Security

4/9/2019

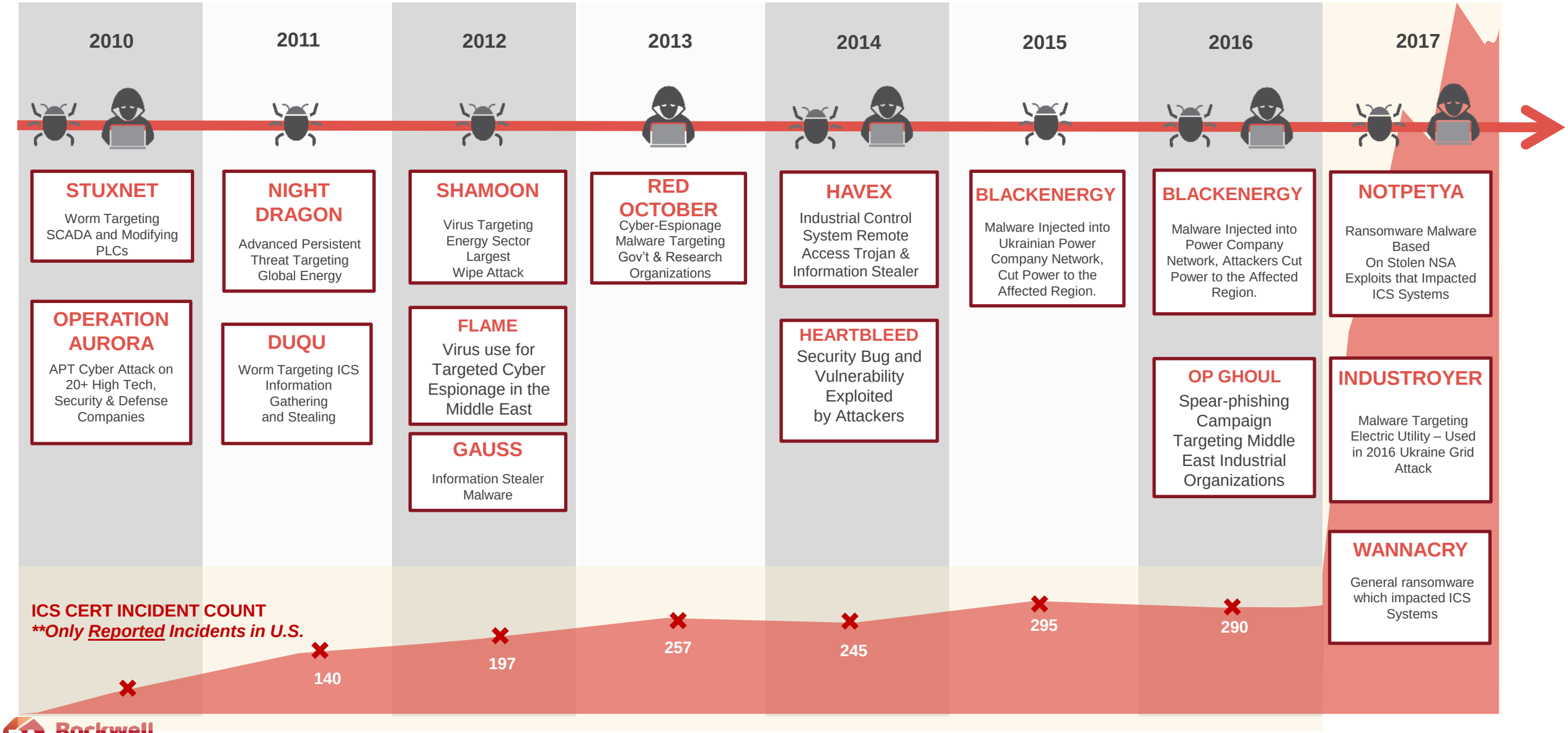
Roman Foukal

“Everything’s fine today, that is our illusion”

-Voltaire

Why should we be concerned with ICS Security?

ICS-Focused Campaigns, Attacks, Frequency



ICS THREAT ACTORS

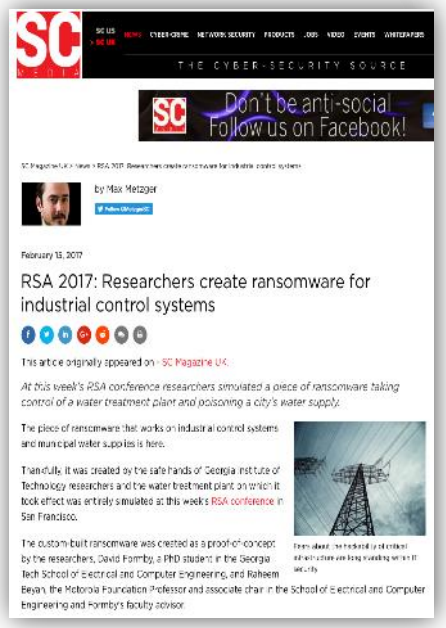
> 40%
Cyber Events

Nation States

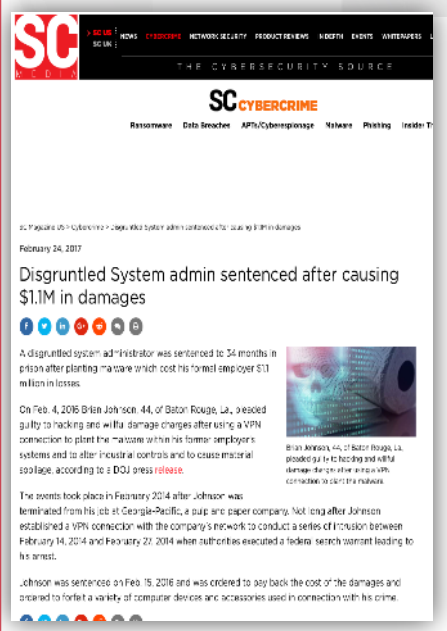
Terrorists

Hacktivists

Cyber Criminals



Insiders



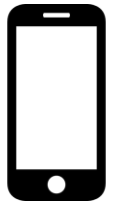
ICS Threat Vectors

Network

Wired | **Wireless**

Network based threat vector is most typically associated with remote access.

Mobile Device



Hotspot | **Wireless**

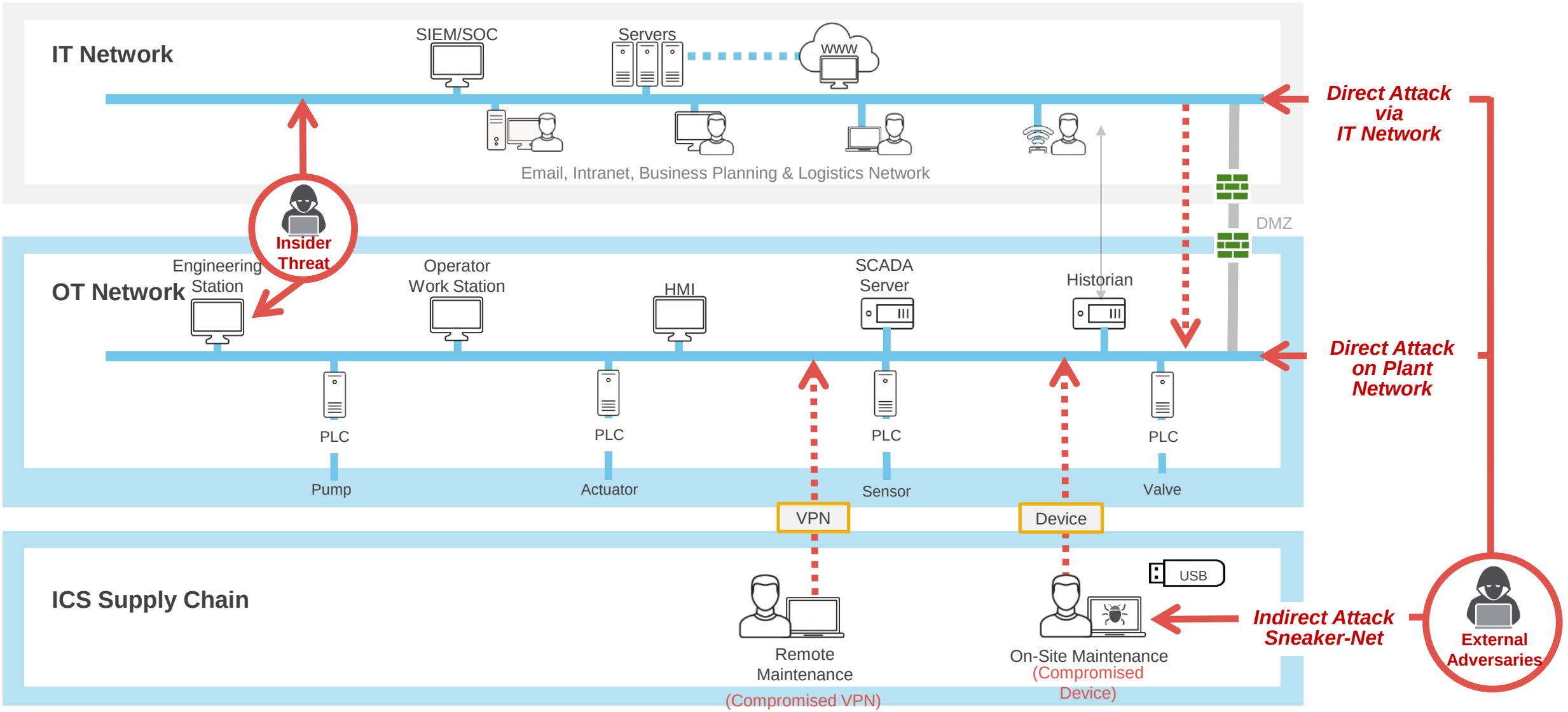
1. Mobile hotspot can present direct internet access to device
2. Inadvertent physical connection to target

Physical Access

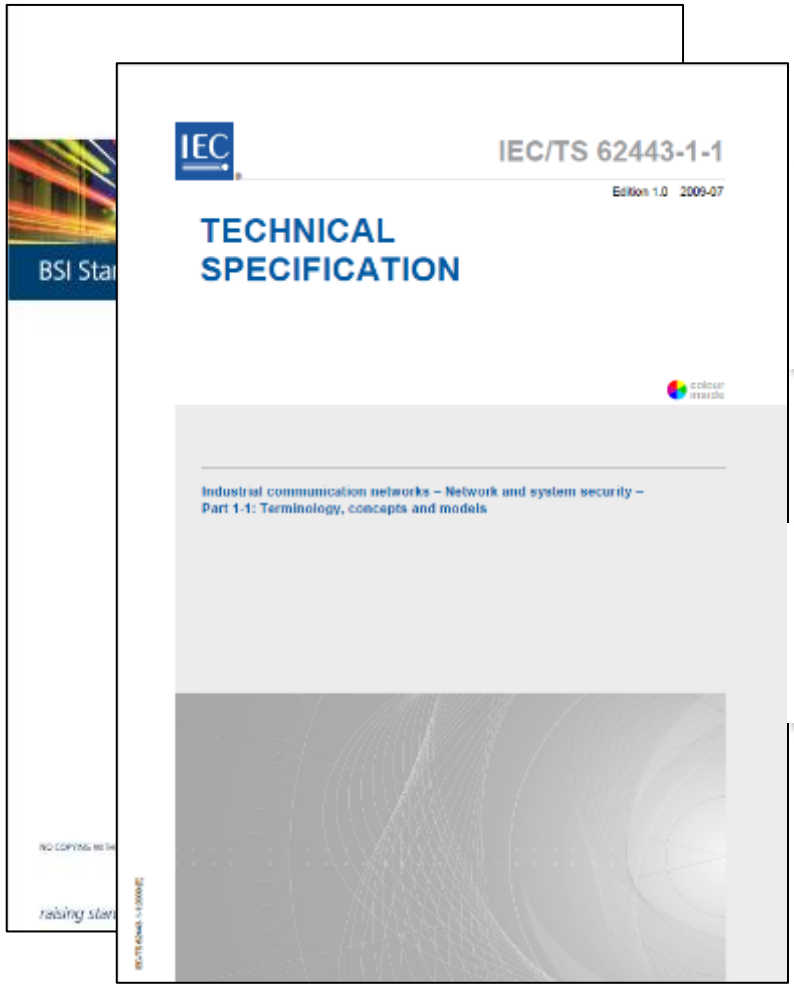
Direct | **Media**

1. Direct access to target by adversary
2. SneakerNET: Inserting malicious removable media to target

ICS THREAT VECTORS



What is Risk?



3.12
risk
combination of the probability of occurrence of harm and the severity of that harm

3.2.87
risk
expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence [10]

Where do we start?

The Approach

Strategic

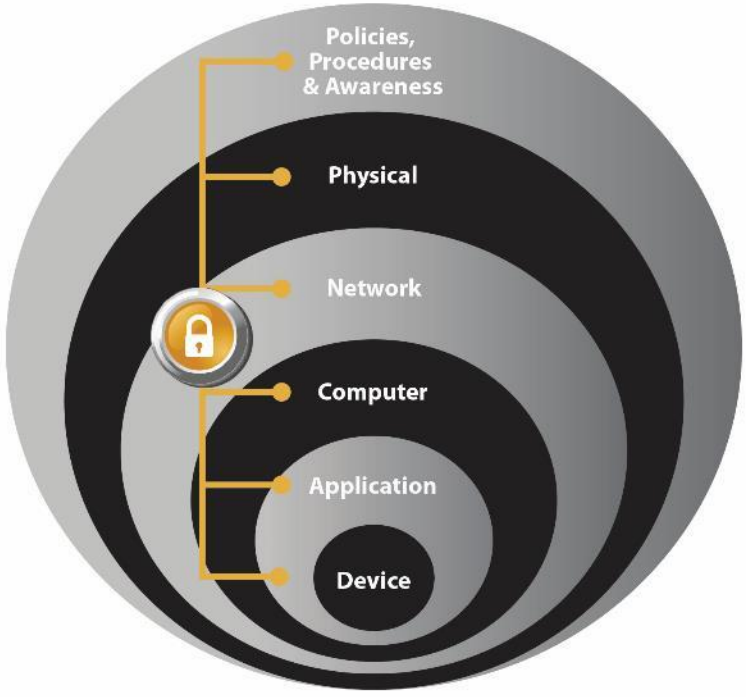
- Develop an OT cybersecurity program
- Adopt an industry framework
- Understand business drivers and risk tolerances to drive target profiles
- Conduct assessments to develop an understanding of gaps
- Create an improvement plan to drive the tactical approach

Tactical

- Execute on filling gaps as defined and prioritized in the strategic approach
- Utilize validated designs and architectures
- Implement pre-engineered infrastructure and software solutions to achieve targets

Holistic View

A secure application depends on multiple layers of protection and industrial security must be implemented as a system.



- ✓ **Flexibility**
- ✓ **Openness**
- ✓ **Consistency**

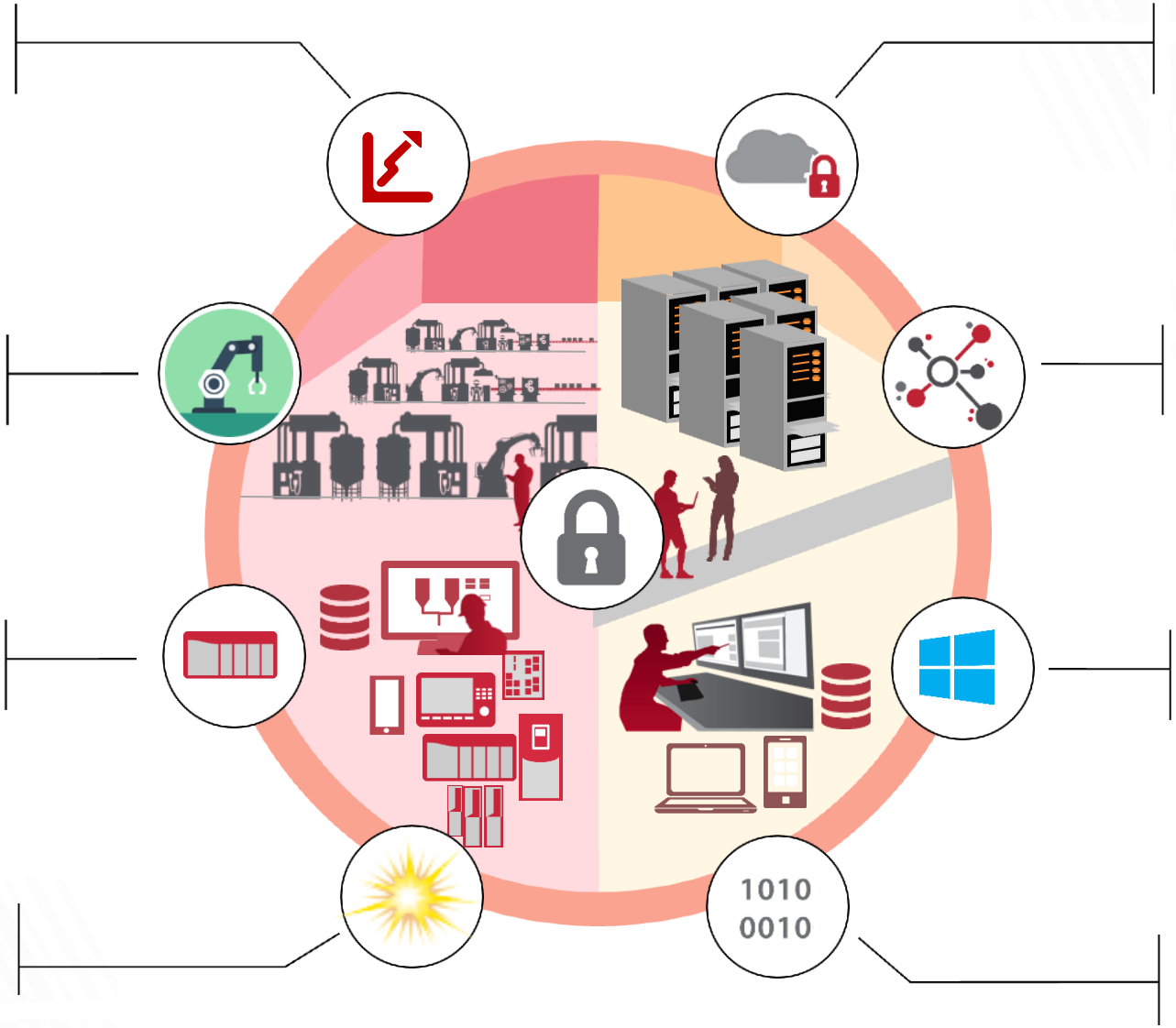
OT vs. IT

Priority is on reliability and integrity of the system.

Architectures are of proprietary nature and consist of isolated, task specific systems.

End-points are of heterogeneous make and task specific with long lifespans

Outcomes are physical



Priority is pervasiveness of data and confidentiality of such data.

Architectures are ubiquitous in nature and consist of mutli-tiered systems to encourage wide accessibility

End-points are of homogenous make and multi-purpose with short lifespans

Outcomes are digital

Compliance & Standards

Certified Products, Architectures and Solution Delivery

ISA/IEC 62443: 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 (i.e. asset owner)
- System integrators
- Security practitioners
- ICS product/systems vendors

**Equivalence to ISO 27001 and NIST Cybersecurity Framework*

Strategic Advisor and Security Practioner

BEFORE

Identify & Protect

- Asset Inventory Services
- Qualified Patch Management
- Vulnerability and Risk Assessments
- ICS Security Zone and Countermeasure Deployment

DURING

Detect

- Real-Time Threat Detection Services
- Remote Monitoring and Administration Services
- Incident Handling and Response
- Incident Response and Disaster Recovery Planning Services

AFTER

Respond & Recover

- Backup and Recovery Solutions

BUILD A SECURE, ROBUST, FUTURE-READY NETWORK FOR YOUR CONNECTED ENTERPRISE

ASSESS — DESIGN — IMPLEMENT — MONITOR

Rockwell Automation

Trusted Supplier

New Security Capabilities

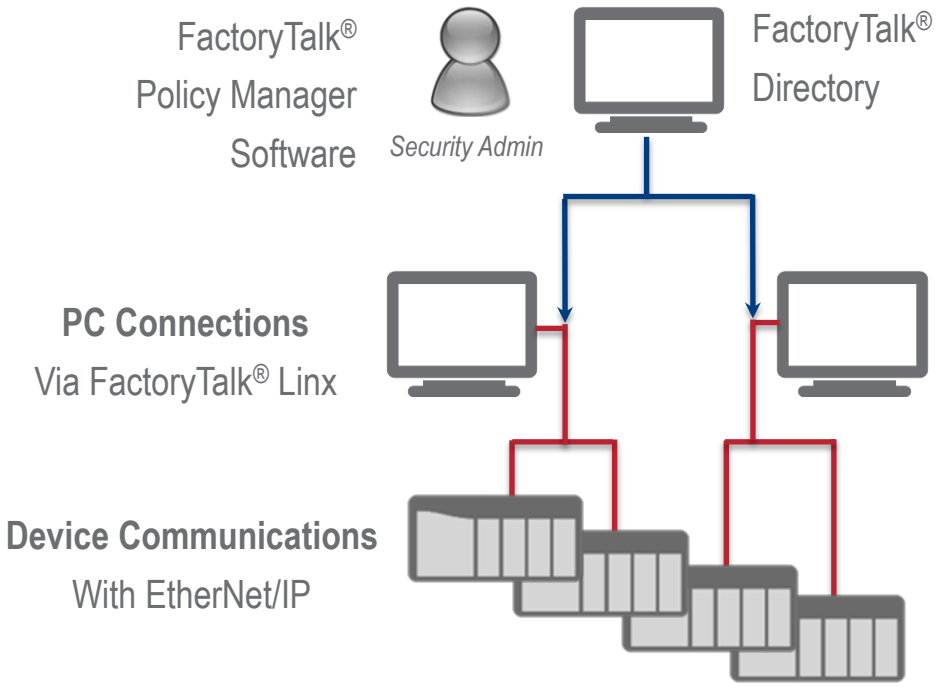
Secure communications with EtherNet/IP

- **Authentication** – helps prevent unauthorized devices from establishing connections
- **Integrity** – helps prevent tampering or modification of communications
- **Confidentiality** – helps prevent snooping or disclosure of data

Notable features:

- **System management**
  - Easily create and deploy security policies to many devices, all at once
- **Micro-segmentation**
  - Segment your automation application into smaller cell/zones.
- **Device-based firewall**
  - Enable/disable available ports/protocols of devices (ie./ HTTP/HTTPS)
- **Legacy Systems Support**
  - Whitelisting – authorize specific communications based on IP address
  - Retrofit 1756 based systems with the new 1756-EN4TR
  - Leverage a “proxy device” in front of legacy products (Future)

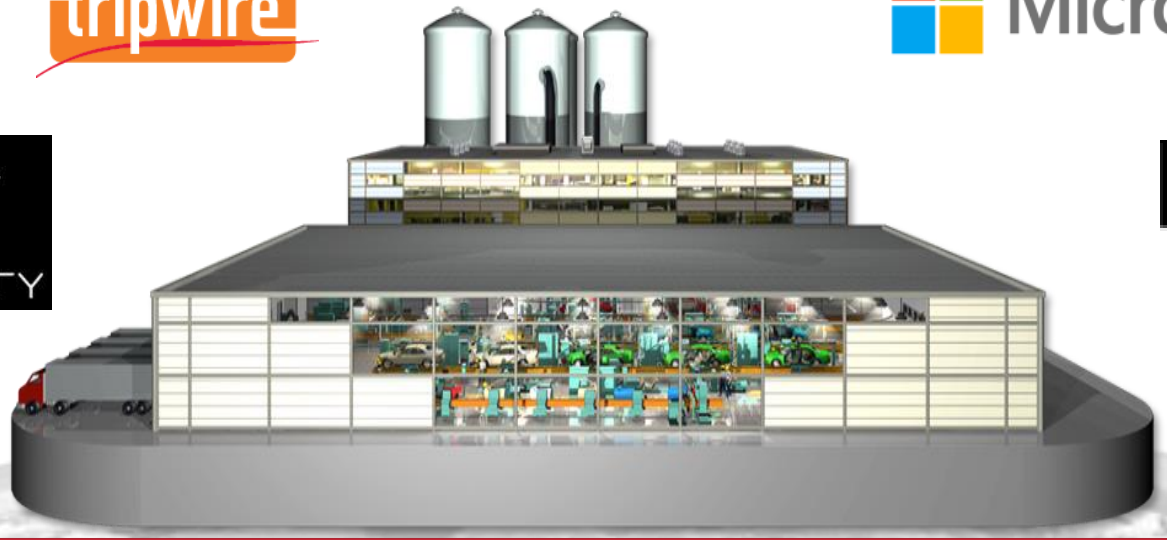
System Components



Industry-Leading Partners

Complimentary Solutions

Rockwell Automation PartnerNetwork™



ROCKWELL AUTOMATION & PARTNER **PORTFOLIO**

Rockwell Automation	Cisco	Claroty	Microsoft	Panduit	VMware	PartnerNetwork™ program
Integrated Control & Information	Wireless, Security, Switching & Routing	Industrial Control System Threat Detection	Operating Systems, Database / Cloud Infrastructure, & Application Security	Physical Layer Network Infrastructure, Zone Enclosures	Data Center Virtualization	Alliances, Encompass™ partner, Distributors, System Integrators, OEMs

Rockwell Automation

Thank you

www.rockwellautomation.com