FORTINET

SMART GRID FORUMS | Understanding IEC 62443

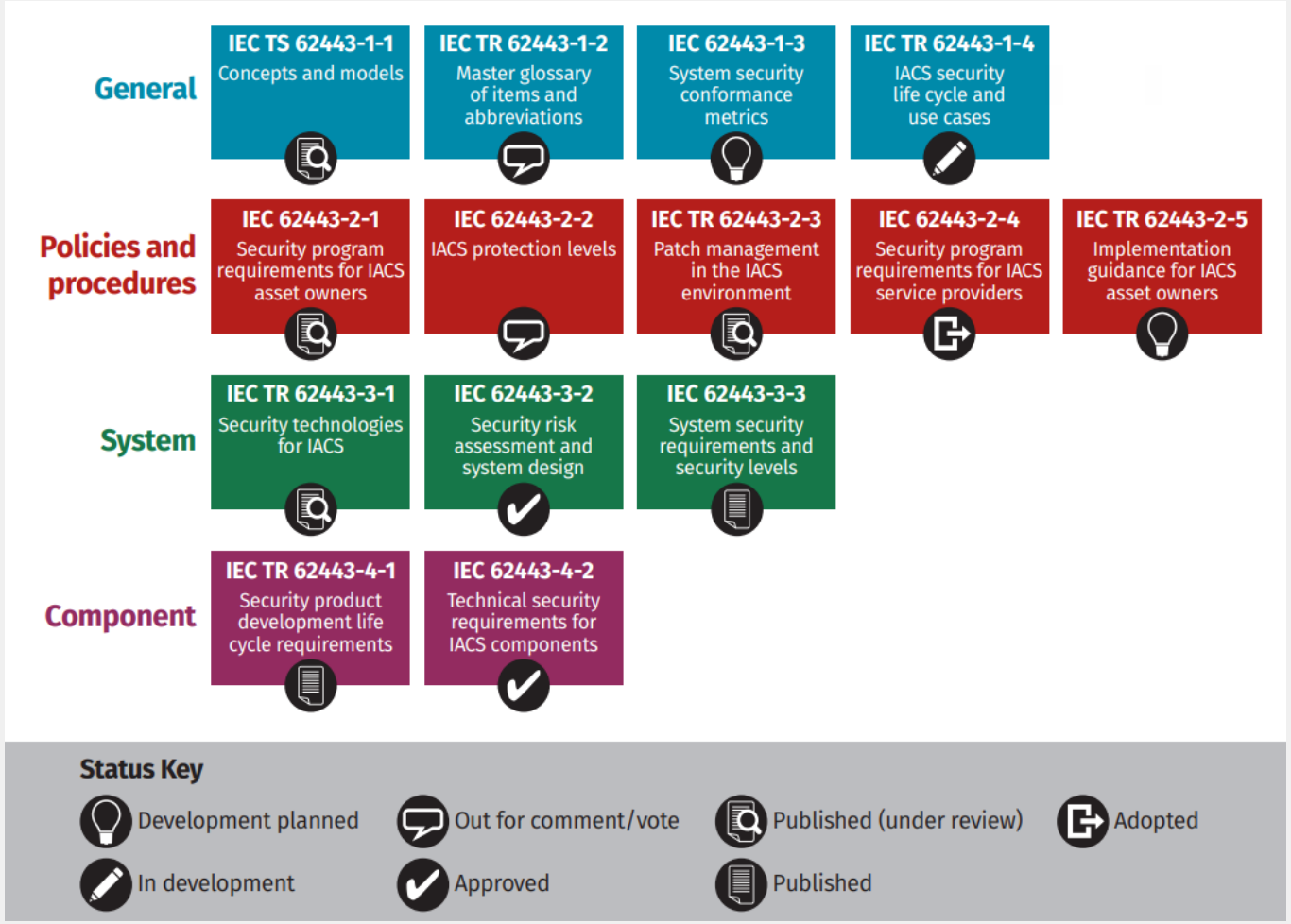
Adopting IEC 62443 across a wider range of power grid industrial automation control systems

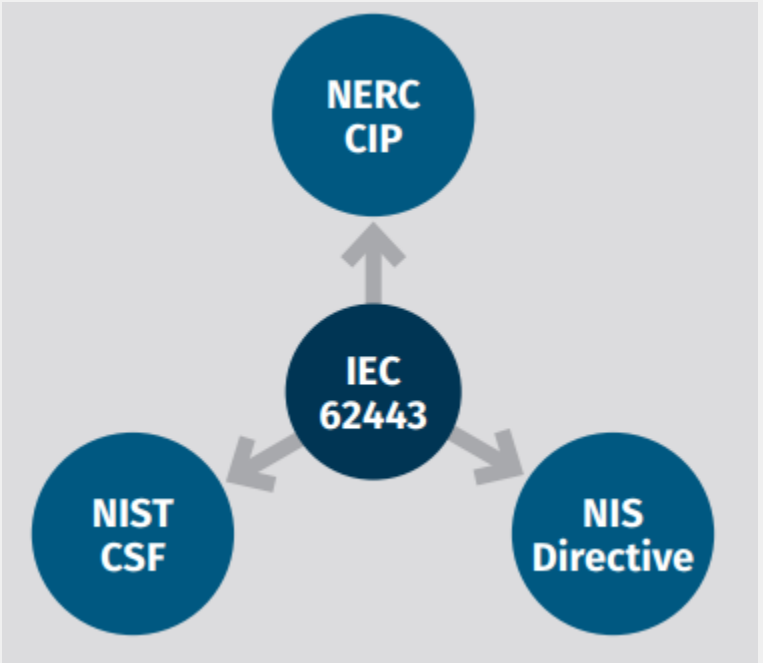
Wednesday 27th October 2021

Antoine d'Haussy – OT SME, Security Practice Head for EMEA

ISA/IEC 62243 Regulatory Compliance

How Product Vendors support Asset Owners and System Integrators?





SANS Institute – Managing ICS Security with IEC 62443 Standard

Compliance is an Ecosystem Responsability

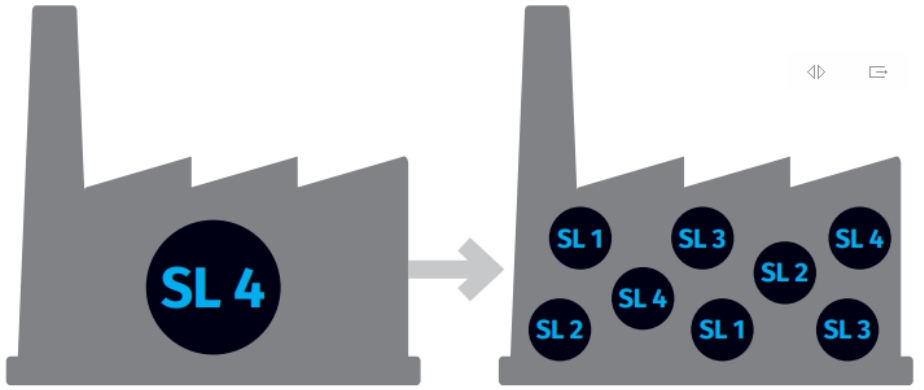
Foundational Requirements & Security Levels

Foundational Requirements (FRs)

- **FR1** Identification and authentication control (IAC)
- **FR2** Use control (UC)
- **FR3** System integrity (SI)
- **FR4** Data confidentiality (DC)
- **FR5** Restricted data flow (RDF)
- **FR6** Timely response to events (TRE)
- **FR7** Resource availability (RA)

SL 0	No specific requirements or security protection necessary
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means with low resoucres, generic skills and low motivation
SL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills and high motivation

SRs and REs			SL 1	SL 2	SL 3	SL 4
FR 1	**Identification and authentication control (IAC)**					
SR 1.1	Human user identification and authentication	5.3	✔	✔	✔	✔
SR 1.1 RE 1	Unique identification and authentication	5.3.3.1		✔	✔	✔
SR 1.1 RE 2	Multifactor authentication for untrusted networks	5.3.3.2			✔	✔
SR 1.1 RE 3	Multifactor authentication for all networks	5.3.3.3				✔
SR 1.2	Software process and device identification and authentication	5.4		✔	✔	✔
SR 1.2 RE 1	Unique identification and authentication	5.4.3.1			✔	✔
SR 1.3	Account management	5.5	✔	✔	✔	✔
SR 1.3 RE 1	Unified account management	5.5.3.1			✔	✔
SR 1.4	Identifier management	5.6	✔	✔	✔	✔



Monolithic Security Approach

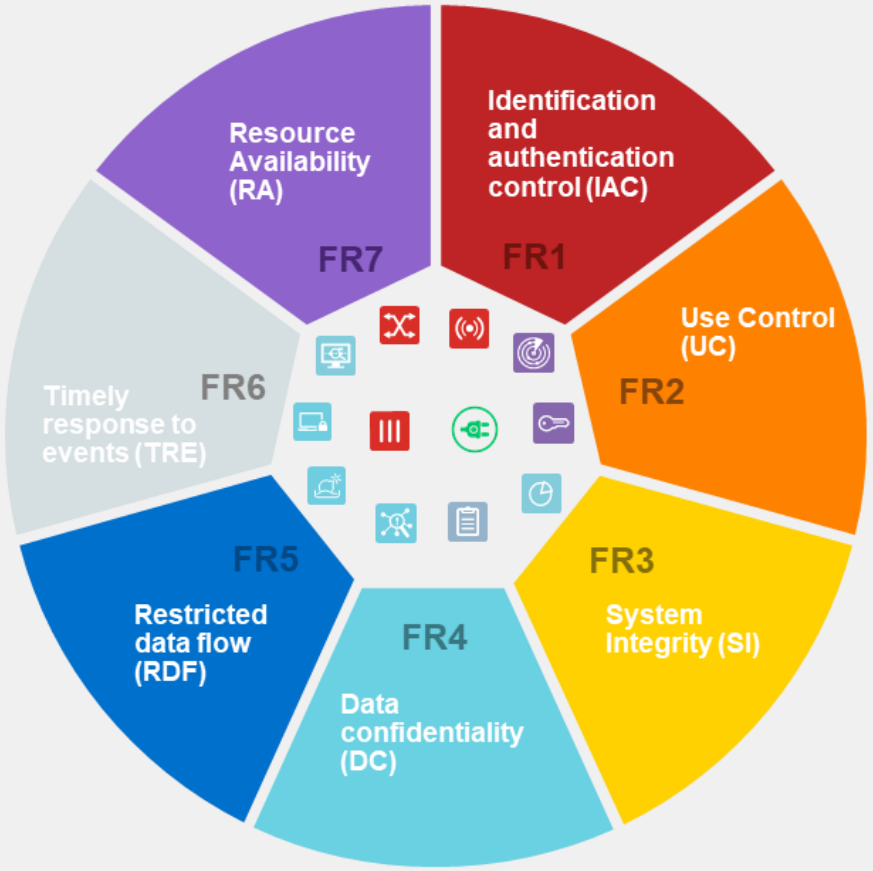
Segmented Security Approach

SANS Institute - Using the IEC 62443 Standard

SL are targets set against Risk Acceptance

Cyber Solutions mapping to IEC 62443

From Critical Controls to NextGen Cyber Security



IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 1 – Identification and Authentication					FR 1 Product Mapping: Fortigate, FortiWiFi/FortiAp, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager		
FR 1 – SRs and REs	Security Levels				Relevance	Compliance	Solution Description
	SL 1	SL 2	SL 3	SL 4	IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 1.1 – Human user identification and authentication	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator

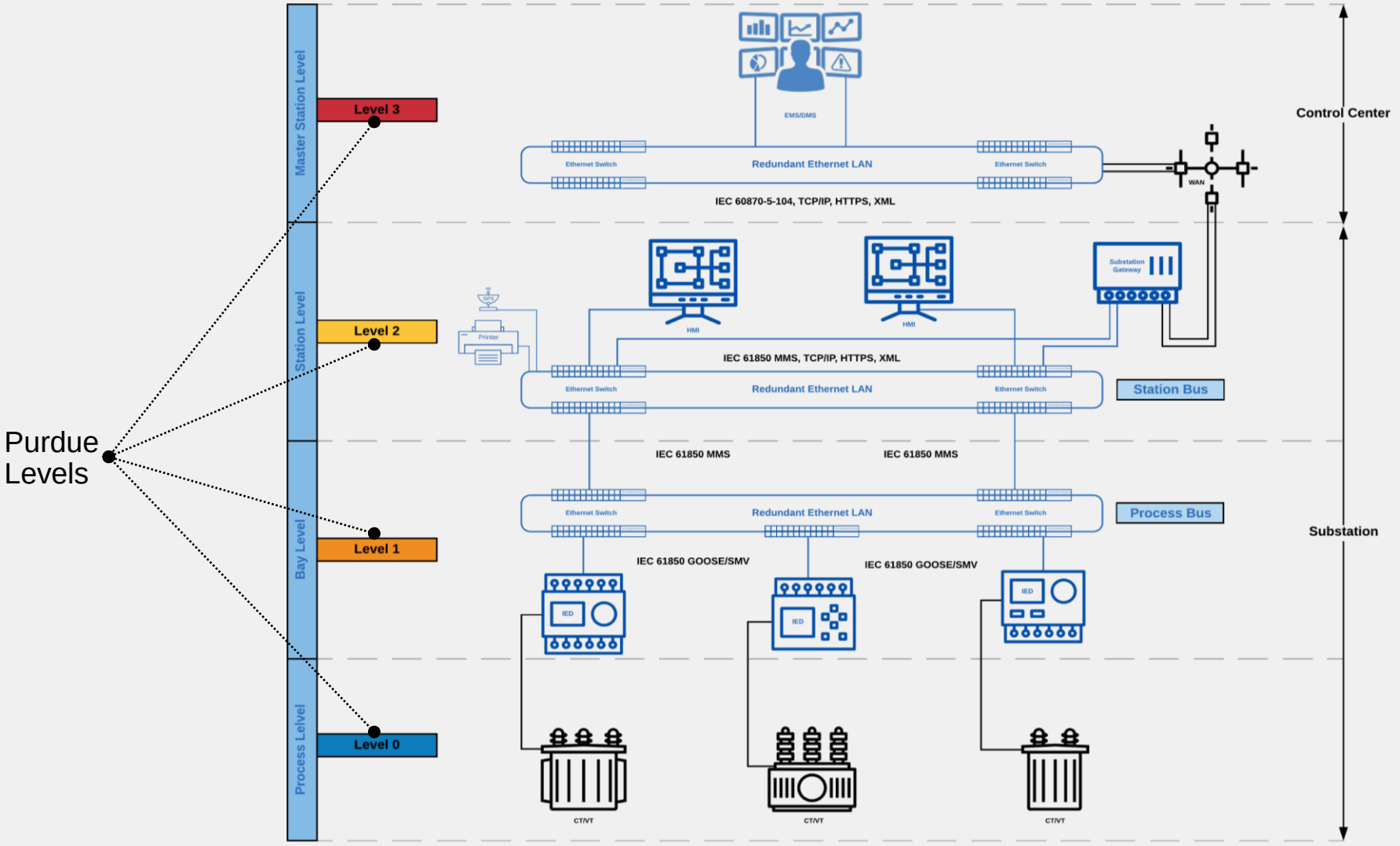
IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 5 – Restricted data flow (RDF)					FR 5 Product Mapping: FortiGate, FortiSwitch, FortiNAC, FortiClient, FortiEDR, FortiAnalyzer		
FR 5 – SRs and REs	Security Levels				Relevance	Compliance	Solution Description
	SL 1	SL 2	SL 3	SL 4	IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 5.1 – Network segmentation	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiNAC C: Product(s) integration and implementation of zones and

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 7 – Resource availability (RA)					FR 7 Product Mapping: FortiGate, FortiClient, FortiEDR, FortiAnalyzer, FortiM Fabric-Ready Partner Solutions		
FR 7 – SRs and REs	Security Levels				Relevance	Compliance	Solution Description
	SL 1	SL 2	SL 3	SL 4	IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 7.1 – Denial of service protection	✔	✔	✔	✔	Fortinet	Full	P: FortiGate C: Using the product(s), implement DoS protection polici
SR 7.1 RE 1 – Manage communication loads		✔	✔	✔	Fortinet	Full	P: FortiGate C: Using the product(s), implement DoS protection, SYN f protection, rate-limit, traffic shaping policies
SR 7.1 RE 2 – Limit DoS effects to other systems or networks			✔	✔	Fortinet	Full	P: FortiGate C: Using the product(s), implement DoS protection, SYN f protection, rate-limit policies
SR 7.2 – Resource management	✔	✔	✔	✔	Both	Full	P: FortiGate

SANS Institute - Using the IEC 62443 Standard

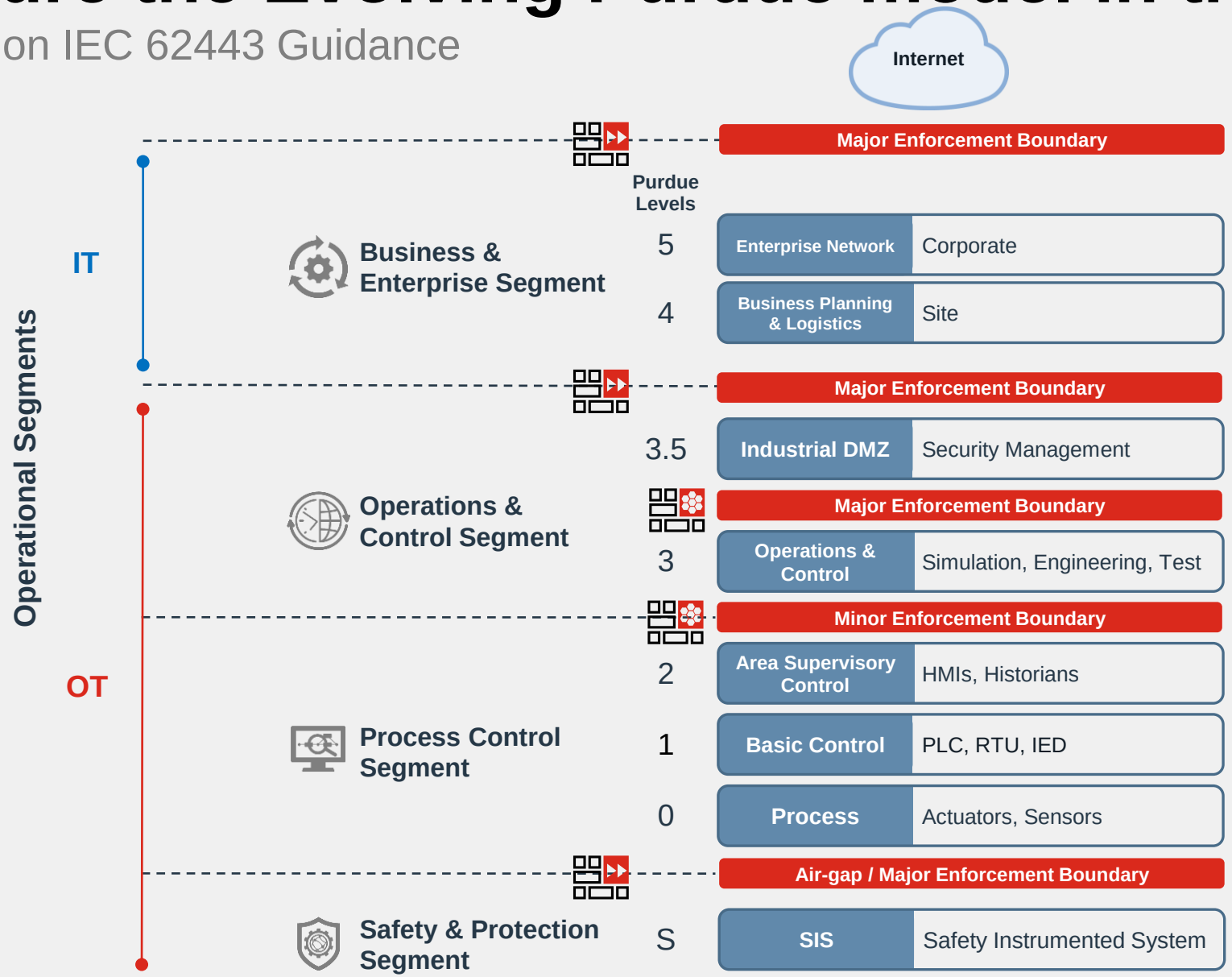
Using PERA Levels for SmartGrid Environments

… To qualify Security Products & Solutions on Reference Architecture



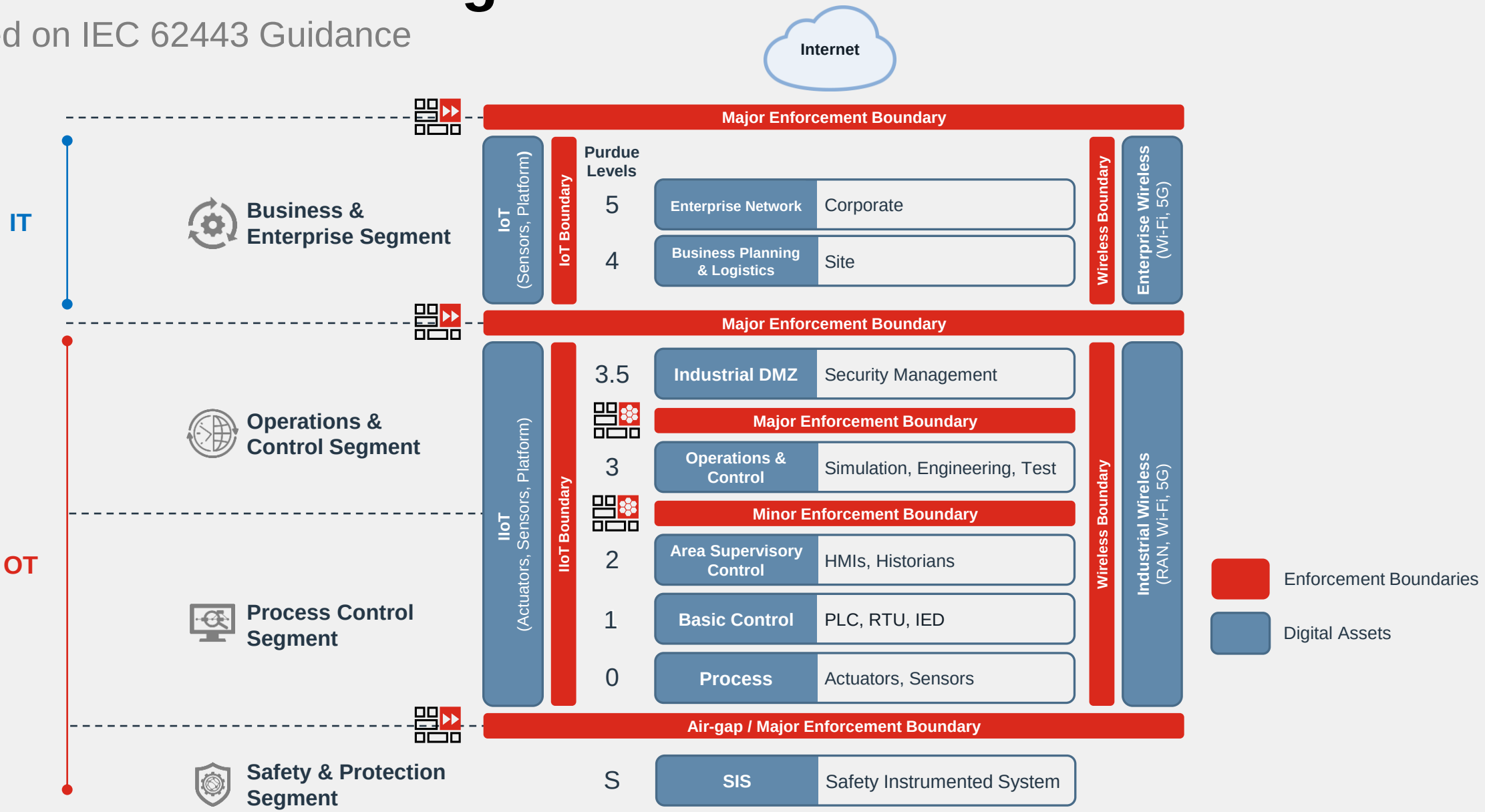
Secure the Evolving Purdue model in the face of IIoT

Based on IEC 62443 Guidance



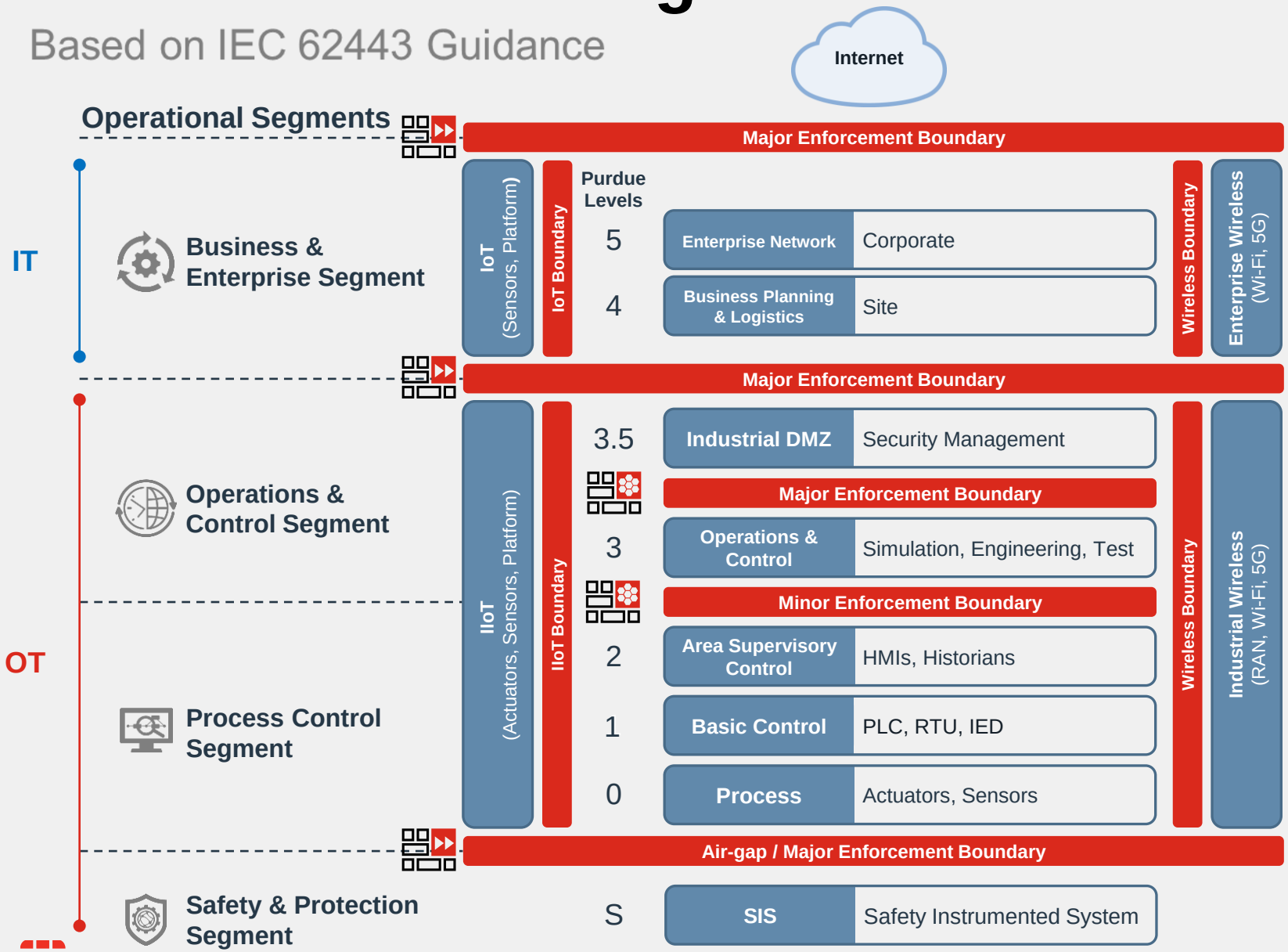
Secure the Evolving Purdue model in the face of IIoT

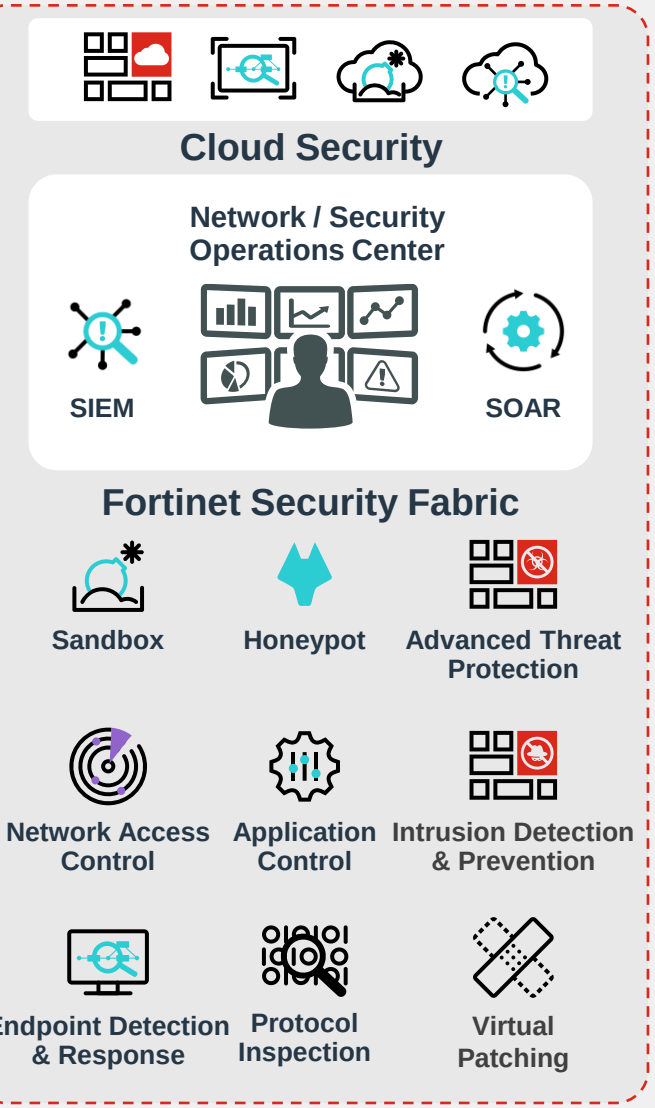
Based on IEC 62443 Guidance



Secure the Evolving Purdue model in the face of IIoT

Based on IEC 62443 Guidance





Digital Assets

Enforcement Boundaries

Key take away for Asset Owner and System Integrators

- Select your Partner ecosystem based on your compliance journey
- Think Simplicity, Life Cycle, Integration, and Orchestration
- Mind IIoTs and Wireless devices
- Make OT Cyber Security Standards and Best Practices your Roadmap

https://www.sans.org/white-papers/39960/

Invest in PEOPLE, Process, and Technology


FORTINET