FORTINET

Verkko- ja tietoturva arkkitehtuuri OT-järjestelmille

Esa Kuusisto

Systems Engineer – OT

ekuusisto@fortinet.com

R3-06-2021

Agenda

- Introduction
- Architectural Models
- Requirement Relations
  - Katakri
  - Pitukri
- Practical Solutions
- Conclusions

Who is Fortinet?

For over 20 years, Fortinet's mission has been to secure people, devices, and data everywhere.

We have been a driving force in the evolution of cybersecurity and the convergence of networking and security. Our network security solutions are the most deployed, most patented, and among the most validated in the industry.

Nasdaq 100
Nasdaq: FTNT
Publicly Traded

S&P 500
Nasdaq: FTNT
GAAP Profitable

BBB+ Baa1
Security Investment Grade Rating
Financially Stable

$4.18B
FY2021 Billing
Top 3

50+
Integrated Fabric Products
Broadest Attack Surface Coverage

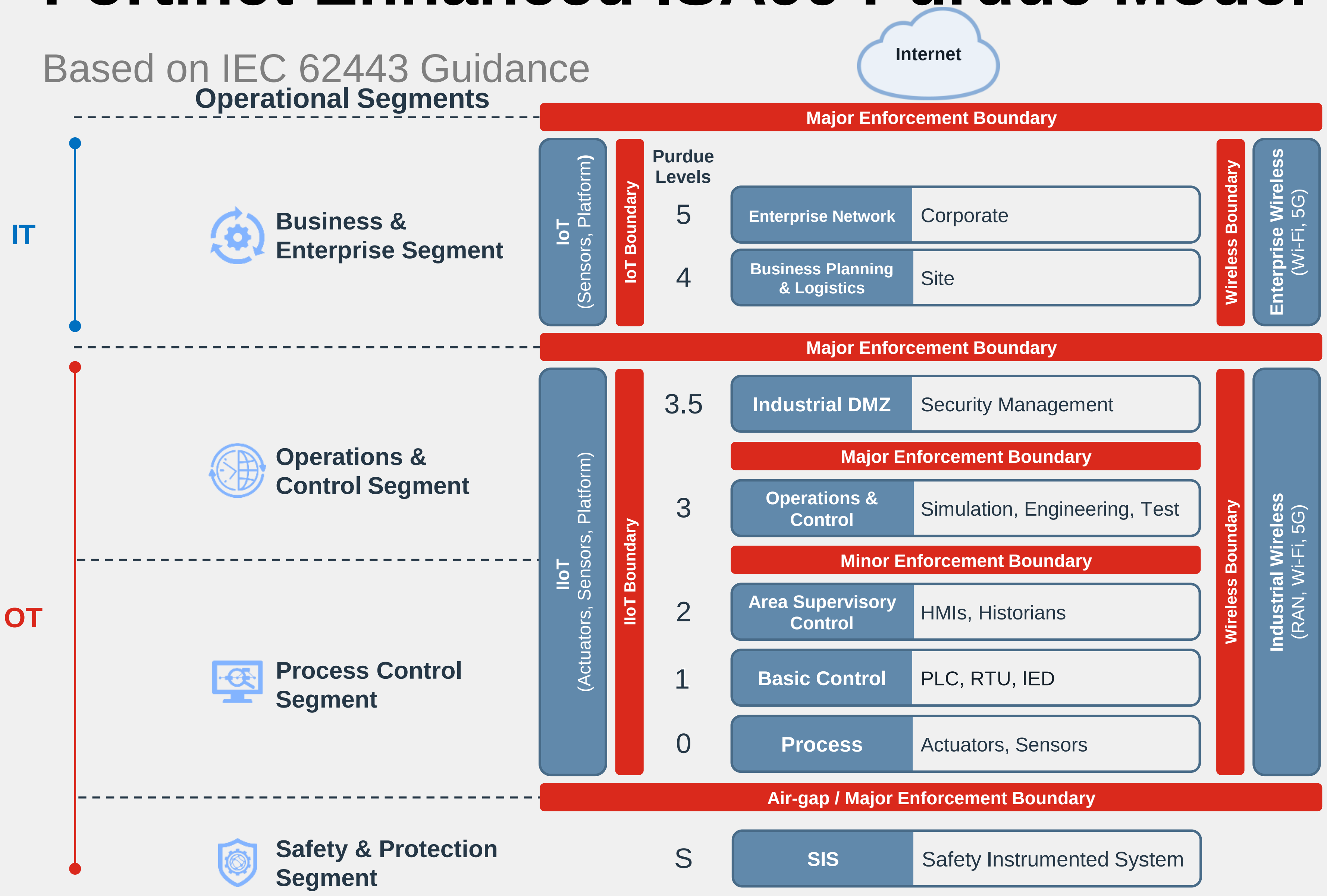
ASIC
Security Processing Unit (SPU)
High Performance

Architecture models

- Different models eg. Purdue, IEC 62443, IAEA Cyber Security
- Not to be confused with data protection/classification levels
    - In some examples there are protection level 1-4 where level 1 is lowest and 4th is highest

Fortinet Enhanced ISA99 Purdue Model

Based on IEC 62443 Guidance



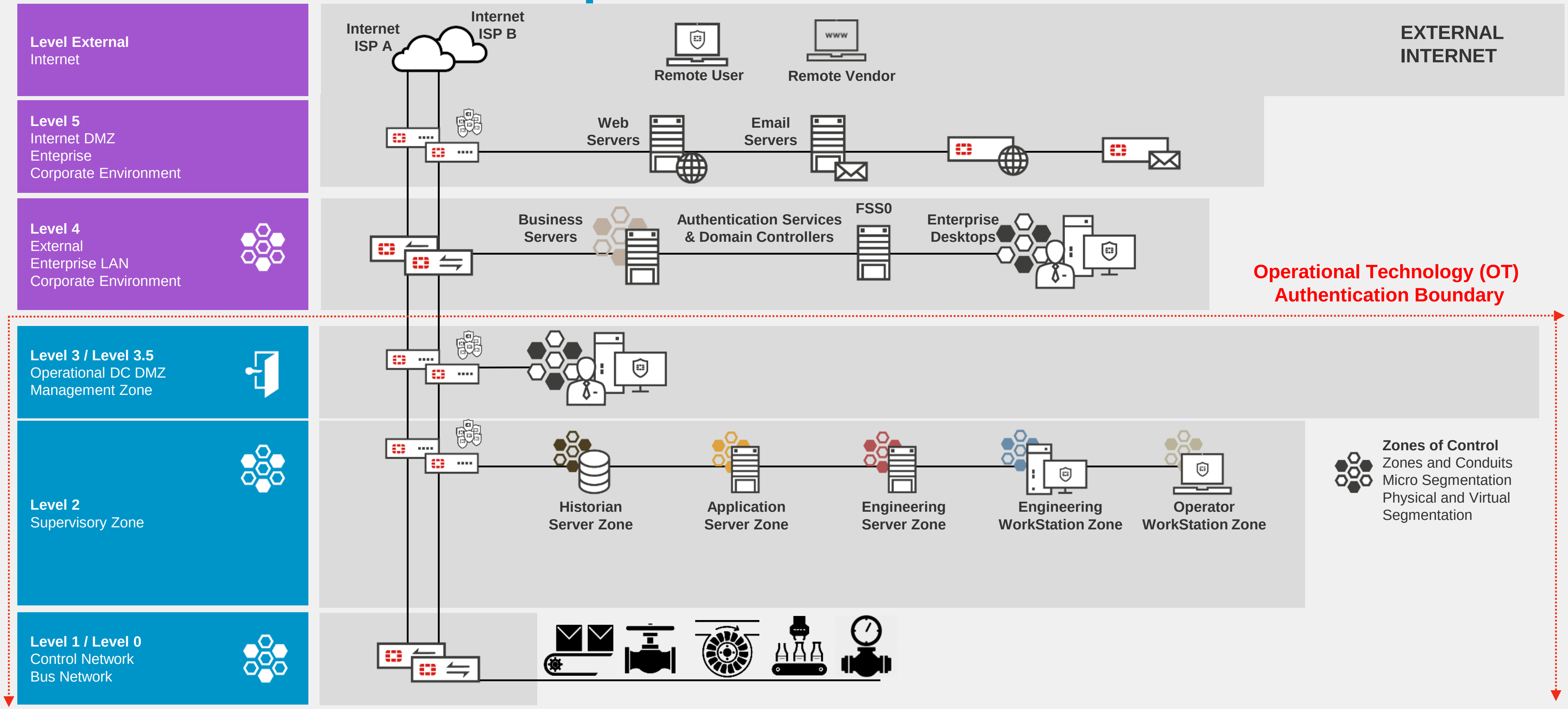
Operational Segments
IT
OT
Business & Enterprise Segment
Operations & Control Segment
Process Control Segment
Safety & Protection Segment
Internet
Major Enforcement Boundary
IoT (Sensors, Platform)
IoT Boundary
Wireless Boundary
Enterprise Wireless (Wi-Fi, 5G)
Major Enforcement Boundary
IIoT (Actuators, Sensors, Platform)
IIoT Boundary
Wireless Boundary
Industrial Wireless (RAN, Wi-Fi, 5G)
Air-gap / Major Enforcement Boundary

Purdue Levels		
5	Enterprise Network	Corporate
4	Business Planning & Logistics	Site
3.5	Industrial DMZ	Security Management
	Major Enforcement Boundary	
3	Operations & Control	Simulation, Engineering, Test
	Minor Enforcement Boundary	
2	Area Supervisory Control	HMIs, Historians
1	Basic Control	PLC, RTU, IED
0	Process	Actuators, Sensors
S	SIS	Safety Instrumented System

Digital Assets

Enforcement Boundaries

IEC 62443 Compliant Solution Architecture



Level External
Internet

Level 5
Internet DMZ
Enteprise
Corporate Environment

Level 4
External
Enterprise LAN
Corporate Environment

Level 3 / Level 3.5
Operational DC DMZ
Management Zone

Level 2
Supervisory Zone

Level 1 / Level 0
Control Network
Bus Network

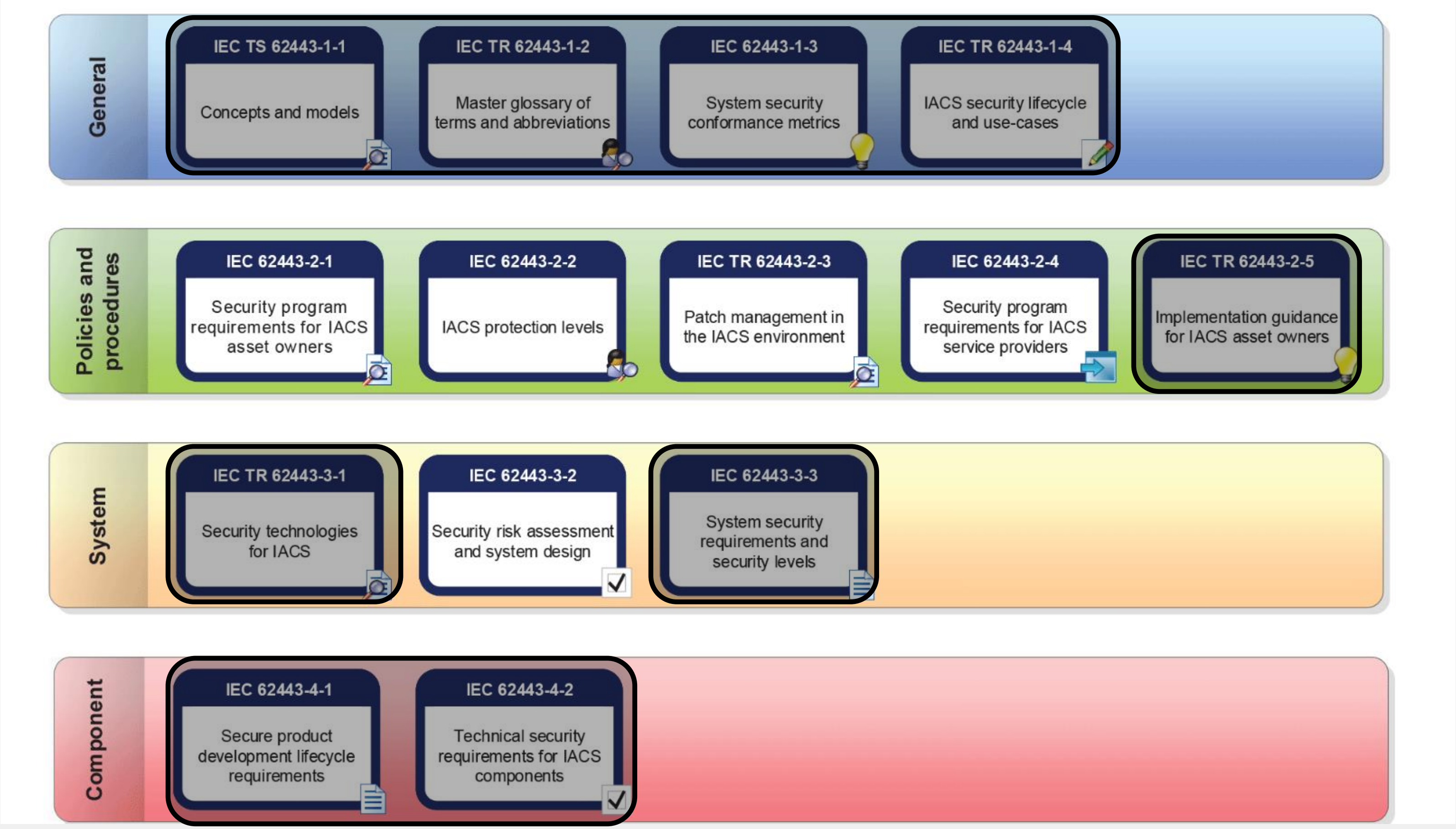
EXTERNAL INTERNET

Operational Technology (OT) Authentication Boundary

Zones of Control
Zones and Conduits
Micro Segmentation
Physical and Virtual
Segmentation

IEC 62443 Compliant

Support asset owners & system integrators with Defense-In-Depth Cybersecurity



General

- IEC TS 62443-1-1: Concepts and models
- IEC TR 62443-1-2: Master glossary of terms and abbreviations
- IEC 62443-1-3: System security conformance metrics
- IEC TR 62443-1-4: IACS security lifecycle and use-cases

Policies and procedures

- IEC 62443-2-1: Security program requirements for IACS asset owners
- IEC 62443-2-2: IACS protection levels
- IEC TR 62443-2-3: Patch management in the IACS environment
- IEC 62443-2-4: Security program requirements for IACS service providers
- IEC TR 62443-2-5: Implementation guidance for IACS asset owners

System

- IEC TR 62443-3-1: Security technologies for IACS
- IEC 62443-3-2: Security risk assessment and system design
- IEC 62443-3-3: System security requirements and security levels

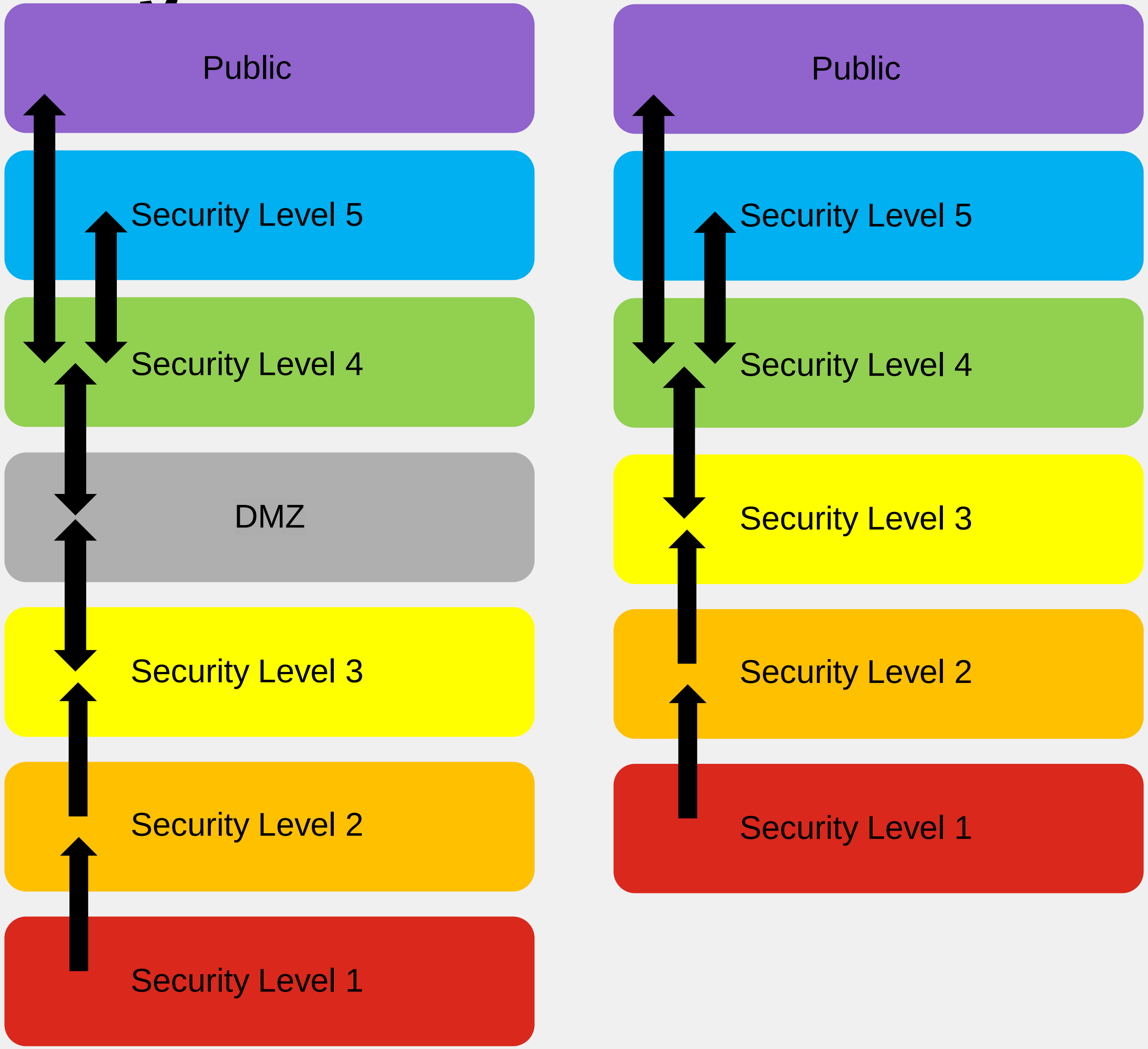
Component

- IEC 62443-4-1: Secure product development lifecycle requirements
- IEC 62443-4-2: Technical security requirements for IACS components

IEC 62443 Zones, Conduits and Security Levels

- **SL 4**: Protection against intentional violation using sophisticated means with extended resources, IACS specific skills, and high motivation
- **SL 3**: Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills, and moderate motivation
- **SL 2:** Protection against intentional violation using simple means with low resources, generic skills, and low motivation
- **SL 1:** Protection against casual or coincidental violation
- **Zones**: A grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence.
- **Conduits:** Groupings of assets dedicated exclusively to communications and which share the same security requirements. Conduits can also be used to describe tunnels communicating between zones.

Security Level Design IAEA

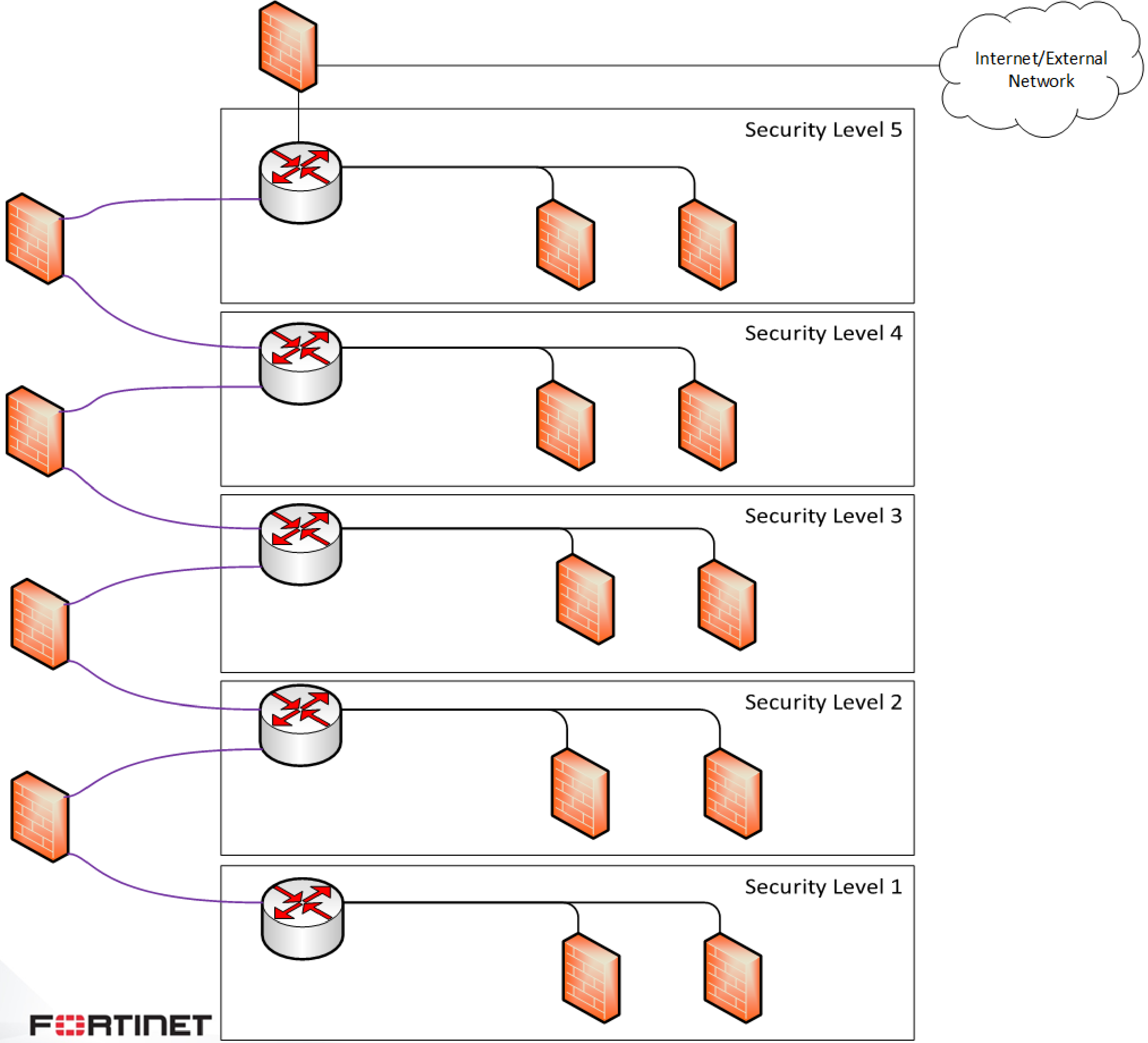


Requirement Relations

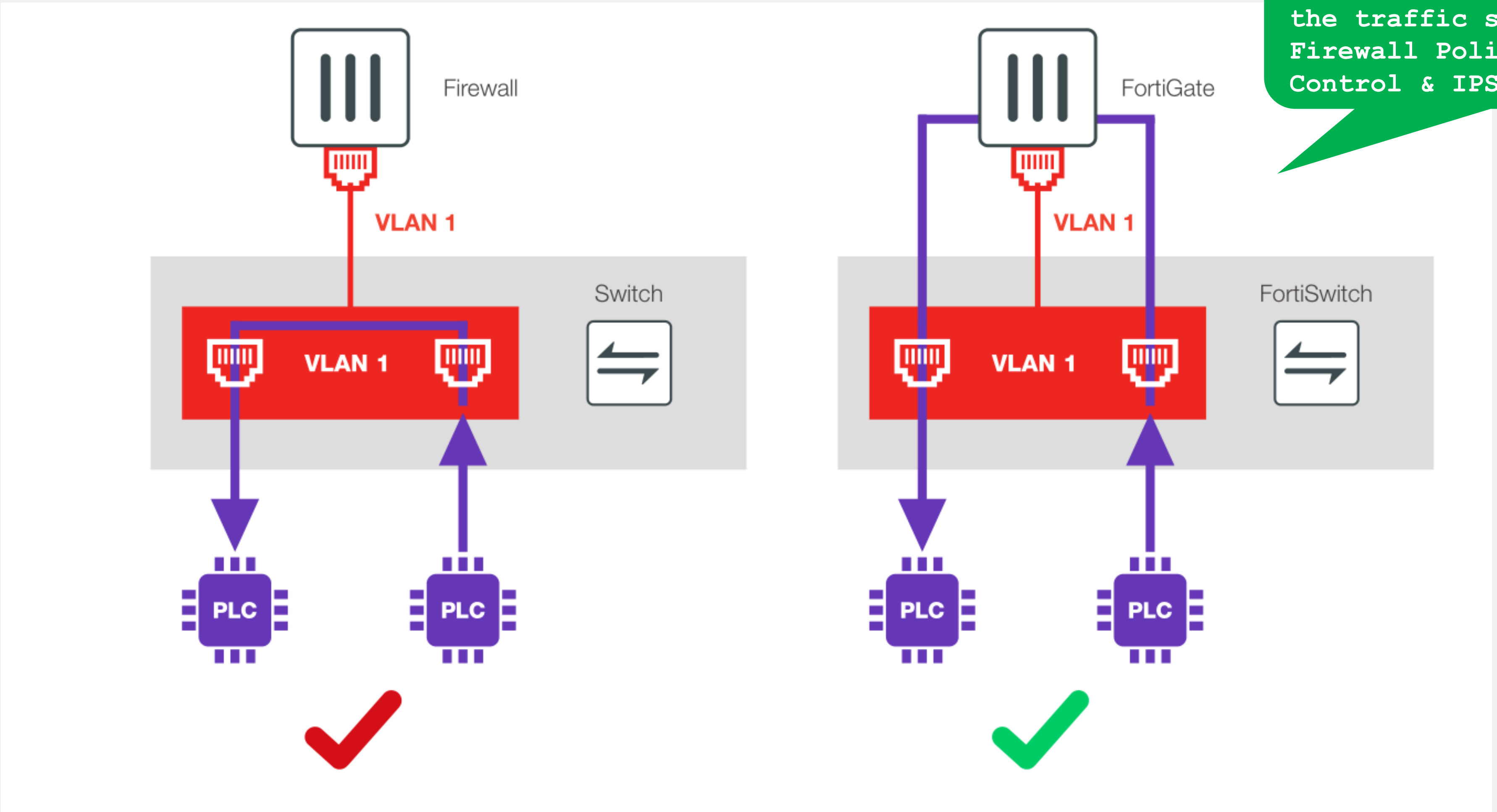
	Katakri	Pitukri	Purdue
Public			
Security Level 5		Cloud*	Level 5
Security Level 4	TL IV		Level 4
Security Level 3	TL III		Level 3/3.5
Security Level 2	TL II		Level 2
Security Level 1	TL I		Level 0/1

- *Cloud Locations
  - Finland
  - EU
  - World

Practical Network Design



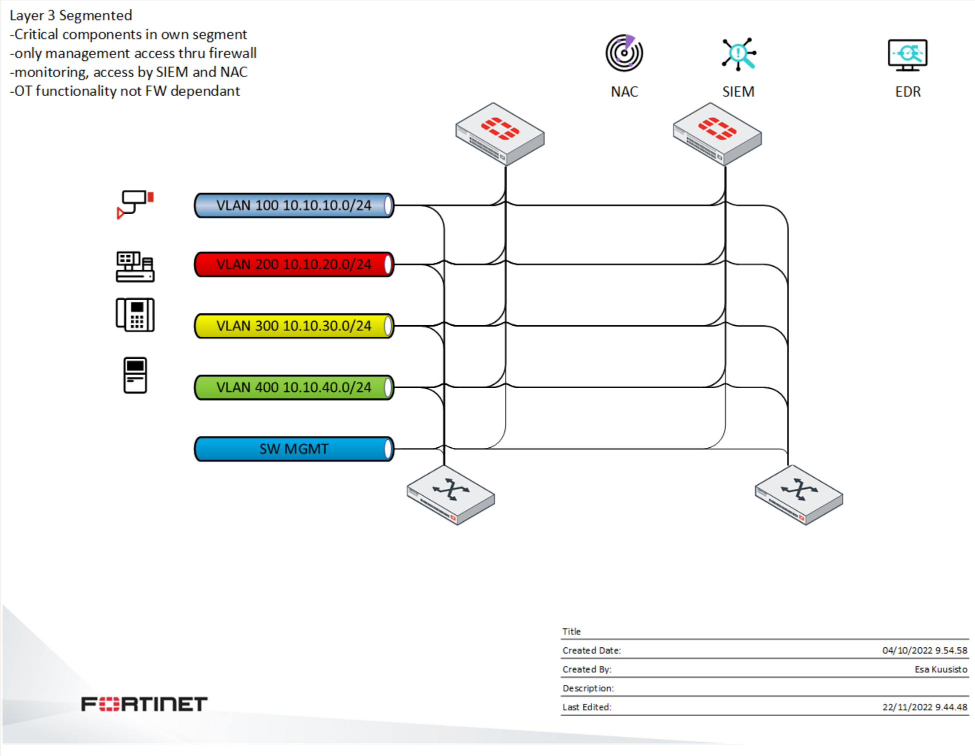
Segmentation



Fine grained control enforcement on FortiGate with the traffic subjected to IP Firewall Policy, Application Control & IPS.

Normal VLAN routing vs. microsegmentation using Fortinet FortiSwitch and FortiGate.

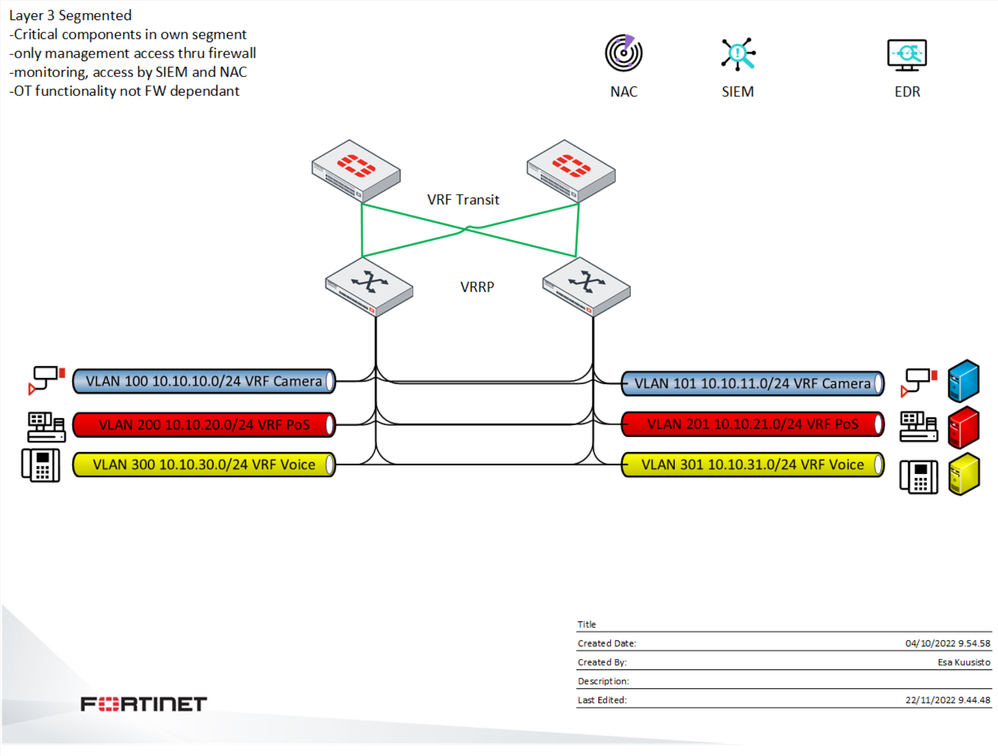
Network Layer 3 segmentation



Layer 3 Segmented
-Critical components in own segment
-only management access thru firewall
-monitoring, access by SIEM and NAC
-OT functionality not FW dependant

Title
Created Date: 04/10/2022 9.54.58
Created By: Esa Kuusisto
Description:
Last Edited: 22/11/2022 9.44.48

Simple Layer 3 network



Layer 3 Segmented
-Critical components in own segment
-only management access thru firewall
-monitoring, access by SIEM and NAC
-OT functionality not FW dependant

NAC
SIEM
EDR
VRF Transit
VRRP
VLAN 100 10.10.10.0/24 VRF Camera
VLAN 200 10.10.20.0/24 VRF PoS
VLAN 300 10.10.30.0/24 VRF Voice
VLAN 101 10.10.11.0/24 VRF Camera
VLAN 201 10.10.21.0/24 VRF PoS
VLAN 301 10.10.31.0/24 VRF Voice
FERTINET

Title
Created Date: 04/10/2022 9.54.58
Created By: Esa Kuusisto
Description:
Last Edited: 22/11/2022 9.44.48

Layer 3 segmented network with VRFs

Conclusions

- Architectural model and data protection model must be defined
- Architectural design should contain target state and states between current and target
- Architectural changes are allowed
- Do not focus on techology solutions.

References

- IAEA
  - Conducting Computer Security Assessments at Nuclear Facilities
  - IAEA Nuclear Security Series No. 33-T
  - IAEA Nuclear Security Series No. 42-G
  - IAEA Nuclear Security Series No. 17-T (Rev. 1)
- https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf
- https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille https://verveindustrial.com/resources/blog/the-ultimate-guide-to-protecting-ot-systems-with-iec-62443/?submissionGuid=eabcd732-db2d-4242-ba8b-fffe58892aea

FORTINET®