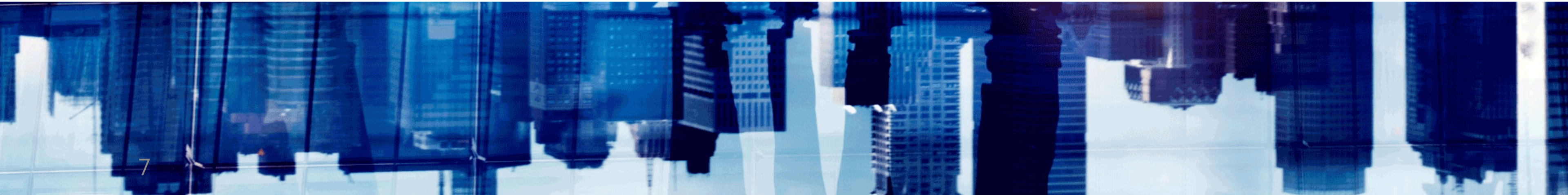
Enabling Connectivity for Mission-critical Industrial Applications

EN50155 IRIS Certification IEC 61850-3 NEMA TS2 DNV·GL Ex

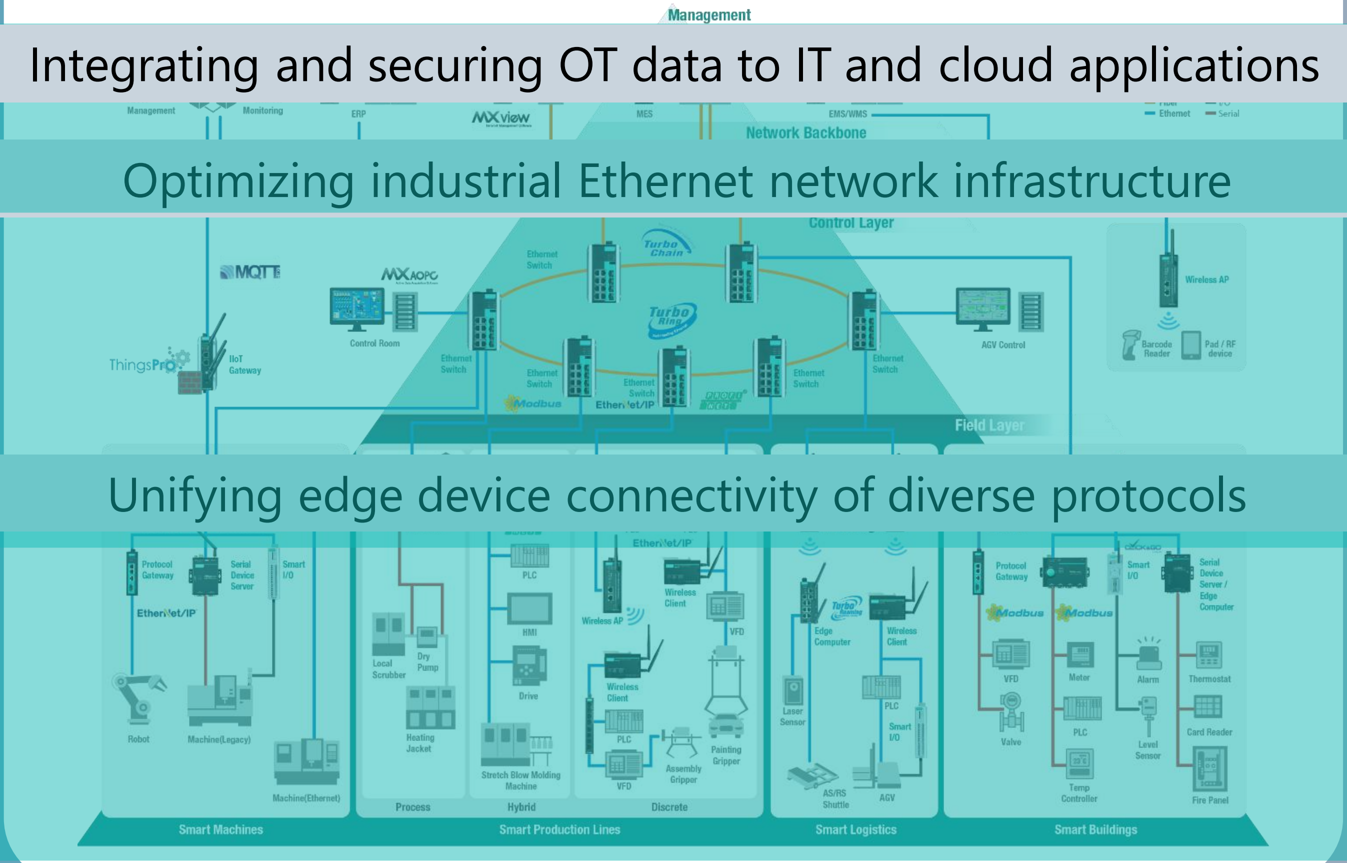
Microsoft Azure · aws · Alibaba Cloud · intel IoT Solutions Alliance · KPMG · TREND MICRO

Your Trusted Partner in Data Communication

IEC · industrial internet CONSORTIUM · Modbus MEMBER · OPC FOUNDATION · EtherCAT Technology Group · THE LINUX FOUNDATION · ODVA MEMBER



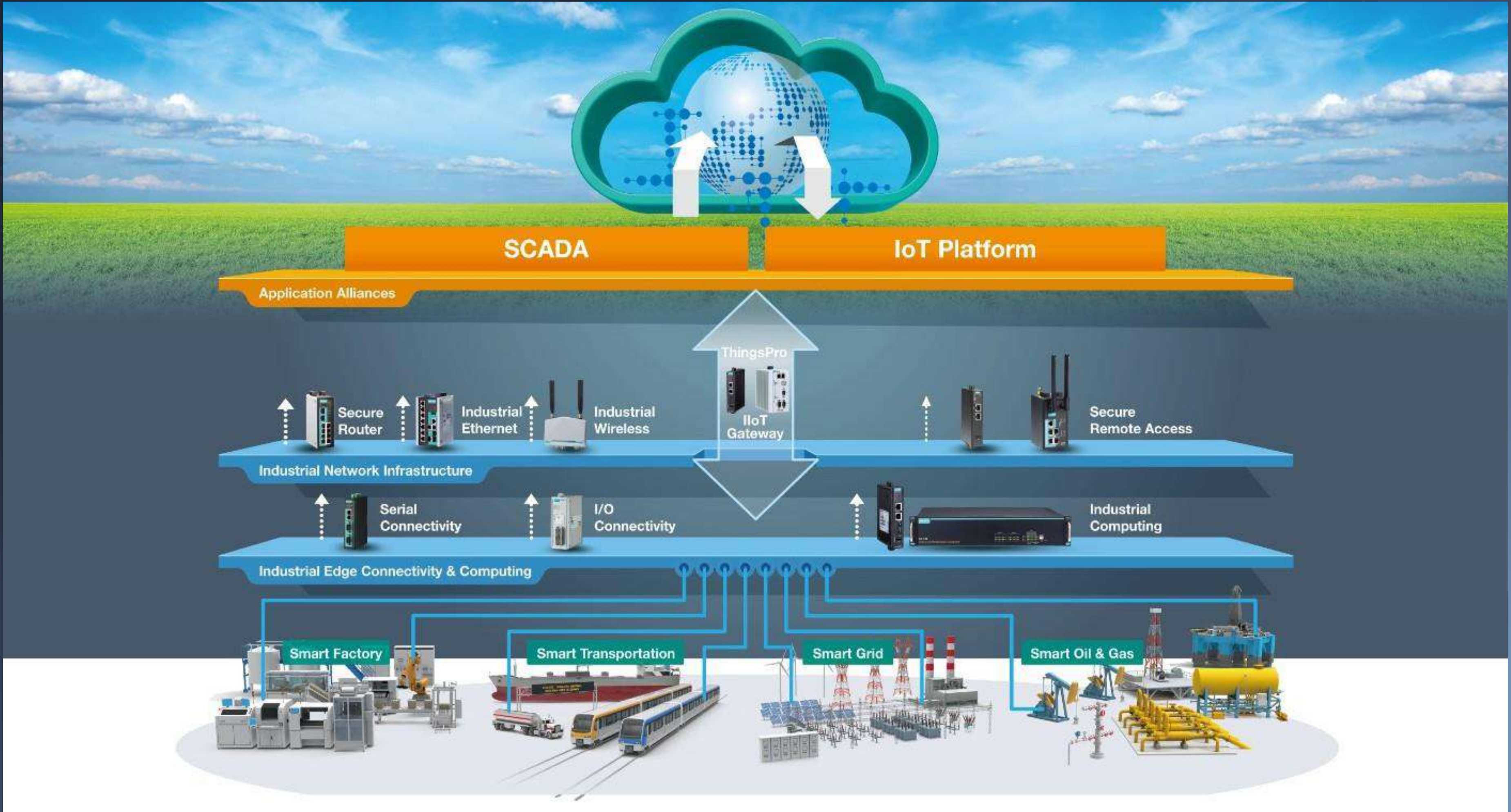
Simplifying Connectivity



Integrating and securing OT data to IT and cloud applications

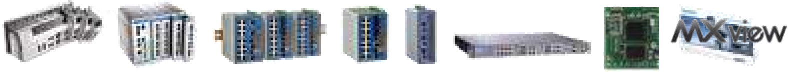
Optimizing industrial Ethernet network infrastructure

Unifying edge device connectivity of diverse protocols


SCADA
IoT Platform
Application Alliances
ThingsPro
Secure Router
Industrial Ethernet
Industrial Wireless
IIoT Gateway
Secure Remote Access
Industrial Network Infrastructure
Serial Connectivity
I/O Connectivity
Industrial Computing
Industrial Edge Connectivity & Computing
Smart Factory
Smart Transportation
Smart Grid
Smart Oil & Gas

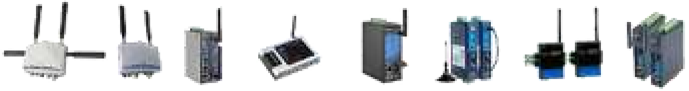
Overview

Industrial Ethernet Switches



Energy & Transportation

Cellular & Wireless



Disp. Serial, USB and Gateways

Industrial Computers

Panel PCs

Remote I/O & RTU

Defend Your Industrial Networks

MOXA®

Reliable Networks ▲ Sincere Service

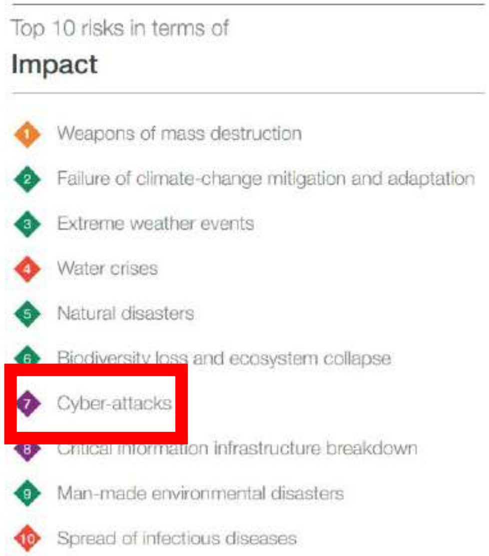
What makes a cybersecurity breach successful ?

What is the key factor to avoid?

Defense-in-Depth

3000 A.C. - Los Millares Espanha

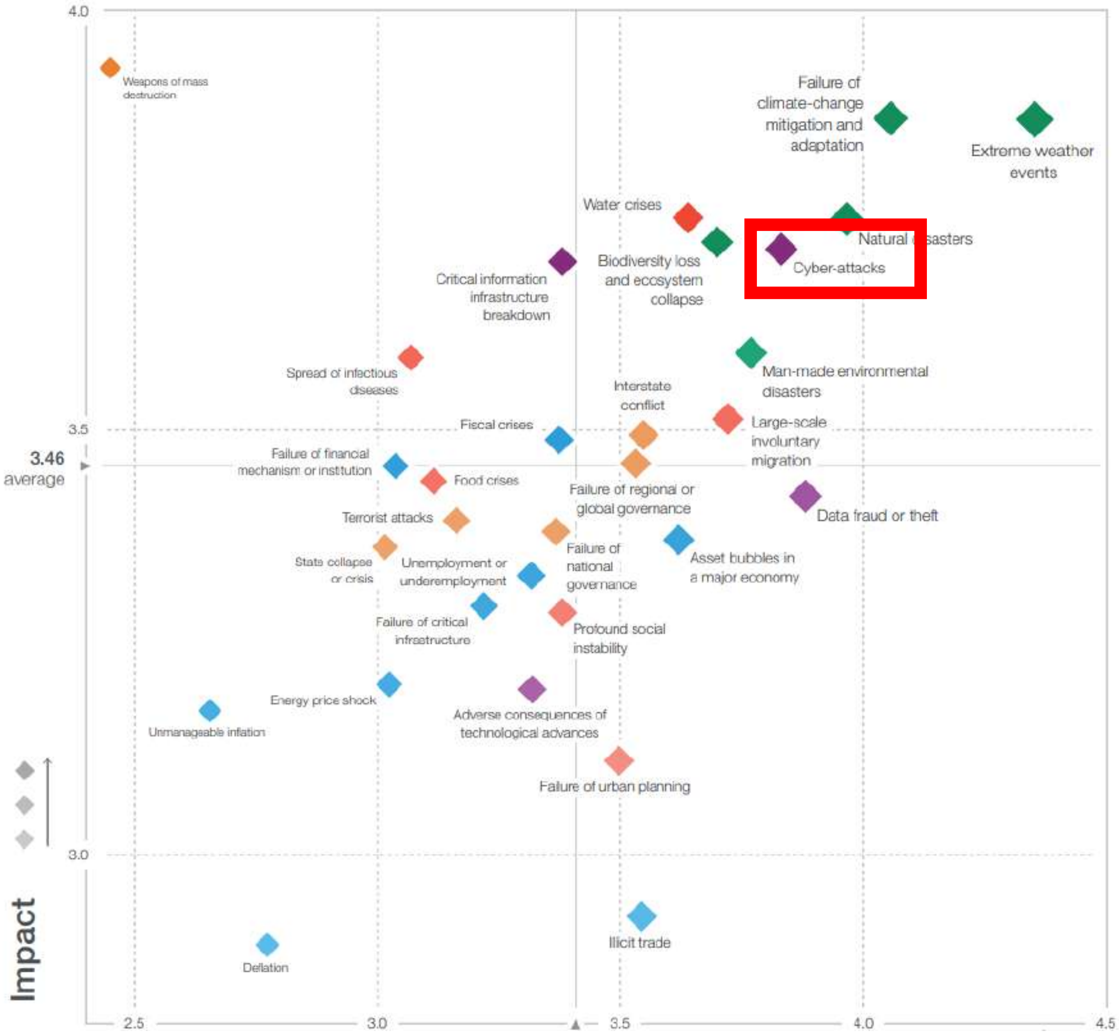
“Global Risks Landscape 2019”



Top 10 risks in terms of

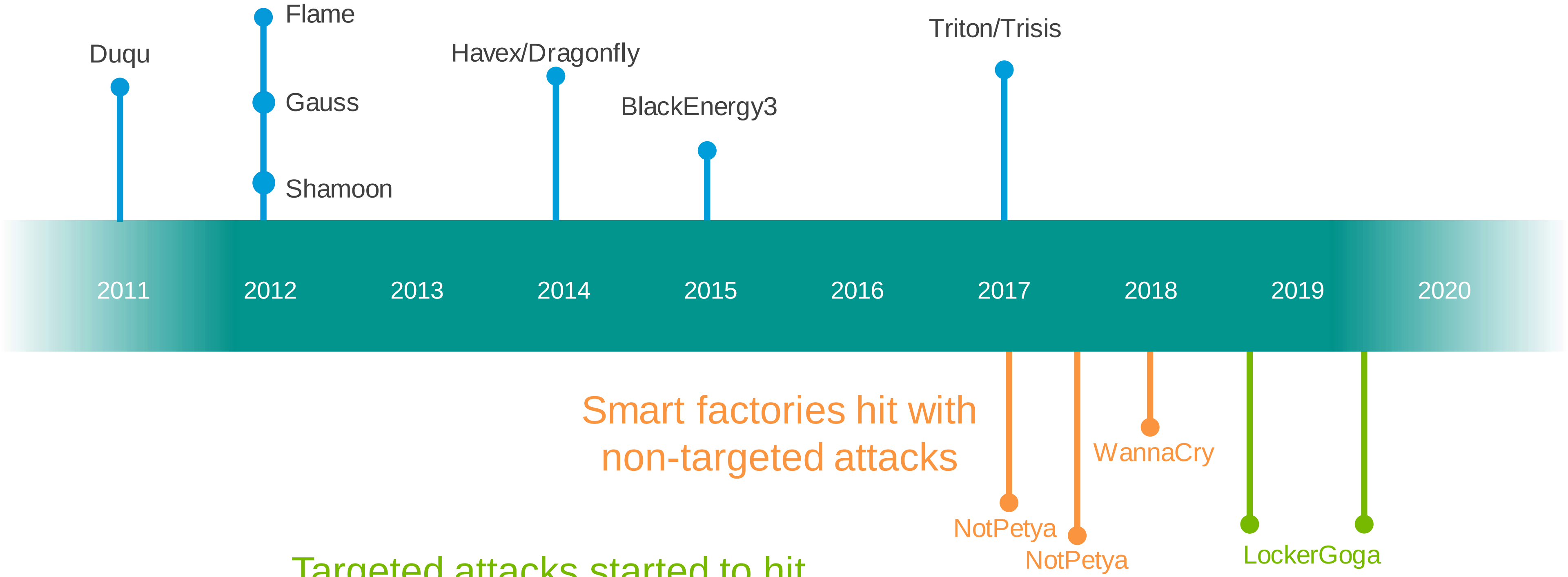
Impact

1. Weapons of mass destruction
2. Failure of climate-change mitigation and adaptation
3. Extreme weather events
4. Water crises
5. Natural disasters
6. Biodiversity loss and ecosystem collapse
7. Cyber-attacks
8. Critical information infrastructure breakdown
9. Man-made environmental disasters
10. Spread of infectious diseases



Industrial Cyberattack Patterns

Targeted Cyberattacks on Critical infrastructure



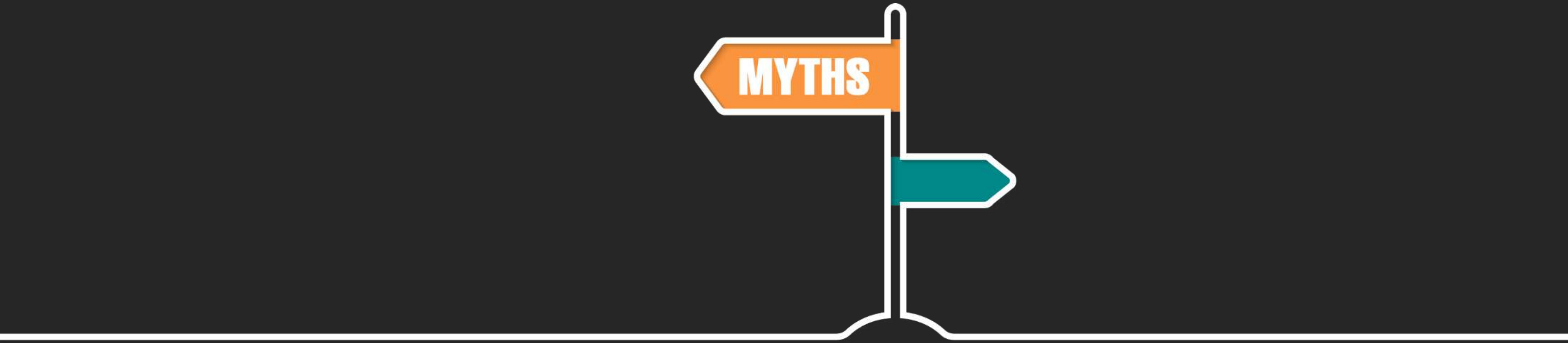
Smart factories hit with non-targeted attacks

Targeted attacks started to hit smart factories only recently

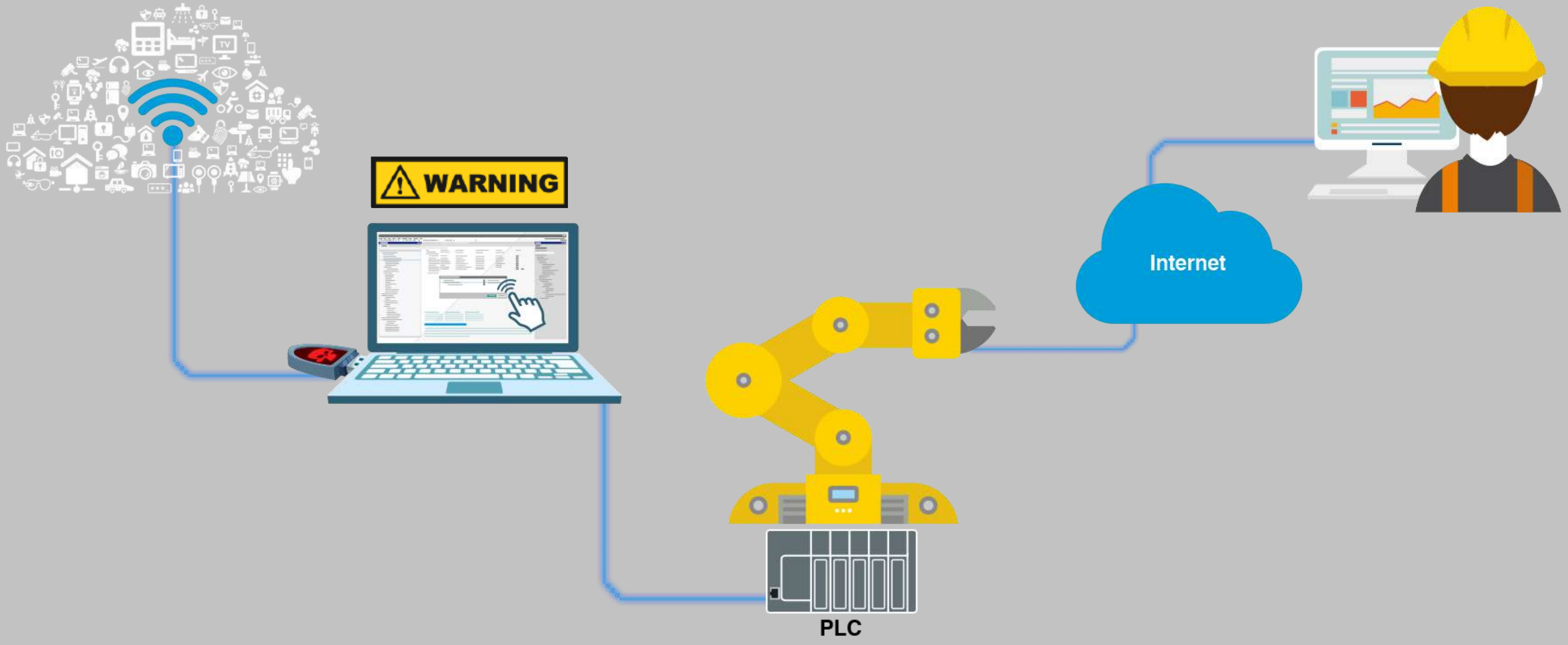
Common Myths About Industrial Cybersecurity

Industrial Cybersecurity Myth 1

Industrial control system networks are physically isolated
and not directly connected to the Internet.
Therefore, my networks are secure.

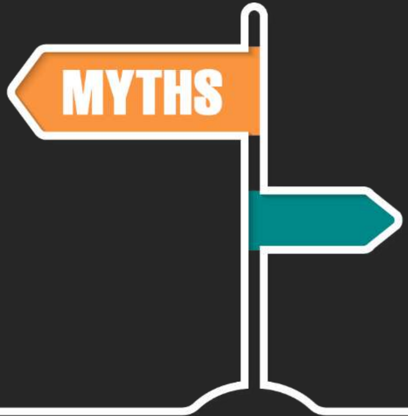


Even if they are isolated with no internet connection, industrial control systems may still have unsecure connections such as maintenance from 3rd part vendors)



Industrial Cybersecurity Myth 2

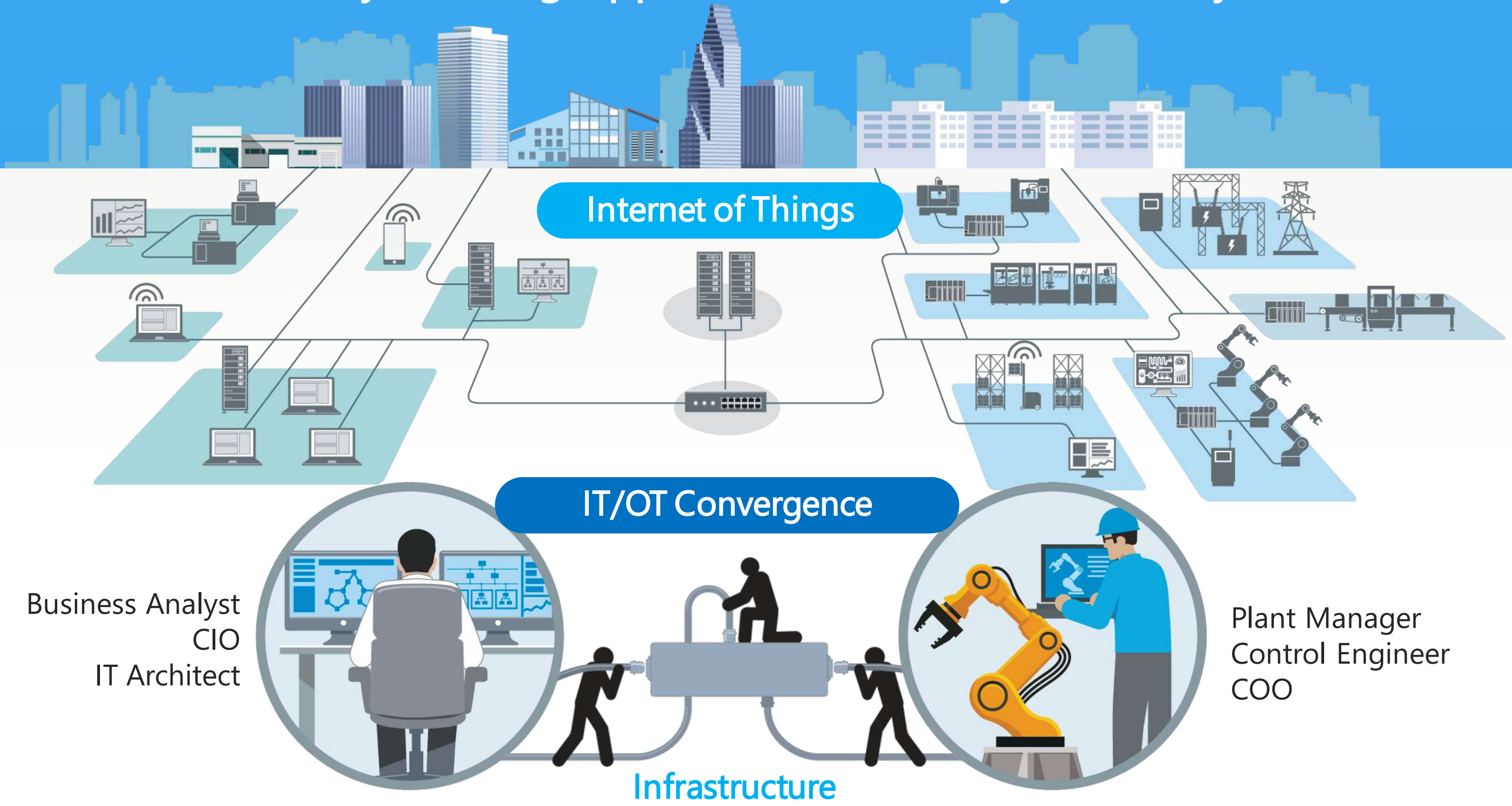
Even if hackers understand ICS networks, I am running
a medium-sized business, so my facilities will not be targeted.
Therefore, my networks are secure.



You don’t have to be a target to become a victim; according to a market research report, around 80% of industrial security incidents are unintentional*, but they can still cause a lot of damage and to your business operations.

Source: 5 Myths of ICS Cyber Security – 2017, KIACS Cyber Security Conference

IIoT and Industry 4.0 Bring Opportunities… and Cybersecurity Threats



Internet of Things

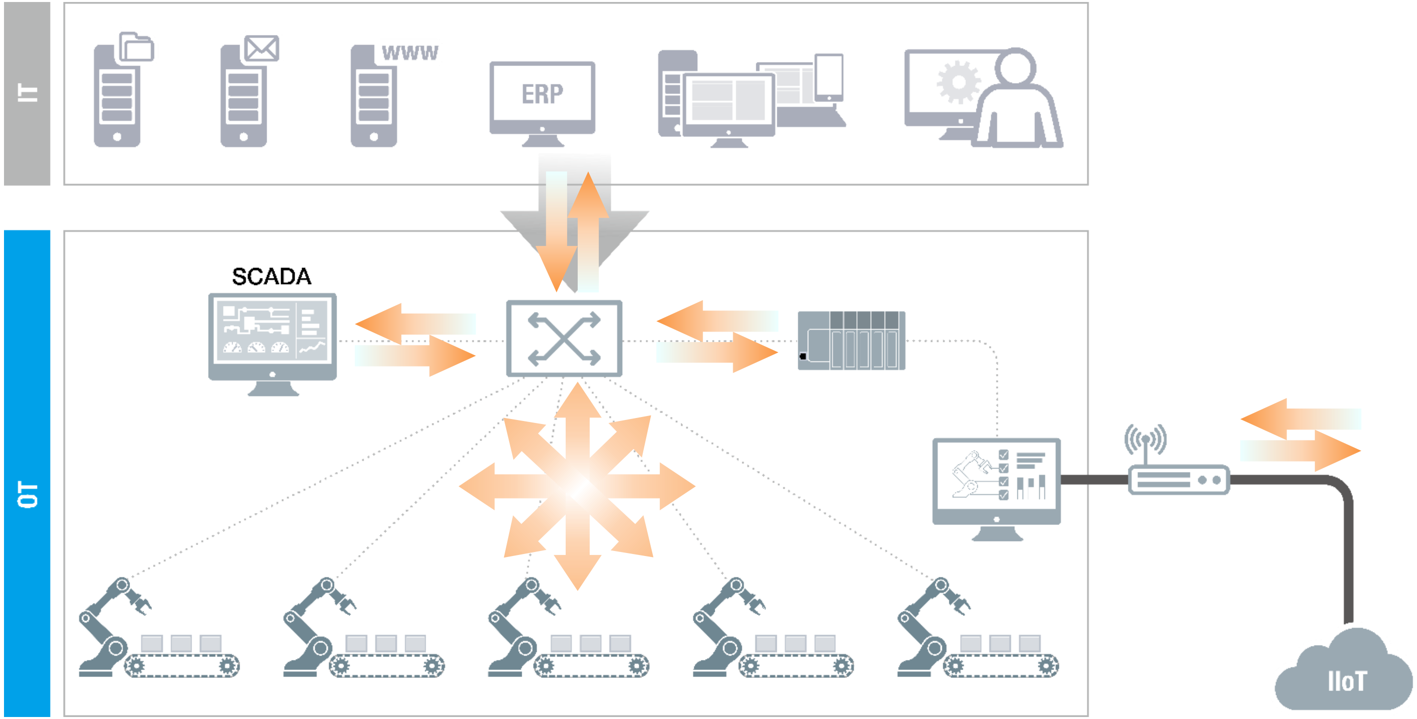
IT/OT Convergence

Business Analyst
CIO
IT Architect

Plant Manager
Control Engineer
COO

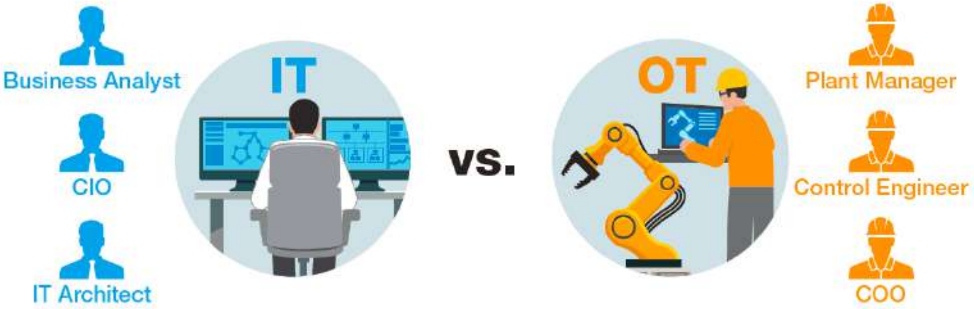
Infrastructure

Industrial Networking, OT-IT Convergence, and Industrial IoT



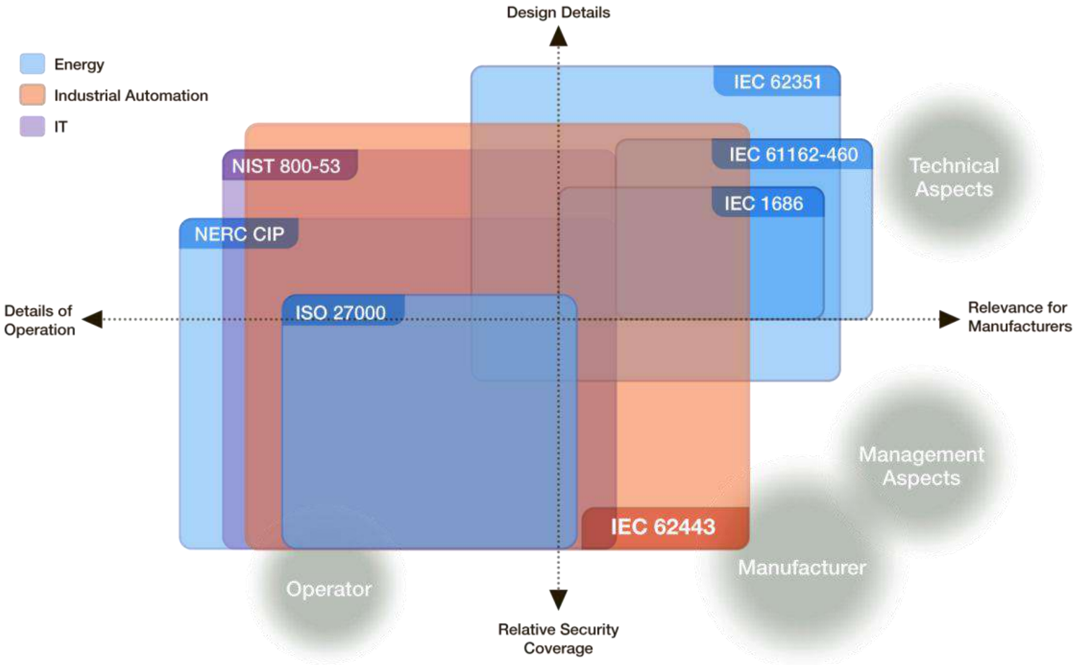
Industrial vs. IT Cybersecurity

IT and OT Have Different Perspectives in Cybersecurity



Business Priority	Confidentiality	Availability
Major Focus	Data integrity is key	Control processes cannot tolerate downtime
Protection Targets	Windows computers, servers	Industrial legacy devices: PLC, HMI, meters
Environmental Conditions	Air-conditioned	Harsh environments: extreme temperatures, vibrations & shocks

Standards



General Industrial Automation
ISA 99 / IEC 62443

ISA IEC

Power Automation
IEC 63351 / NERC CIP (U.S.)

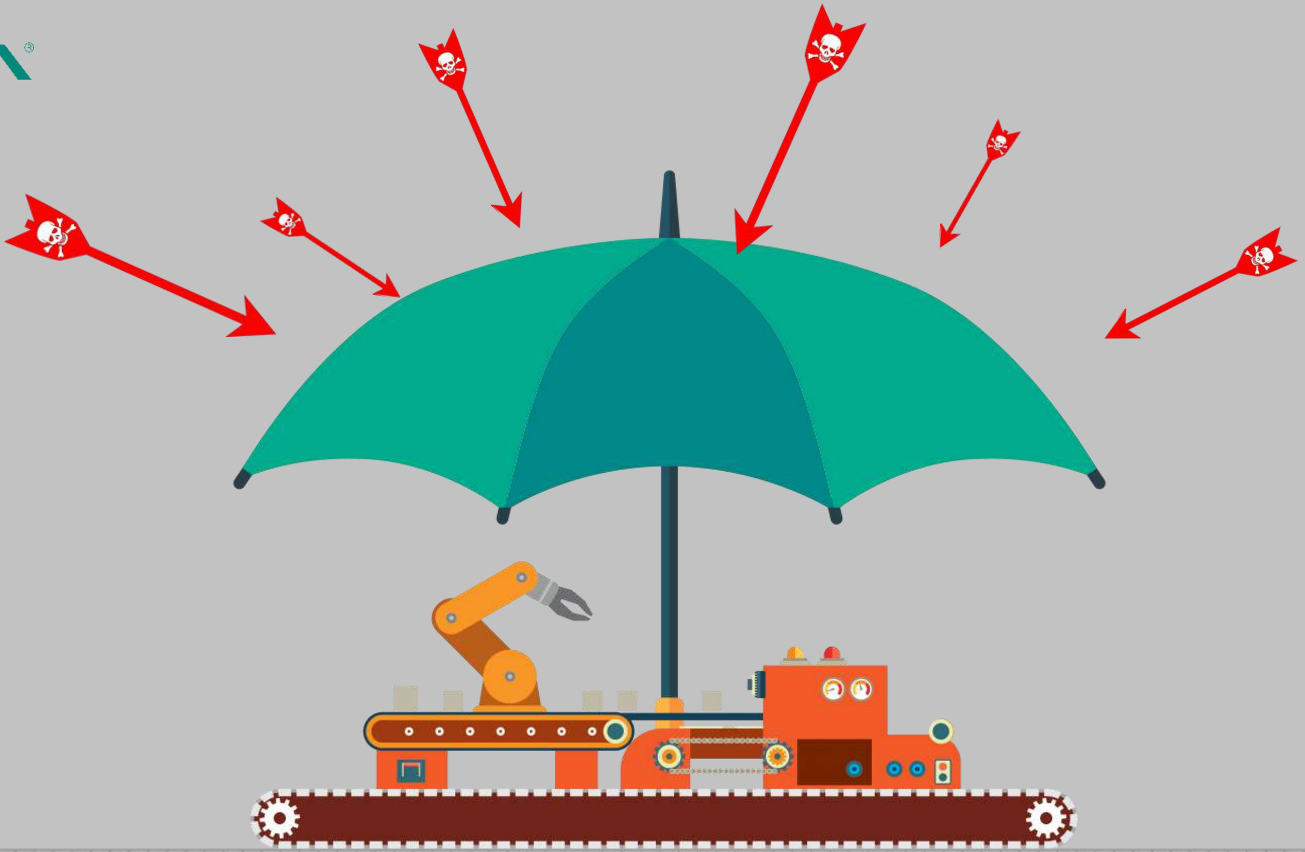
IEC NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Guide to ICS Security
NIST SP 800-53 (U.S.)

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

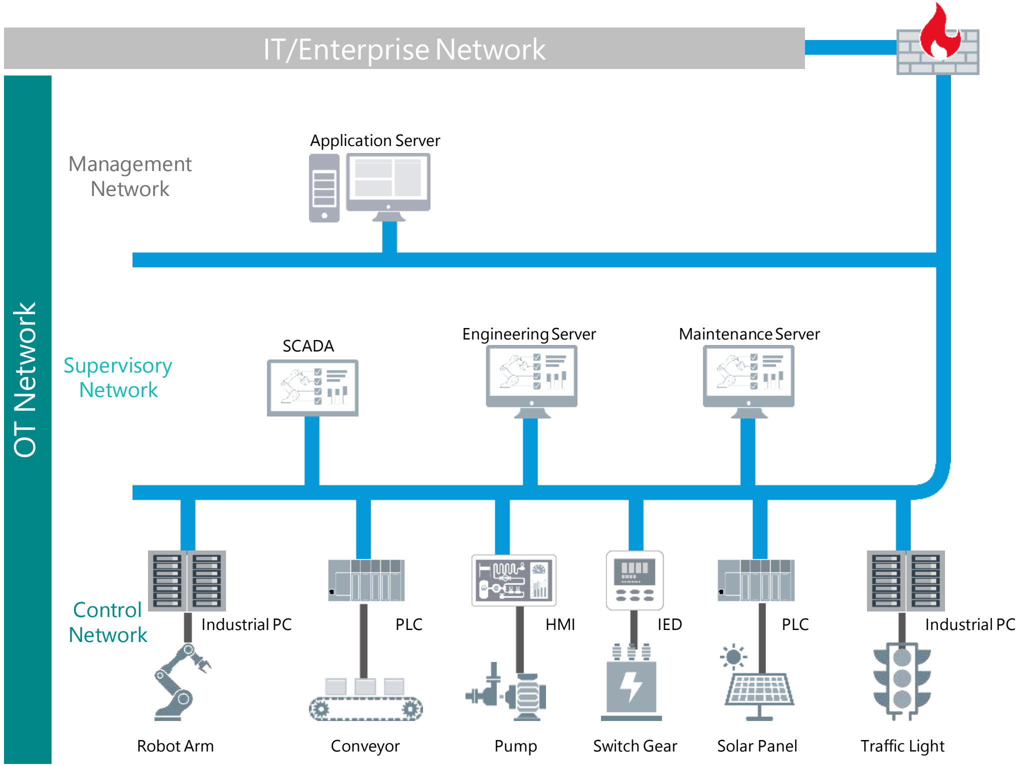
Marine Automation
IEC 61162-460

IT Security System
ISO / IEC 27000



Device security is the first step but from a system perspective, your network will need **defense-in-depth security protection**

Challenges for Traditional OT Network



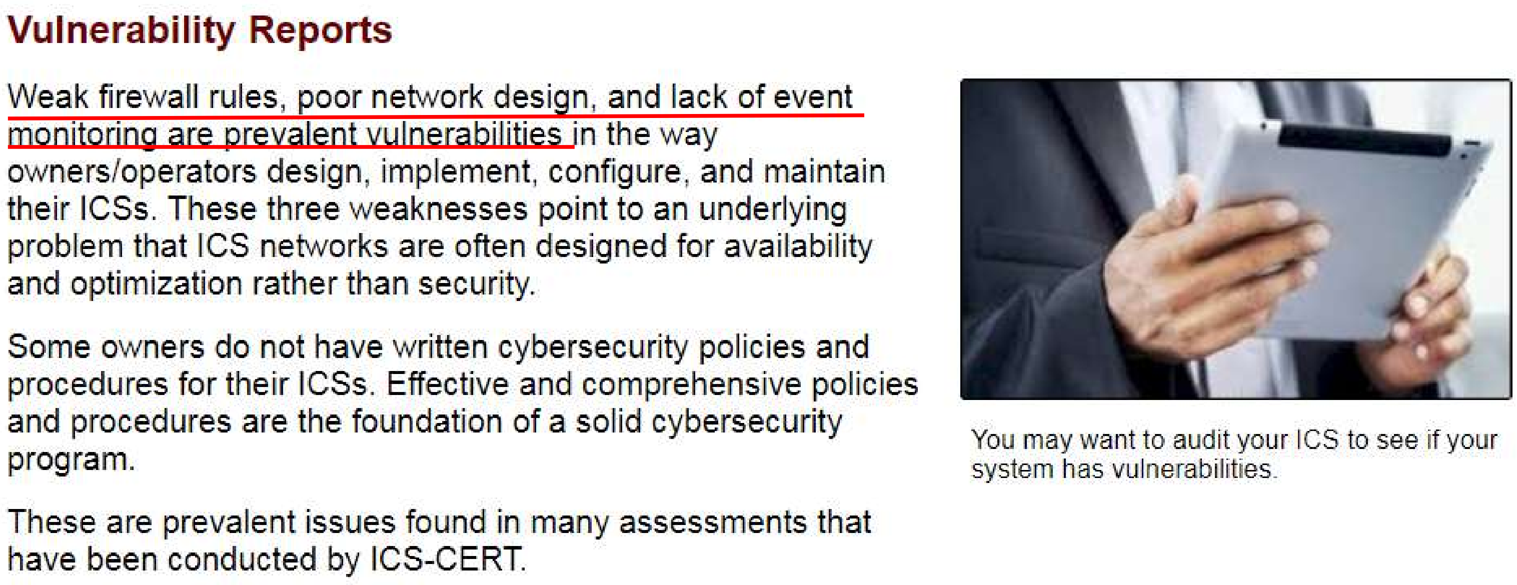
Lack of OT Visibility
Unknown devices, connections, and cyber threat status

Lack of Security Boundary for OT Network
Over-trust single point firewall perimeter protection

Uncontrolled Access on OT Network & Device
Unauthorized user or device from inside or outside of OT network

Insecure OT Communication
Unencrypted / Unauthorized OT communication

Difficult to patching Devices
Patching is not feasible or available



Vulnerability Reports

Weak firewall rules, poor network design, and lack of event monitoring are prevalent vulnerabilities in the way owners/operators design, implement, configure, and maintain their ICSs. These three weaknesses point to an underlying problem that ICS networks are often designed for availability and optimization rather than security.

Some owners do not have written cybersecurity policies and procedures for their ICSs. Effective and comprehensive policies and procedures are the foundation of a solid cybersecurity program.

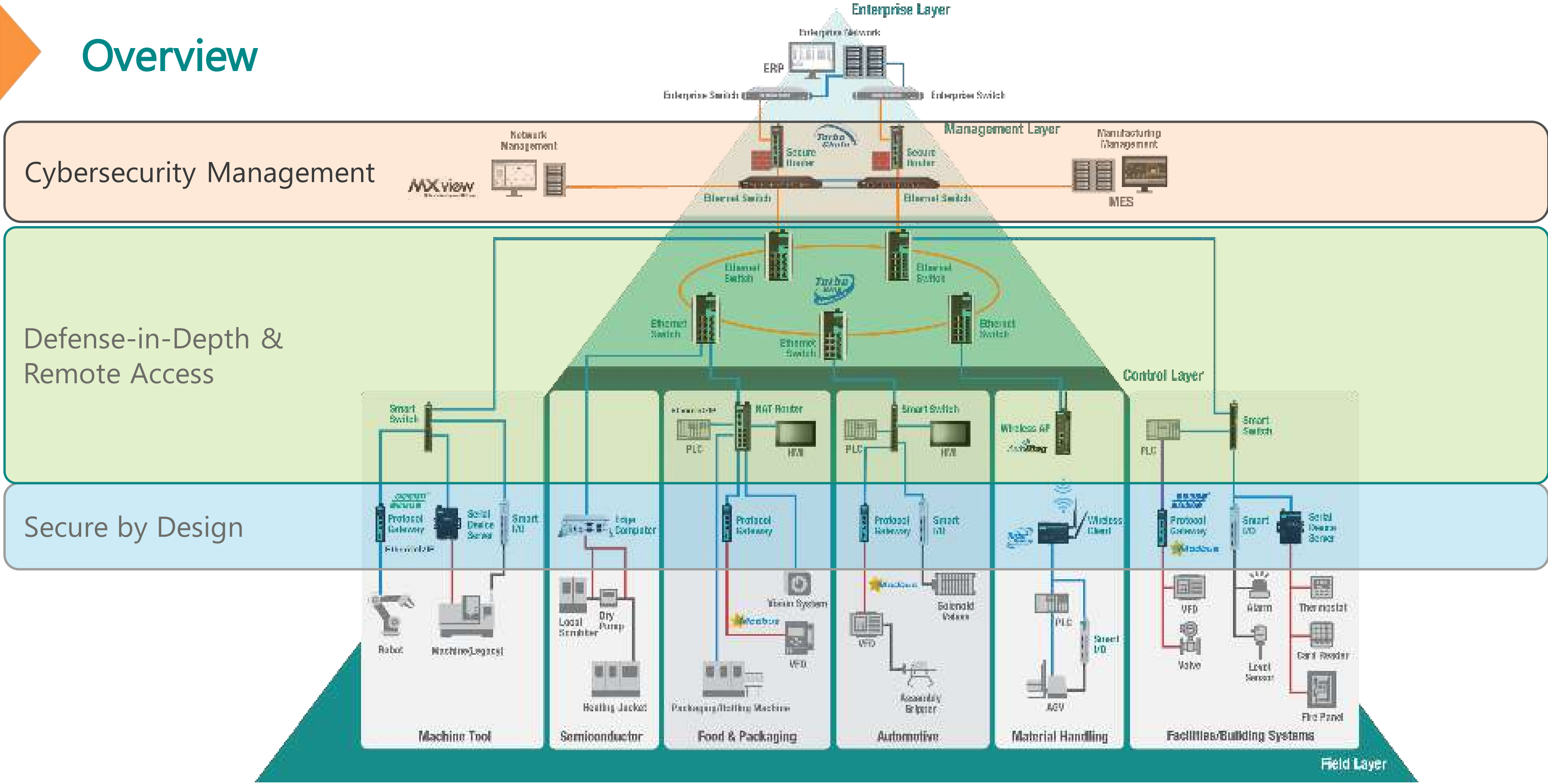
These are prevalent issues found in many assessments that have been conducted by ICS-CERT.

You may want to audit your ICS to see if your system has vulnerabilities.

Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (DHS ICS-CERT)®

Solutions

Overview

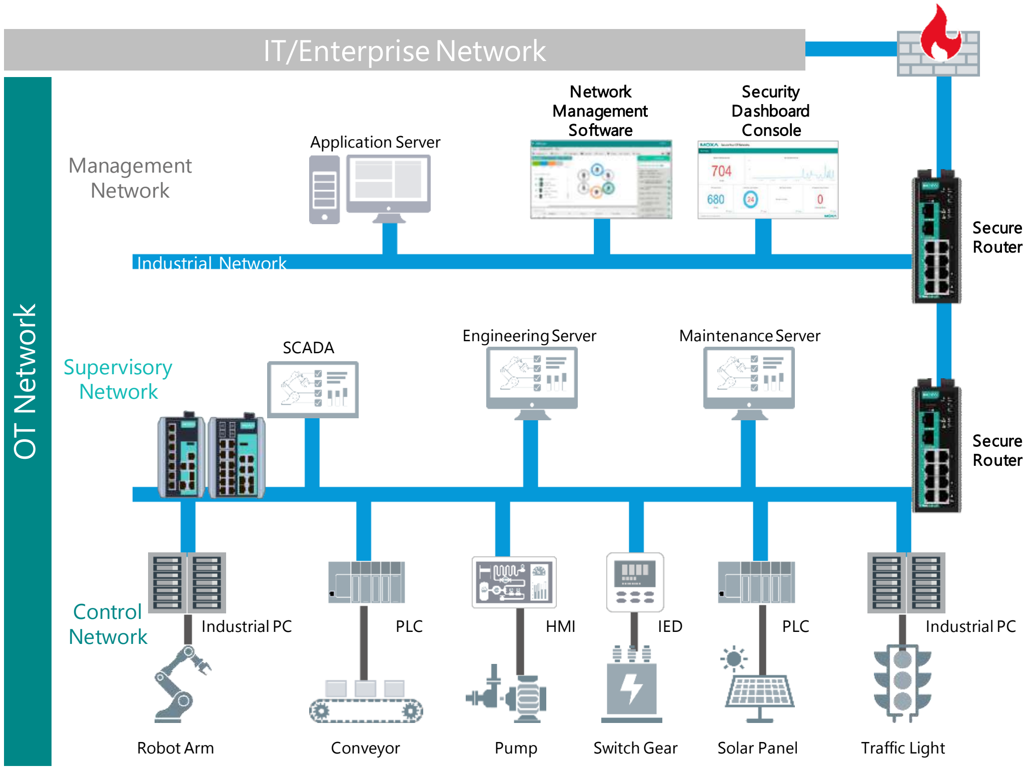


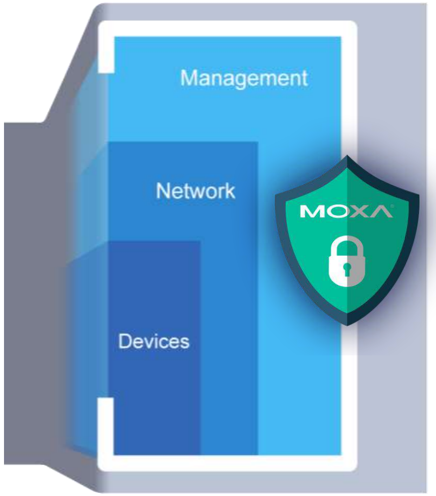
Cybersecurity Management

Defense-in-Depth & Remote Access

Secure by Design

Secure Network Infrastructure Reference Architecture



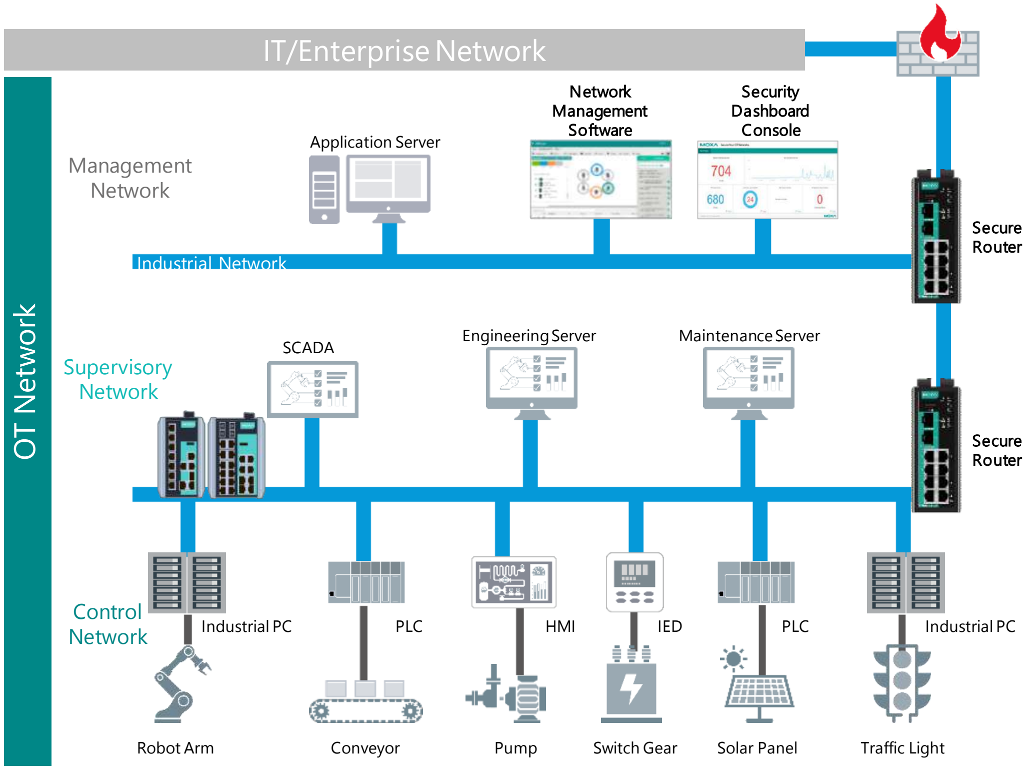


Network Management

Network Protection

Device Security

Secure Network Infrastructure Reference Architecture



Holistic Approach

- CSRT Team
- Threat Intelligence

Security Management

- NMS with Security View

Secure Infrastructure

- Data Encryption
- Secure Router
- Secure Remote Access

Network Access

- Access Control List
- Port Security

Device Security

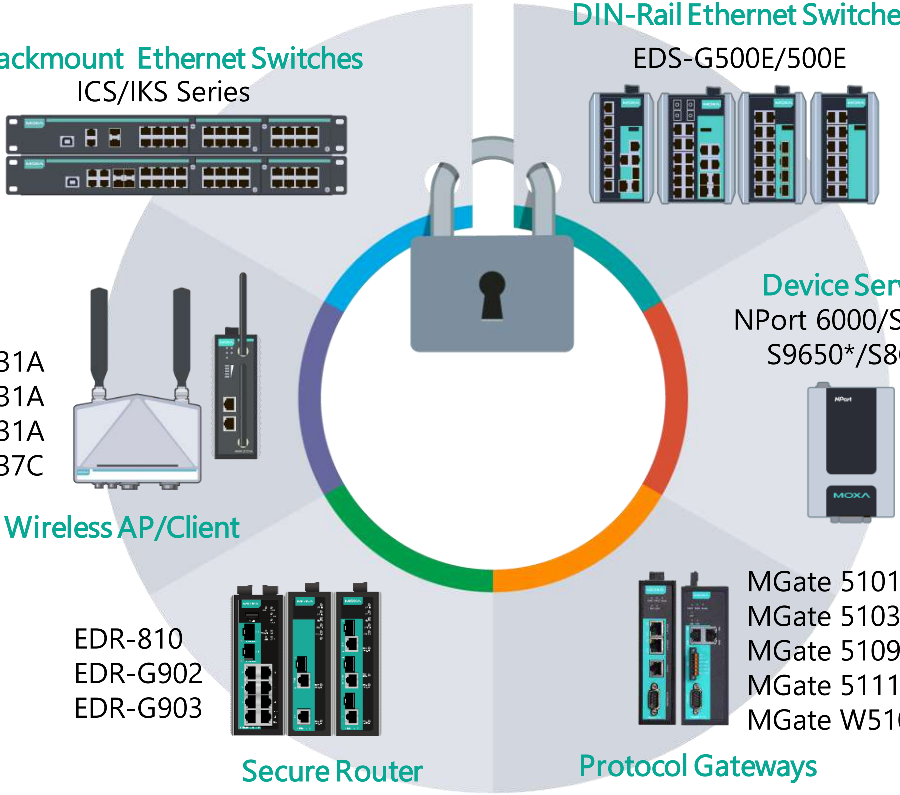
- Application Whitelisting
- IEC 62443-4-2 features

Network Management

Network Protection

Device Security

Product Portfolio



Rackmount Ethernet Switches
ICS/IKS Series

DIN-Rail Ethernet Switches
EDS-G500E/500E

Device Servers
NPort 6000/S9450/
S9650*/S8000

MGate 5101/5102
MGate 5103/5105
MGate 5109
MGate 5111/5118
MGate W5108/W5208

Protocol Gateways

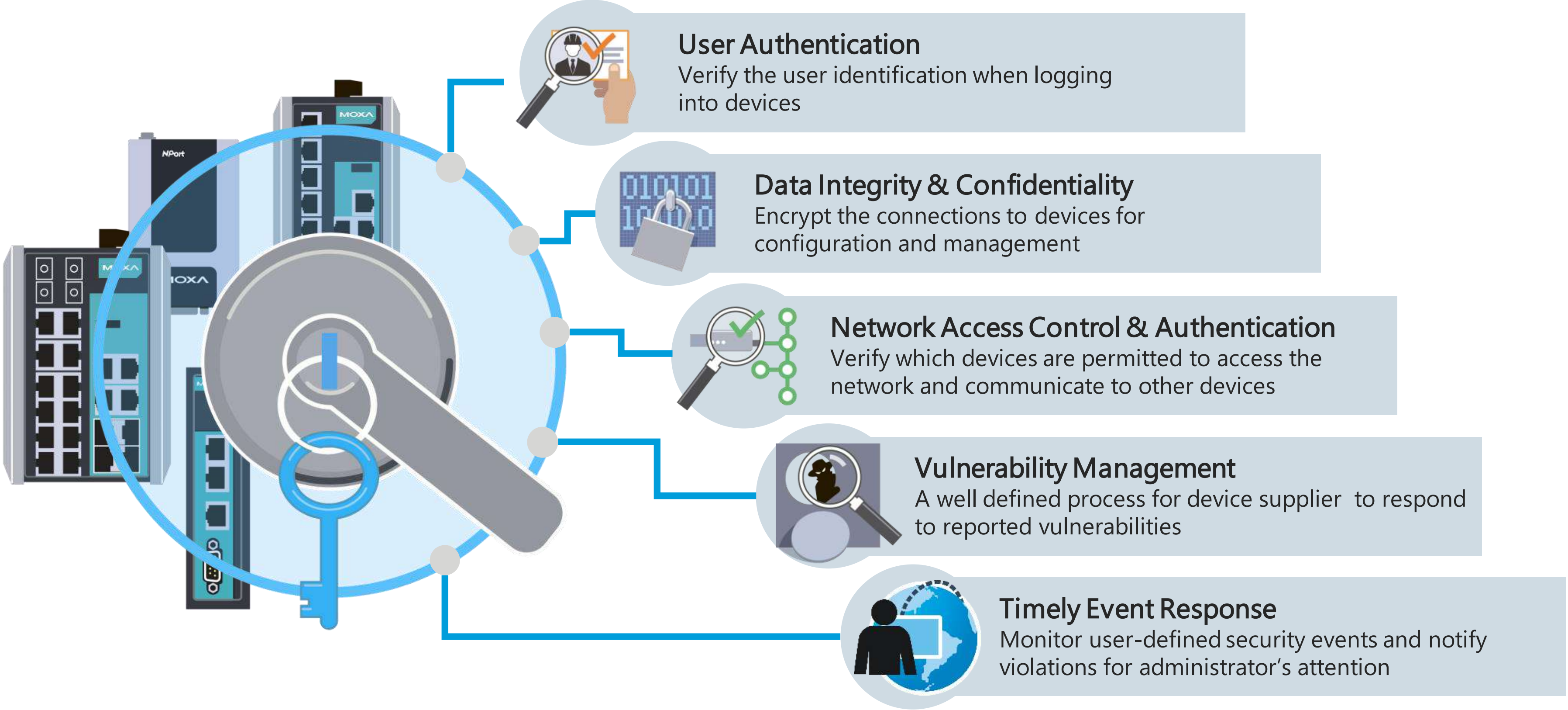
EDR-810
EDR-G902
EDR-G903

Secure Router

AWK-4131A
AWK-3131A
AWK-1131A
AWK-1137C

Industrial 802.11n Wireless AP/Client

Security Hardened Devices with Embedded Security Functions



User Authentication
Verify the user identification when logging into devices

Data Integrity & Confidentiality
Encrypt the connections to devices for configuration and management

Network Access Control & Authentication
Verify which devices are permitted to access the network and communicate to other devices

Vulnerability Management
A well defined process for device supplier to respond to reported vulnerabilities

Timely Event Response
Monitor user-defined security events and notify violations for administrator's attention

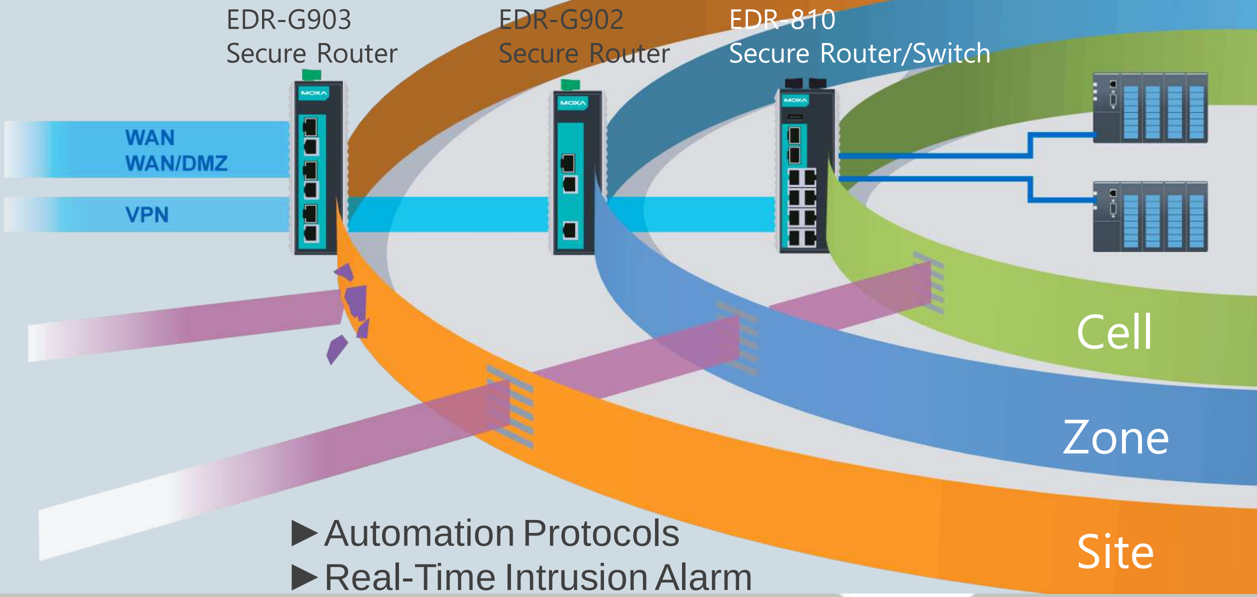
Product Portfolio

EDR-G902/G903/810 Series

Industrial Secure Router

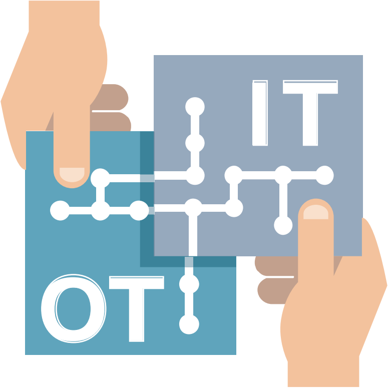
Key Features

- NAT/Firewall isolate unwanted traffic
- Support IPSec and OpenVPN protocols
- DoS Protection
- Dual WAN redundant interfaces* (EDR-G903 only)

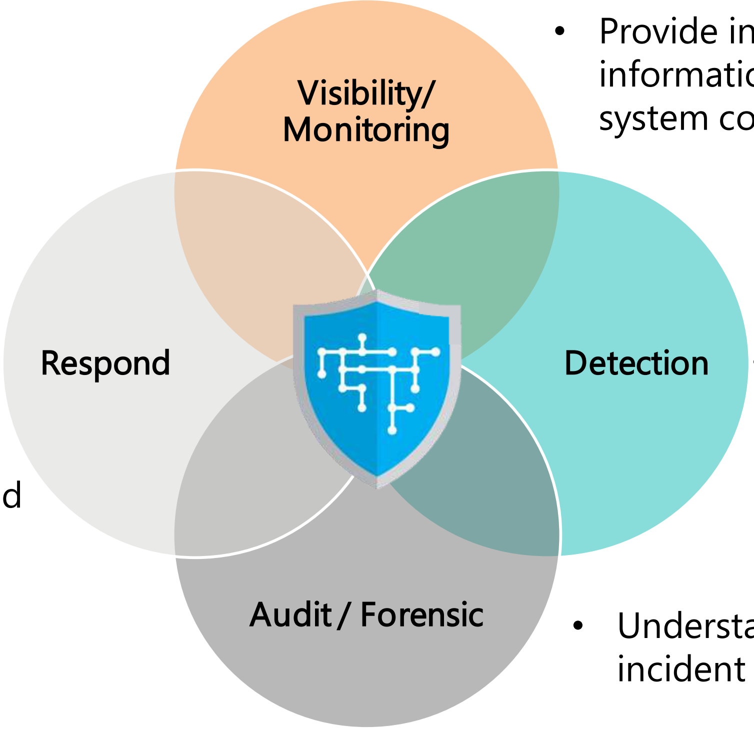


- ► Automation Protocols
- ► Real-Time Intrusion Alarm

Needs to cover



- An anomaly is detected what to do?



- Provide in real time information about the system components

- Malicious and Anomalies patterns

- Understand how an incident happened

Moxa Solution

Visualized Management for Security Audit and Monitoring

Asset Management

Auto discover and track the devices on your network

Device Security Policy Audit

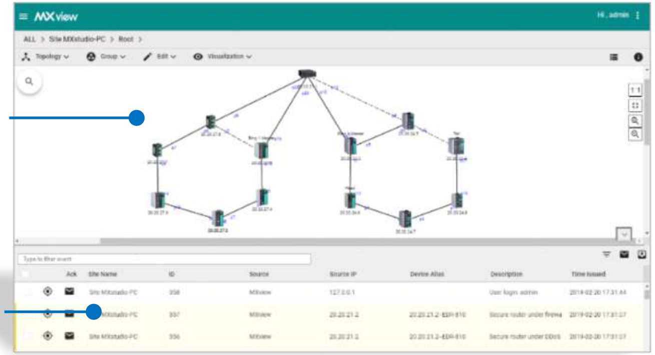
Check if the device settings meet the security policies

Configuration Management

Backup and restore the configuration if a device is compromised

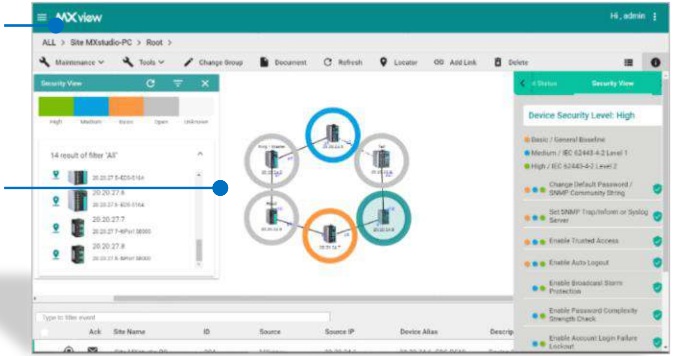
Security Event Detection and Logging

Log events when a security policy is breached



Asset Management

Event Detection & Logging



Configuration Management

Security Policy Audit

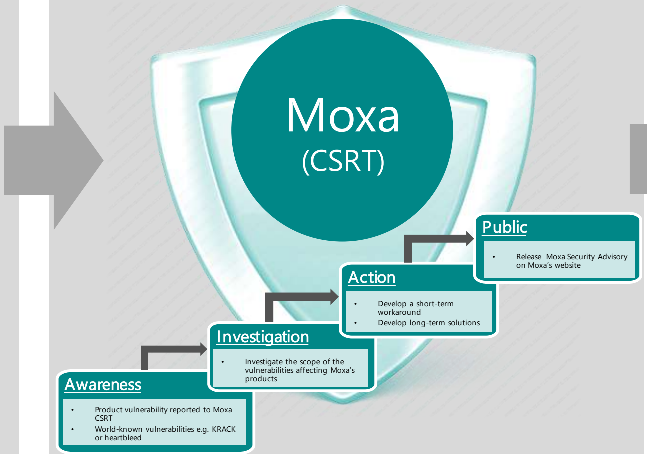
Moxa Cyber Security Response Team (CSRT)

The Moxa CSRT was established to provide a *quick response* to the market when cybersecurity issues / IT vulnerabilities are raised from outside of Moxa

Industry wide vulnerability Or product vulnerabilities

intel
Here's How Intel AMT Hack Works
Technical Explanation of CVE-2017-5689

Dedicated Moxa Cyber Security Response Team handling issues



Awareness

- Product vulnerability reported to Moxa CSRT
- World-known vulnerabilities e.g. KRACK or heartbleed

Investigation

- Investigate the scope of the vulnerabilities affecting Moxa's products

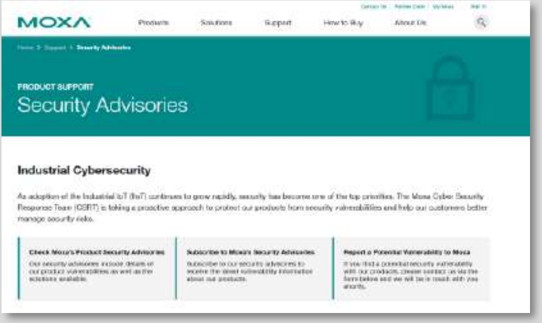
Action

- Develop a short-term workaround
- Develop long-term solutions

Public

- Release Moxa Security Advisory on Moxa's website

Transparent and responsible disclosure vulnerability into public


Contact Us | Partner Zone | My Moxa | Sign In
MOXA
Products
Solutions
Support
How to Buy
About Us
Home > Support > Security Advisories

PRODUCT SUPPORT

Security Advisories

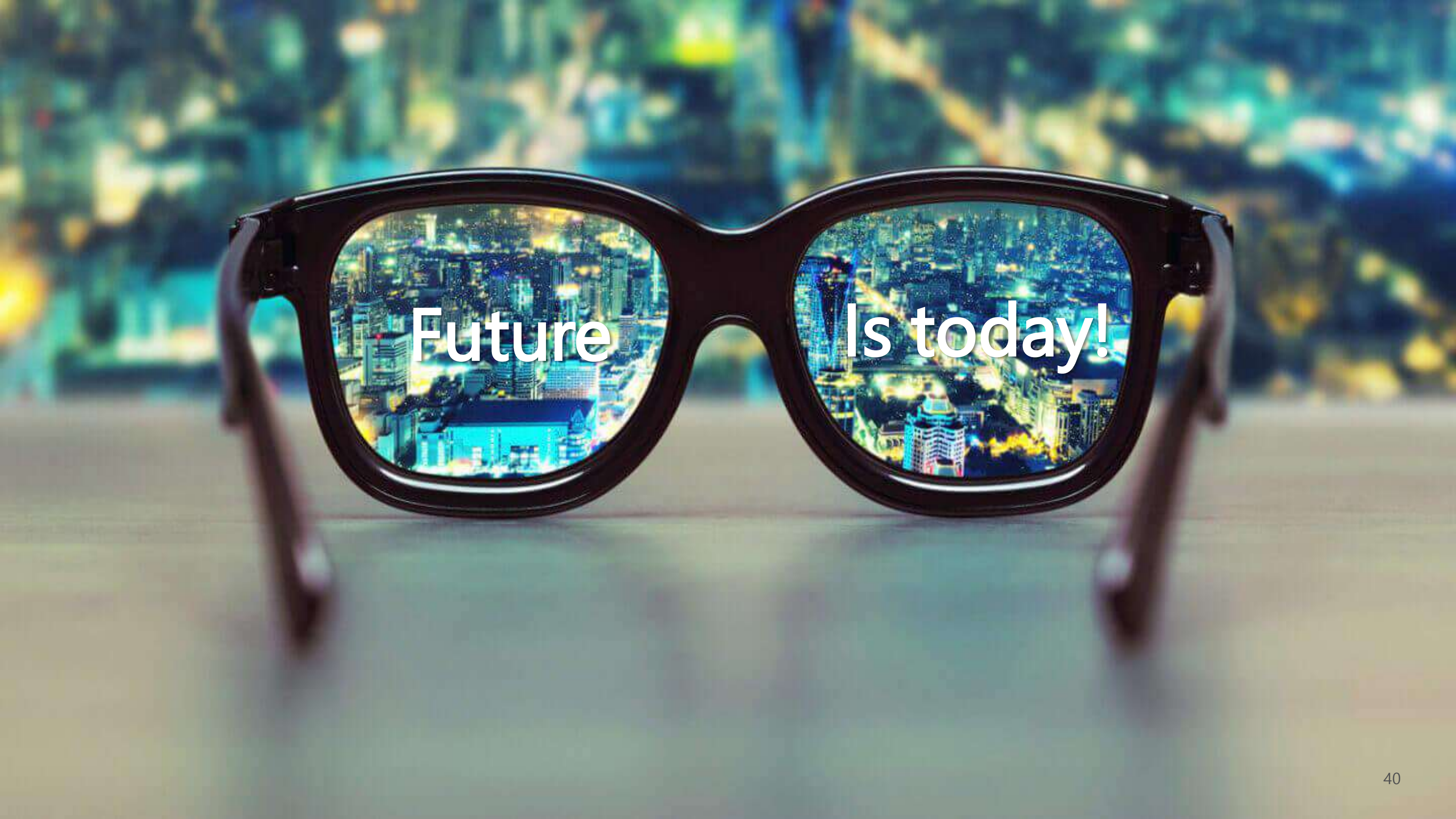
Industrial Cybersecurity

As adoption of the Industrial IoT (IIoT) continues to grow rapidly, security has become one of the top priorities. The Moxa Cyber Security Response Team (CSRT) is taking a proactive approach to protect our products from security vulnerabilities and help our customers better manage security risks.

Check Moxa's Product Security Advisories
Our security advisories include details of our product vulnerabilities as well as the solutions available.

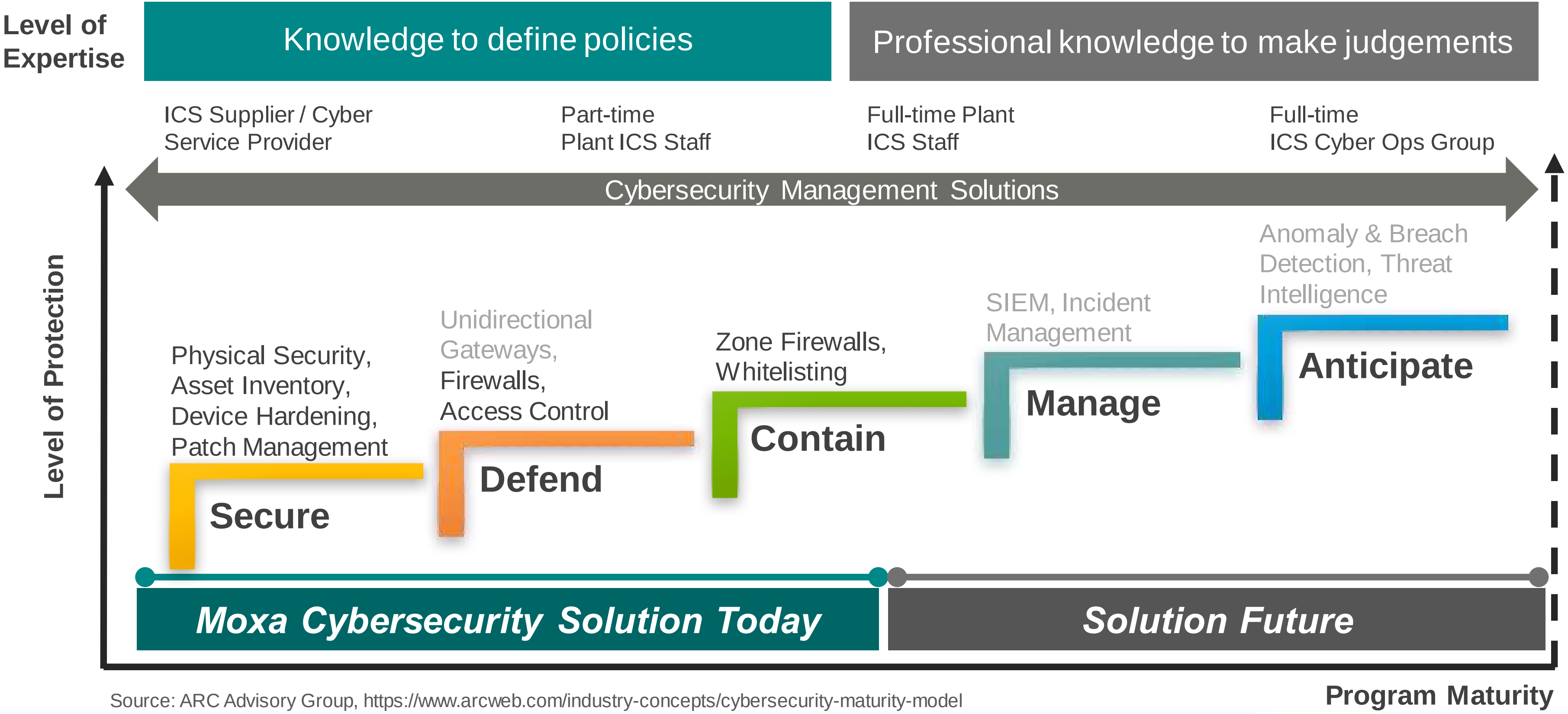
Subscribe to Moxa's Security Advisories
Subscribe to our security advisories to receive the latest vulnerability information about our products.

Report a Potential Vulnerability to Moxa
If you find a potential security vulnerability with our products, please contact us via the form below and we will be in touch with you shortly.



Future Is today!

Moxa's Positioning in Industrial Cybersecurity



Level of Expertise

Knowledge to define policies

Professional knowledge to make judgements

ICS Supplier / Cyber Service Provider

Part-time Plant ICS Staff

Full-time Plant ICS Staff

Full-time ICS Cyber Ops Group

Cybersecurity Management Solutions

Level of Protection

Secure: Physical Security, Asset Inventory, Device Hardening, Patch Management

Defend: Unidirectional Gateways, Firewalls, Access Control

Contain: Zone Firewalls, Whitelisting

Manage: SIEM, Incident Management

Anticipate: Anomaly & Breach Detection, Threat Intelligence

Moxa Cybersecurity Solution Today

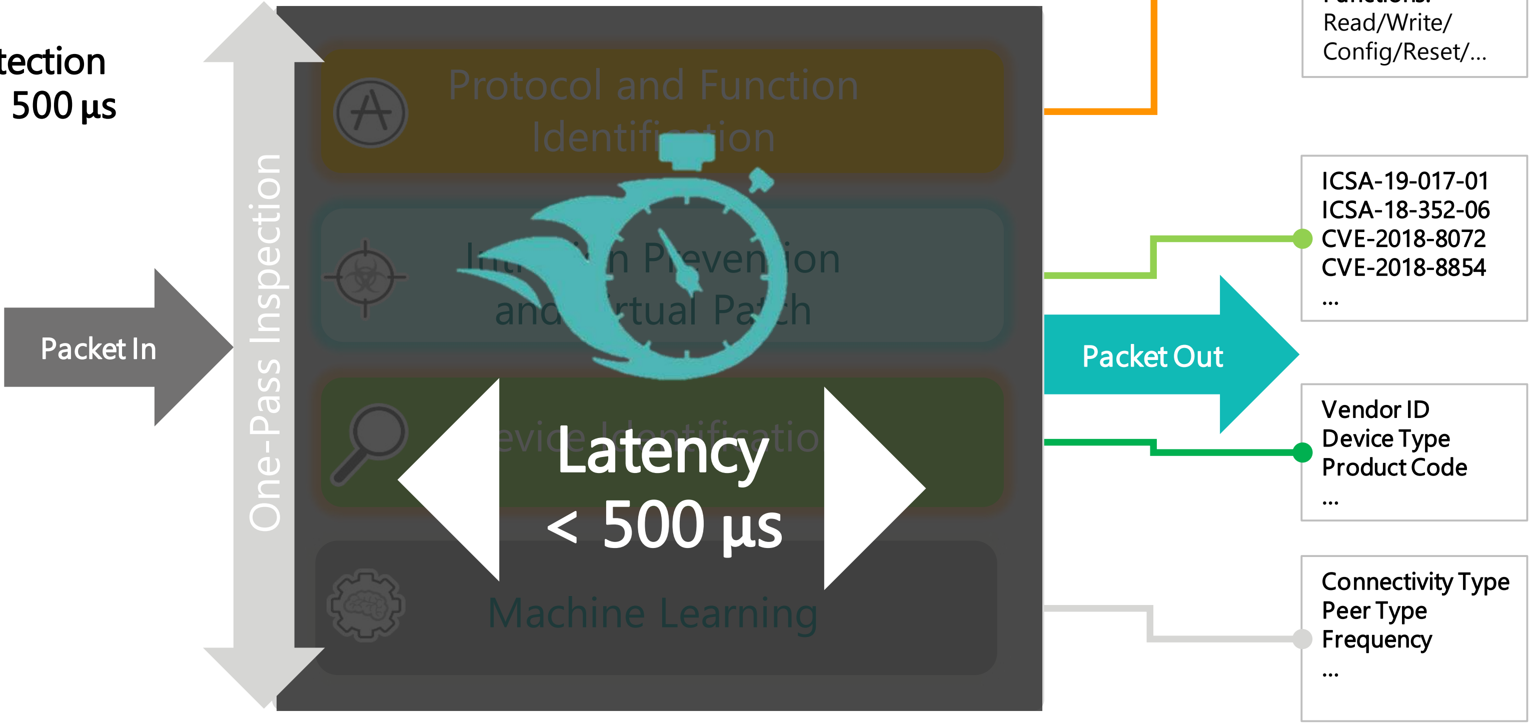
Solution Future

Program Maturity

Source: ARC Advisory Group, https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model

OT-Centric Deep Packet Inspection
- One-Pass Inspection

- IT-OT DNA Integration
- Visibility
- Control & Protection
- Low Latency < 500 µs



Protocols:
CC-Link
Modbus
Ethernet/IP
Profinet
...
Functions:
Read/Write/
Config/Reset/...

ICSA-19-017-01
ICSA-18-352-06
CVE-2018-8072
CVE-2018-8854
...

Vendor ID
Device Type
Product Code
...

Connectivity Type
Peer Type
Frequency
...

Secured by txOne networks

OT-IT Integrated Network Security Solution

OT-Centric

Integrated

Simple

Secure Network Infrastructure

Industrial Cybersecurity Solution

What makes a cybersecurity breach successful ?

Underestimate

(the problem + the probabilities)

+

Overtrust

(the defenses)

What is the key factor to avoid it?

Information

(visibility + anticipation + where apply the defenses)

Felipe Sabino Costa

National Industrial Automation Cybersecurity Specialist (IACS) / Deplo...

Felipe Sabino Costa

Felipe.costa@moxa.com

+55 11 96852-3781

/moxa inc
/felipecybersecurity

Thank You

MOXA®
Reliable Networks ▲ Sincere Service

DISTRIBUIDO EN MÉXICO POR TELSA MAYORISTA

Tels.: +52 (55) 5740 2142 / 55 5740 0606 • ventas@telsa.com.mx • www.telsa.com.mx
Síguenos en: Twitter.com/TelsaMayorista • Facebook.com/TelsaMexico

telsa®
La Alternativa en Conectividad
Más de 33 años de experiencia en soluciones de TIC

Contáctanos: