An end-to-end approach to OT Cybersecurity

Stéphane Palumbo, System Engineer, Belux

What is Operational Technology (OT)

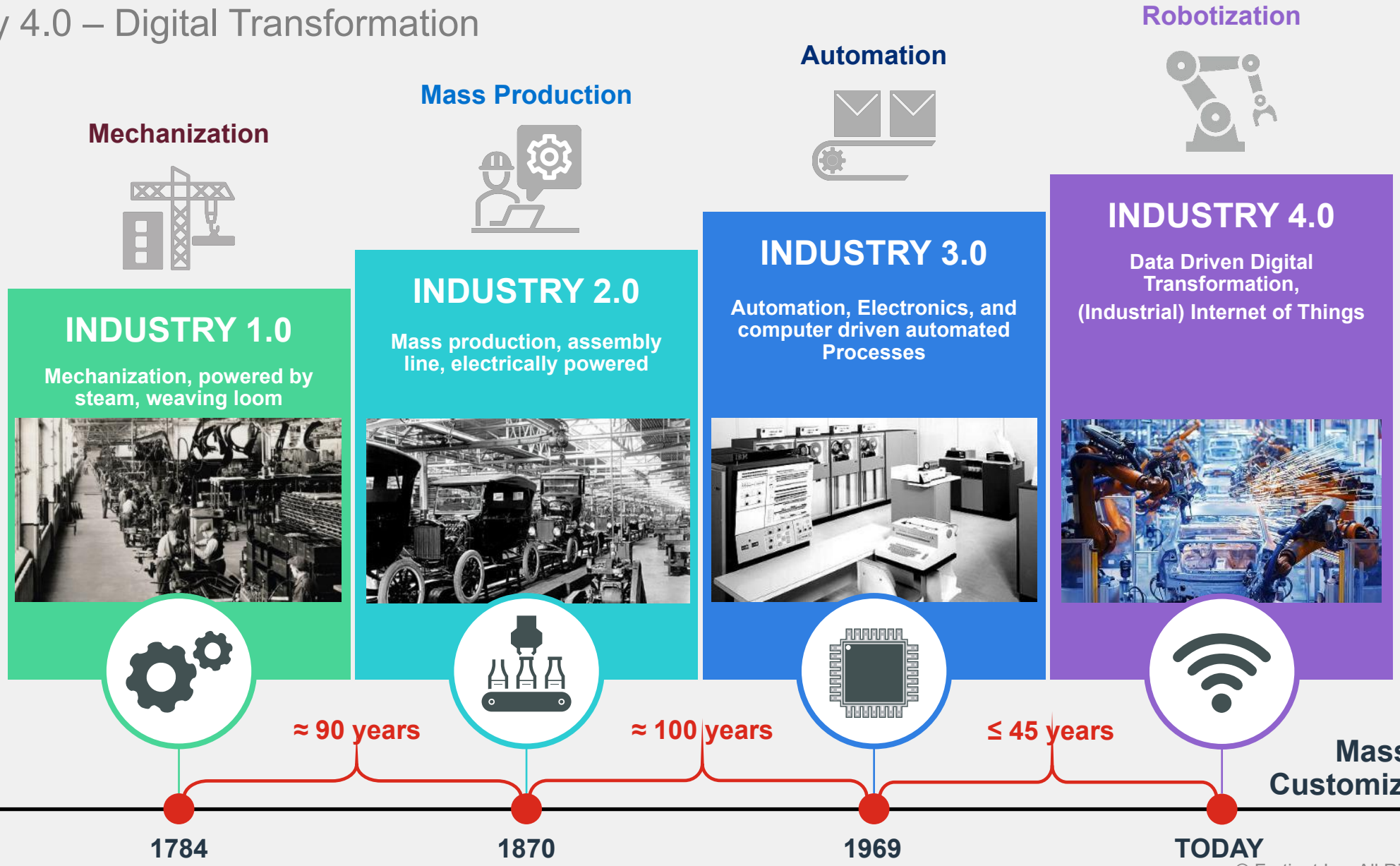
Used by

Diverse Industries
Often “critical” infrastructures

All environmental conditions
Harsh (heat, moisture, vibration); Office & Data Center

Operational Technology (OT)

Industry 4.0 – Digital Transformation

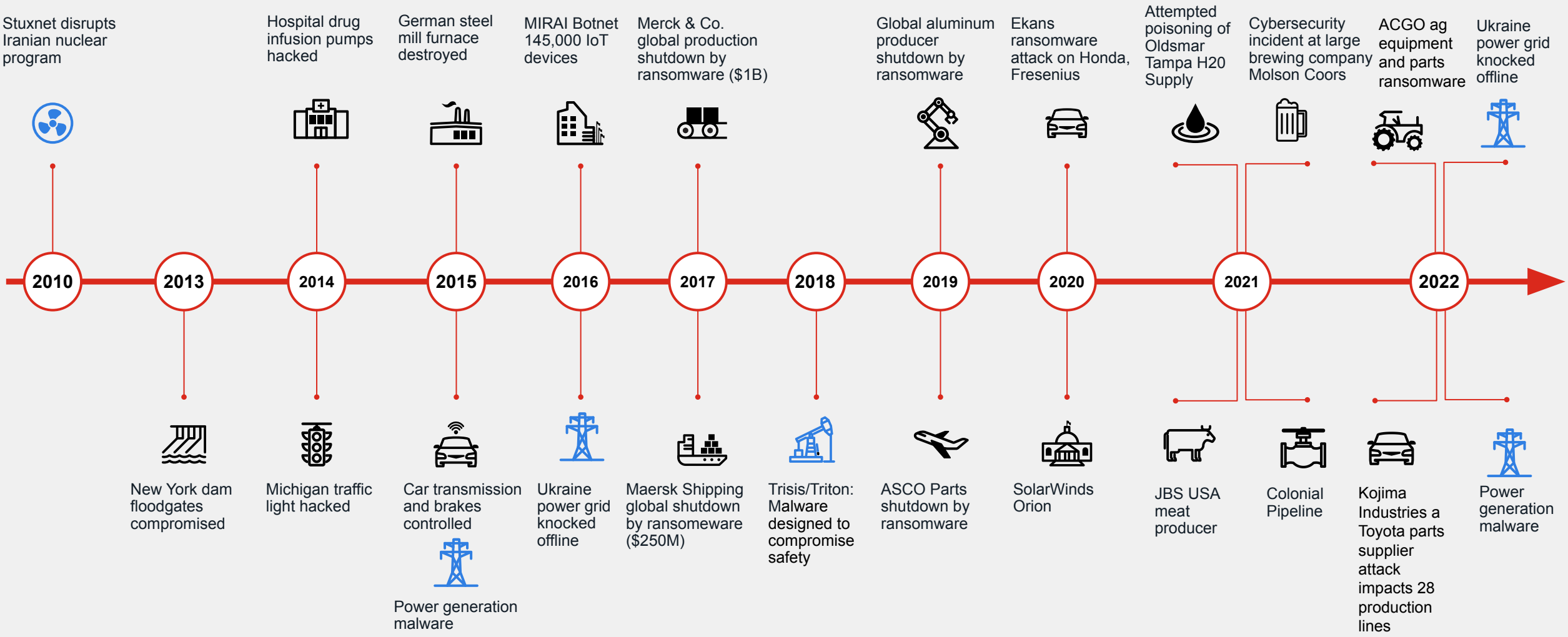


Common Myths Regarding OT Security

1. We don’t connect to the Internet
2. Our control systems are behind a Firewall
3. Hackers don’t understand control systems
4. Our facility is not a target
5. Our traditional safety system will protect us

OT Infrastructure Attacks Are Getting Worse

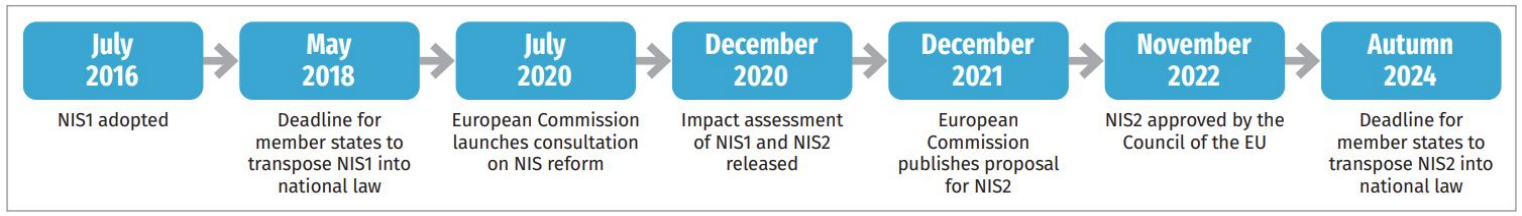
Attacks are increasing in frequency and impact



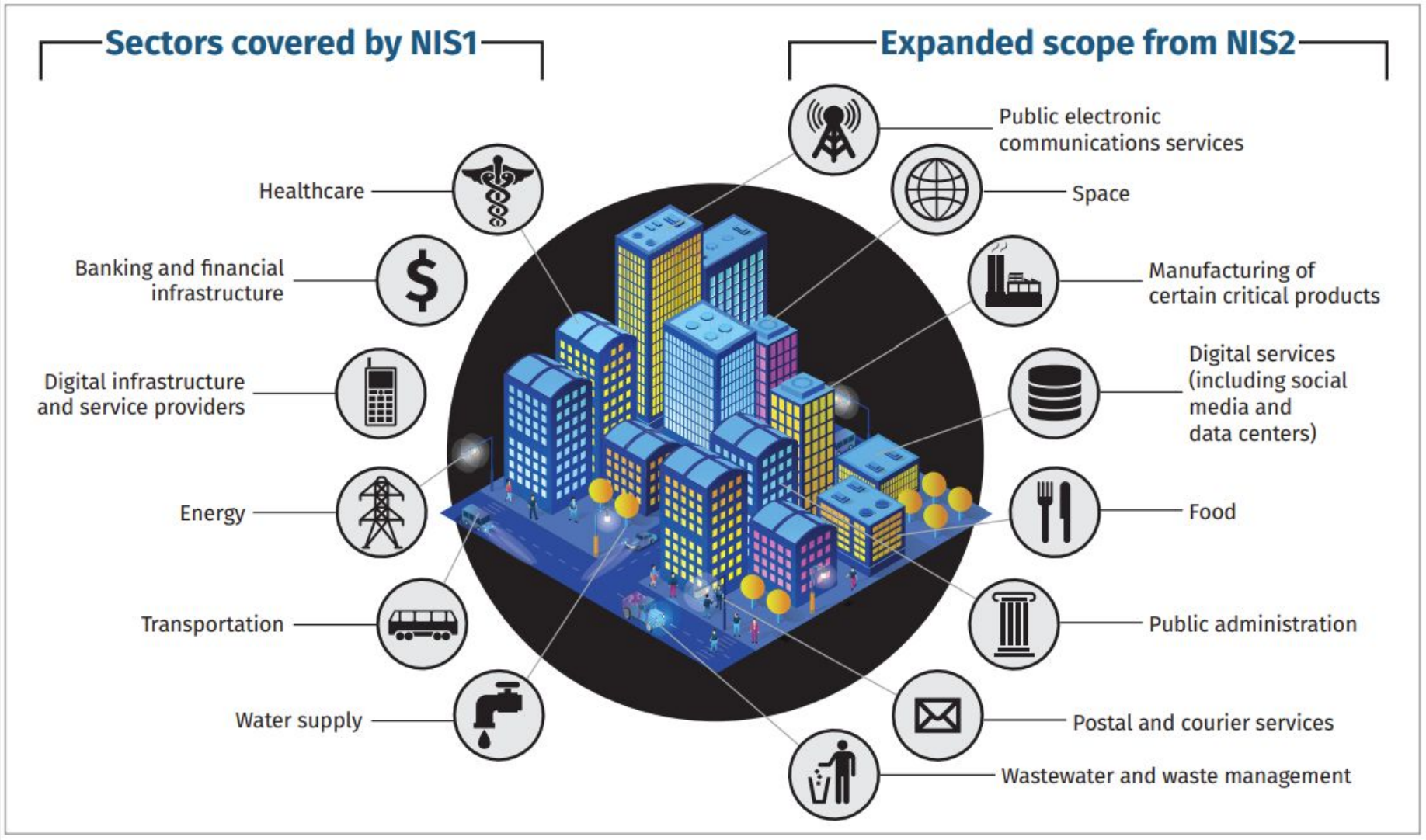
Securing Operational Technology Challenges

- Digital Transformation (Industry 4.0) initiatives driving **IT-OT network convergence**
- Increasing adoption of **5G, IoT, and Cloud**
- **Remote access** requirements for third-parties and employees
- Most industrial control systems **lack security by design**
- The **attack surface** for cyber-physical assets is expanding, air-gap protection is diminishing
- Asset owners' **reliance on OEMs and SIs** exposes critical systems to additional risks

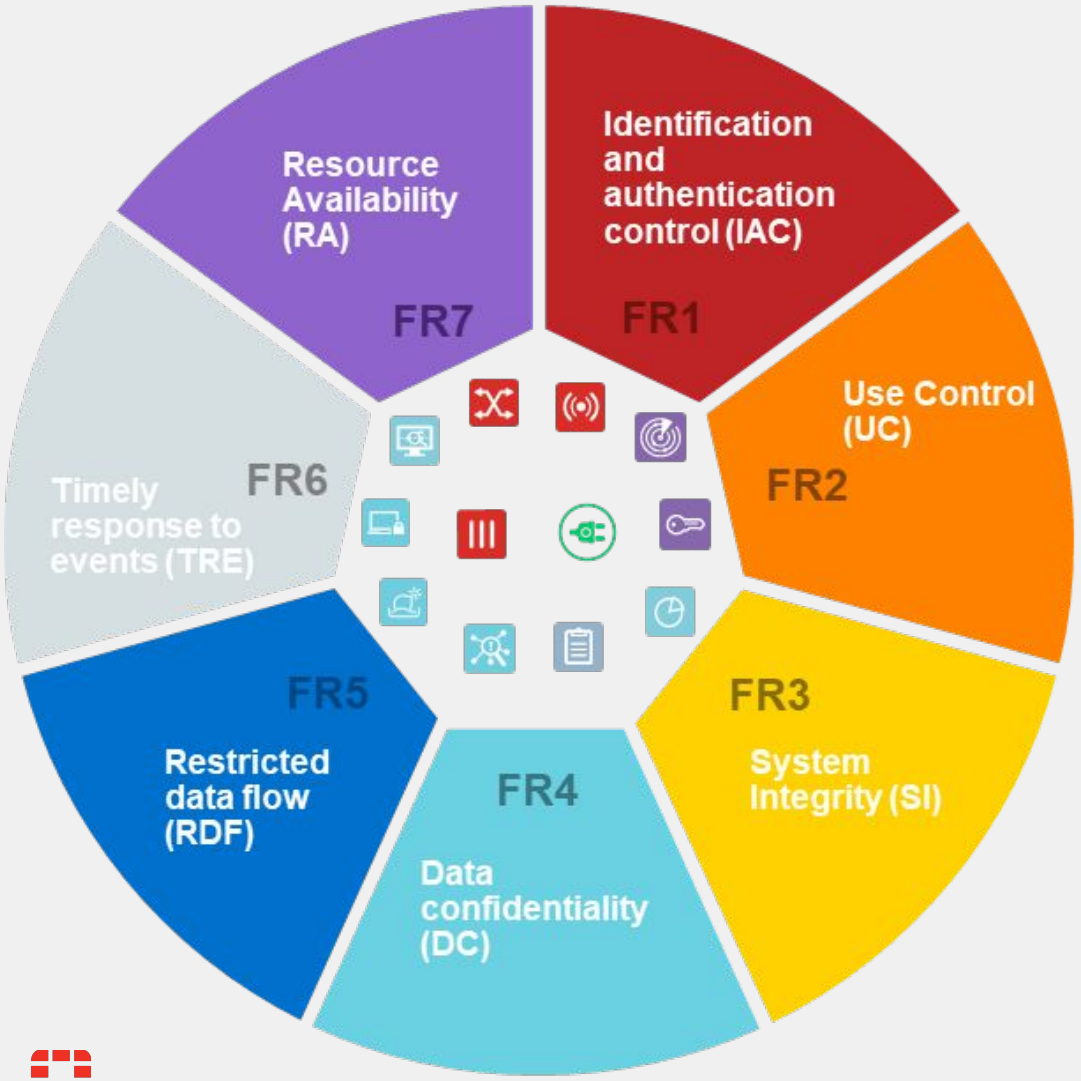
NIS 2 Compliance

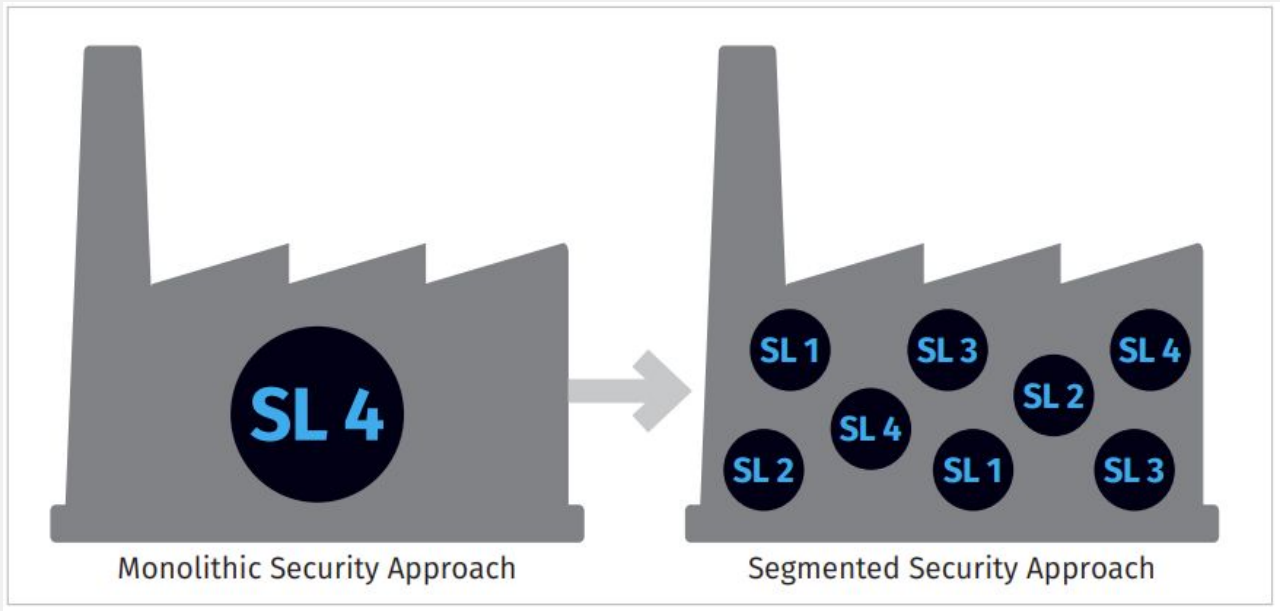


...and ISA/IEC 62443, NIST SP 800-82, NISTIR 7628, NERC CIP, IEC 62351, API 1164



IEC 62443 – Applying Risk and Safety principles

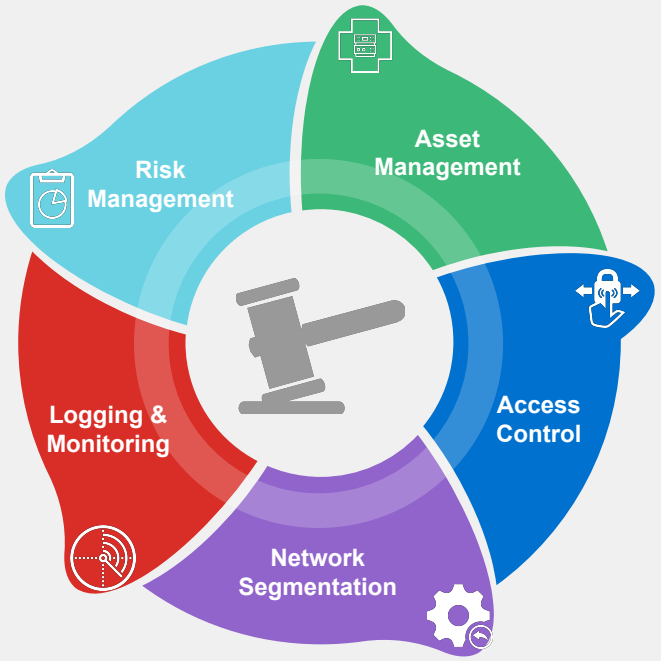




SANS Effective ICS Cybersecurity Using the IEC 62443 Standard

Alignment with OT standards & guidelines

Meet compliance requirements with Fortinet Security Fabric



NIS 2 Pillars

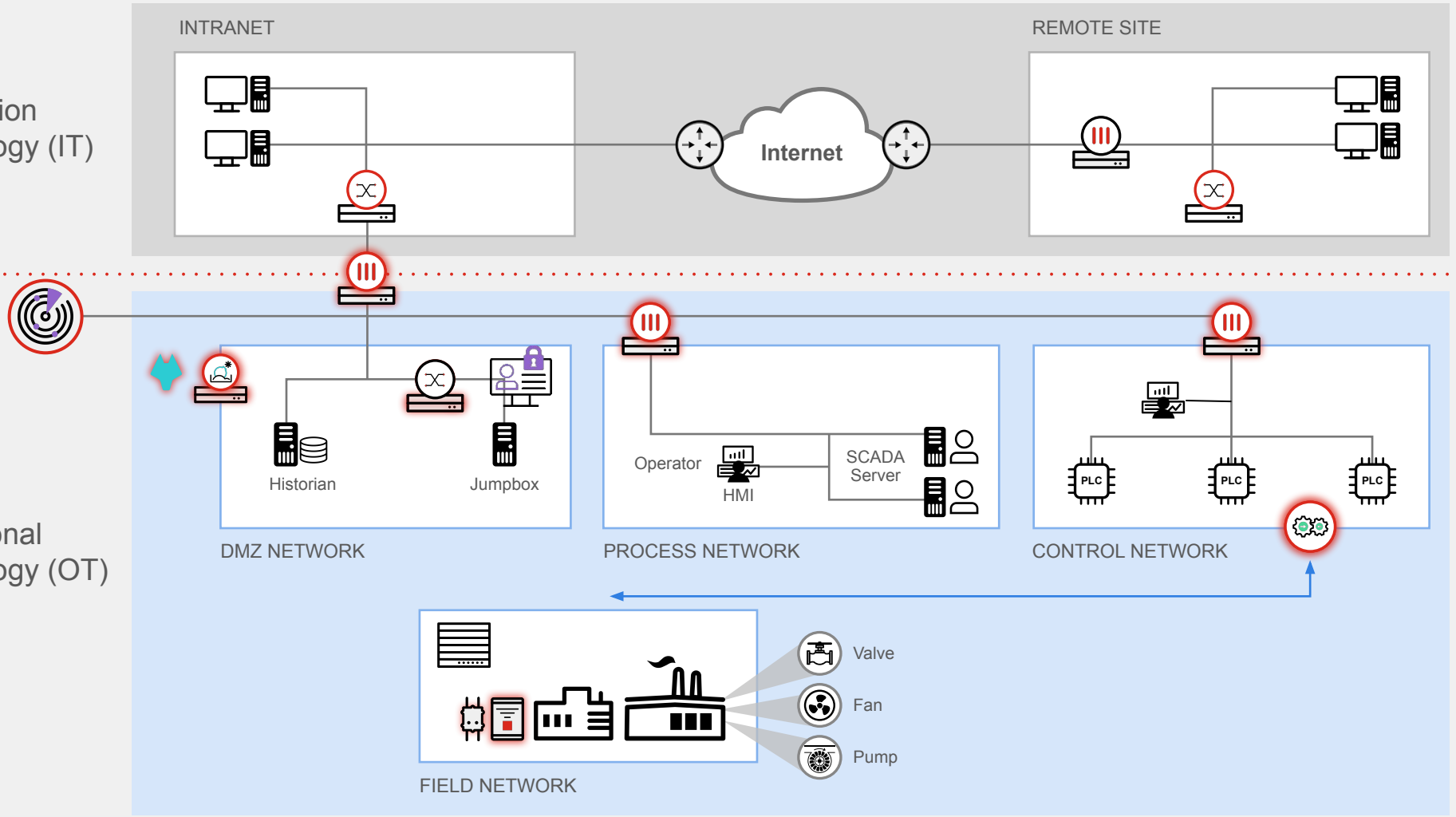
Asset Management	SIEM, NAC, NGFW
(Remote) Access Control	NGFW, NAC, FAuth, Client, 2FA Token, PAM
Segmentation, Protection & Response	NGFW, Switch, WIFI, EDR, Extender
Events, Alerts and Incident Detection	SOAR, SIEM, Analyzer, Deceptor, SandBox
Risk Management	Manager, SIEM, Analyzer, Recon

- Single Pane Management
- Threat Intelligence
- Interoperability

The Basics – Addressing Critical Controls in OT and IT

Information Technology (IT)

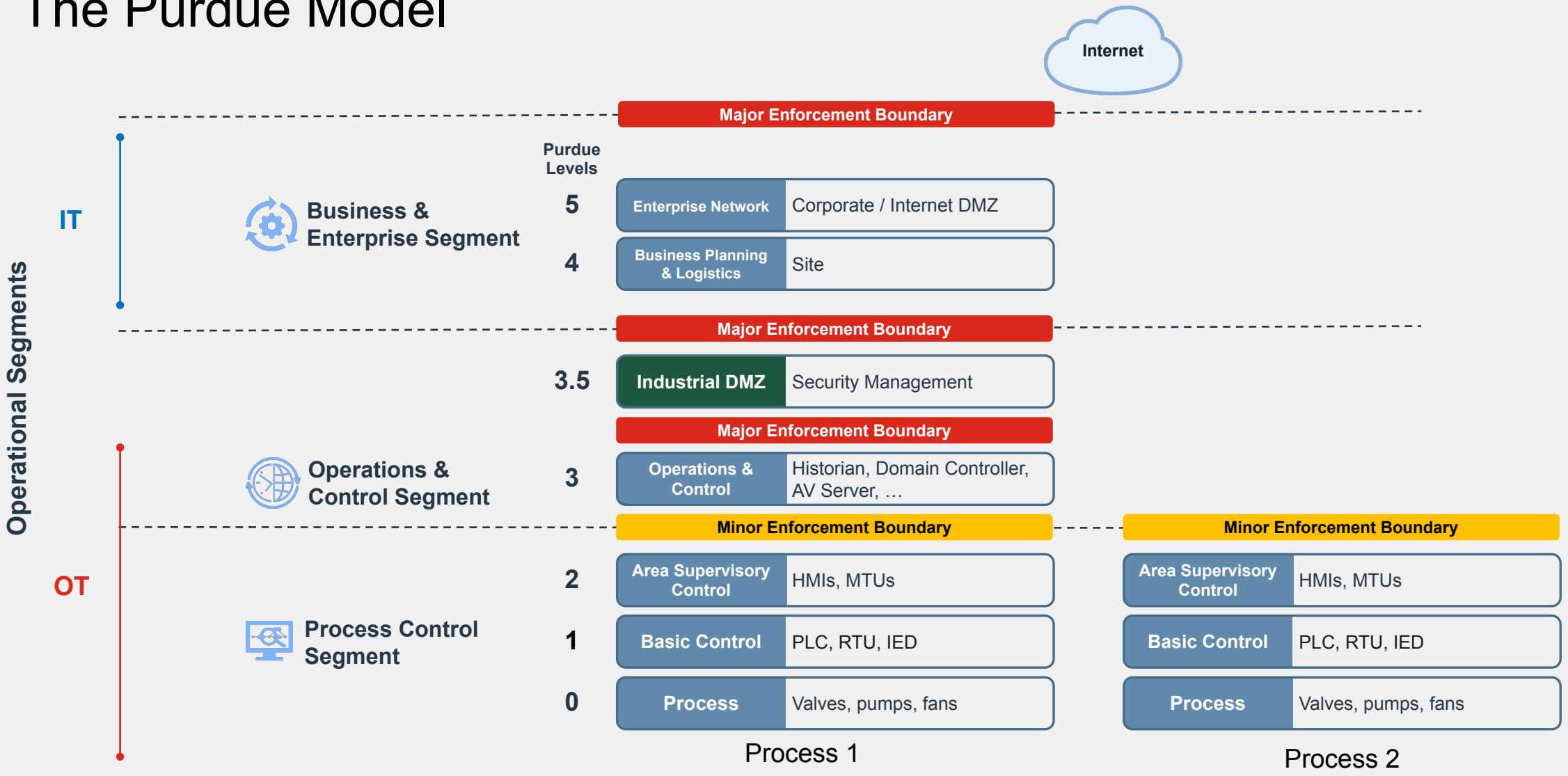
Operational Technology (OT)



- Segmentation
- Visibility in IT and OT
- Remote Access + PAM
- Application Control + Virtual Patching
- APT + Early Reconnaissance
- Risk Management + Compliance

A framework for segmenting OT

The Purdue Model




FORTINET