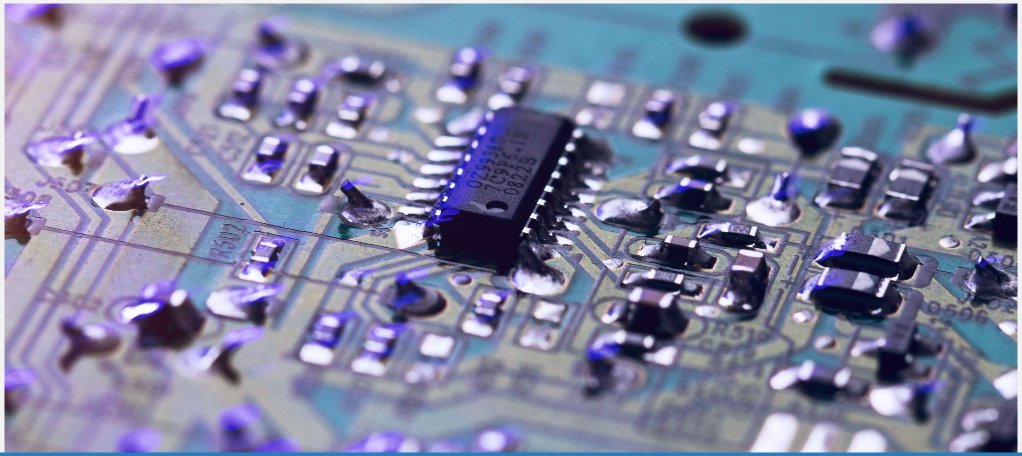
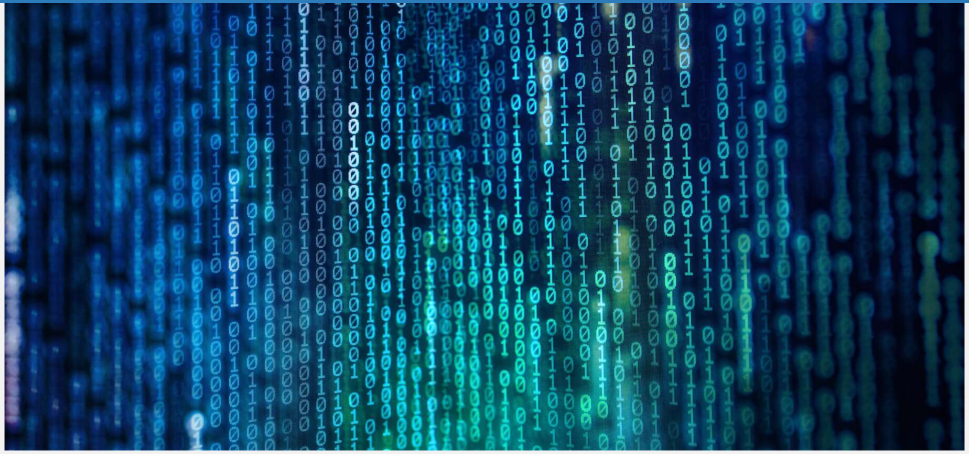


U.S. DEPARTMENT OF ENERGY

OFFICE OF Cybersecurity, Energy Security, and Emergency Response

SEI ETF Securing Energy Infrastructure Executive Task Force

Reference Architecture for Electric Energy OT and Accompanying Profiles



Introduction

The SEI ETF is a working group composed of senior government, industry, and nonprofit representatives, stood up by the Secretary of Energy as mandated by Sec. 5726 of the 2020 NDAA.

Through review of existing reference models and architectures, the Technical Project Team tasked with evaluating technology and standards identified a gap that there is no existing commonly accepted reference architecture for ICS. To produce a new model for ICS, the TPT reviewed 16 existing models—including the Purdue Enterprise Reference Architecture and Methodology and DHS's recommended practices for improving ICS cybersecurity through defense-in-depth strategies—and developed a cumulative list of core elements that would fill gaps to make a more broadly applicable reference architecture structure to build unique ICS profiles onto. Specifically, the TPT prioritized developing this reference architecture

- specifically for the electrical sector,
- not limited to localized industrial processes,
- focused on properties of information passing between devices, and
- flexible enough to reflect advances in technology and design practices.

To this end, the TPT developed the SEI ETF Reference Architecture for Electric Energy OT (RA) from which other domain-specific profiles could be derived. Upon reaching consensus, the team further developed specific profiles for substation, generation, distributed energy resources, and operation/network control center.

The RA and profiles are presented as a stack of six levels grouped into four zones. Each level contains a set of devices and systems, with the physical processes and field devices on the lowest level and a hierarchy of processes and technical controls in each level above. The profiles also include new conceptual elements: security features and participating parties assigned to each of the six levels of the model.

The SEI ETF Reference Architecture for Electric Energy OT serves as a baseline for the other profiles and introduces elements common to all the profiles, such as the five columns across all levels (security level/name, typical device examples, function, security features, actors). The Generic Profile includes six security levels spread across four zones: physical assets, operations, enterprise, and public. Zones are separated by demilitarized zones (DMZs), network segments typically located between two firewalls.

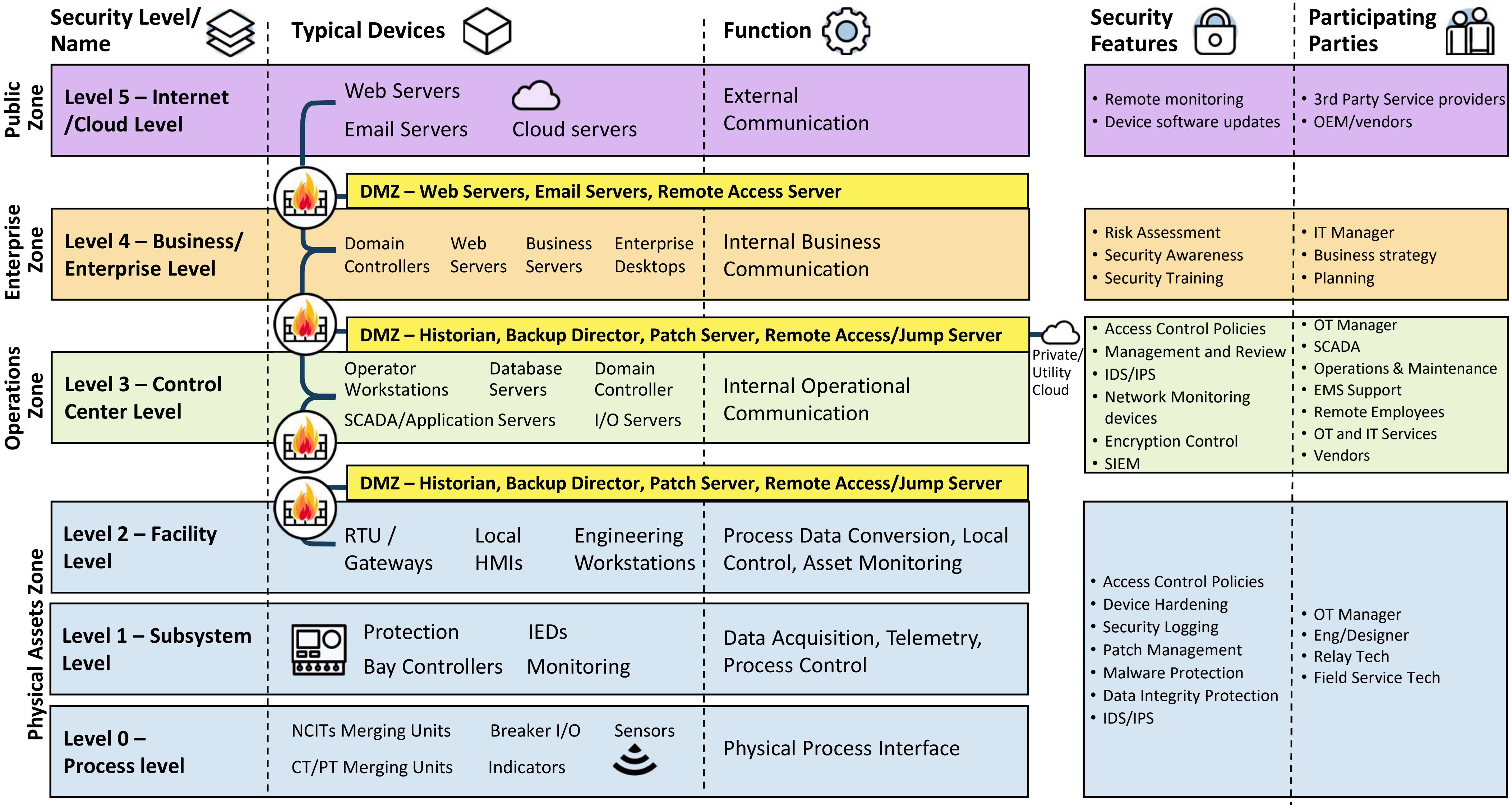
Moving towards security implementation, the RA and profiles can be used as a starting point for the Engineered Cybersecurity Process flow, as detailed in slide 11.

Reference Architecture for Electric Energy OT

	Security Level/ Name	Typical Device Examples	Function	Security Features	Participating Parties
Public Zone	Level 5 – Internet /Cloud Level	Domain Name System Server Public Cloud Servers	External Communication		
	DMZ – Web Servers, Email Servers, Remote Access Server				
Enterprise Zone	Level 4 – Business/ Enterprise Level	Domain Controllers Web Servers Business Servers Private Cloud Servers	Internal Business Communication		
	DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server				
Operations Zone	Level 3 – Control Center Level	Operator Workstations Database Servers I/O Servers Domain Controller SCADA/ Application Servers	Internal Operational Communication		
	DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server				
Physical Assets Zone	Level 2 – Facility Level	RTU / Gateways Local HMIs Engineering Workstations	Process Data Conversion, Local Control, Asset Monitoring		
	Level 1 – Subsystem Level	Protection Subsystem Controllers IEDs Monitoring	Data Acquisition, Telemetry, Process Control		
	Level 0 – Process level	NCITs Merging Units Breaker I/O CT/PT Merging Units Indicators Sensors	Physical Process Interface		

Note: RA does not include all possible security implementations (e.g. data diode vs firewall for ingress protection

Substation Profile

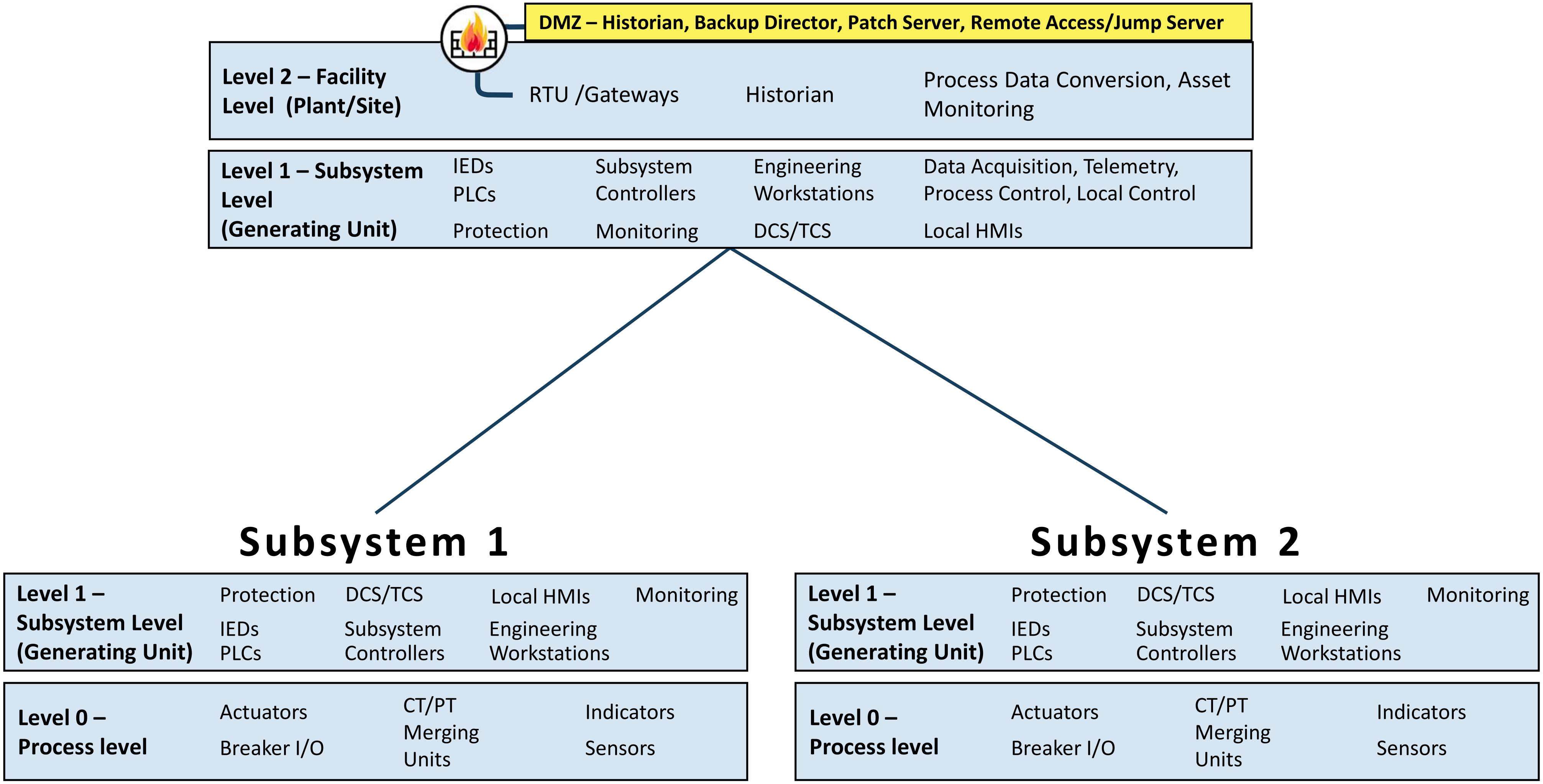


Zone	Security Level/ Name	Typical Devices	Function	Security Features	Participating Parties
Public Zone	Level 5 – Internet /Cloud Level	Web Servers Email Servers Cloud servers	External Communication	• Remote monitoring • Device software updates	• 3rd Party Service providers • OEM/vendors
	DMZ – Web Servers, Email Servers, Remote Access Server				
Enterprise Zone	Level 4 – Business/ Enterprise Level	Domain Controllers Web Servers Business Servers Enterprise Desktops	Internal Business Communication	• Risk Assessment • Security Awareness • Security Training	• IT Manager • Business strategy • Planning
	DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server	Private/ Utility Cloud		• Access Control Policies • Management and Review • IDS/IPS • Network Monitoring devices • Encryption Control • SIEM	• OT Manager • SCADA • Operations & Maintenance • EMS Support • Remote Employees • OT and IT Services • Vendors
Operations Zone	Level 3 – Control Center Level	Operator Workstations Database Servers Domain Controller SCADA/Application Servers I/O Servers	Internal Operational Communication		
	DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server				
Physical Assets Zone	Level 2 – Facility Level	RTU / Gateways Local HMIs Engineering Workstations	Process Data Conversion, Local Control, Asset Monitoring	• Access Control Policies • Device Hardening • Security Logging • Patch Management • Malware Protection • Data Integrity Protection • IDS/IPS	• OT Manager • Eng/Designer • Relay Tech • Field Service Tech
	Level 1 – Subsystem Level	Protection IEDs Bay Controllers Monitoring	Data Acquisition, Telemetry, Process Control		
	Level 0 – Process level	NCITs Merging Units Breaker I/O Sensors CT/PT Merging Units Indicators	Physical Process Interface		

Generation Profile

	Security Level/ Name	Typical Devices	Function	Security Features	Participating Parties
Public Zone	Level 5 – Internet /Cloud Level	Web Servers Email Servers Public Cloud servers	External Communication	- Remote monitoring - Device software updates	- 3rd Party Service providers - OEM/vendors
		DMZ – Web Servers, Email Servers, Remote Access Server			
Enterprise Zone	Level 4 – Business/ Enterprise Level	Domain Controllers Business Servers Web Servers Private Cloud Servers	Internal Business Communication	- Risk Assessment - Security Awareness - Security Training	- IT Manager - Business strategy - Planning
		DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server		- Access Control Policies - Management and Review - IDS/IPS - Network Monitoring devices - Encryption Control - SIEM	- OT Manager - SCADA - Operations & Maintenance - EMS Support - Remote Employees - OT and IT Services - Vendors
Operations Zone	Level 3 – Control Center Level	Operator Workstations Database Servers I/O Servers SCADA/ Application Servers Domain Controller	Internal Operational Communication		
		DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server			
Physical Assets Zone	Level 2 – Facility Level (Plant/Site)	RTU /Gateways Historian	Process Data Conversion, Asset Monitoring	- Access Control Policies - Device Hardening - Security Logging - Patch Management - Malware Protection - Data Integrity Protection - IDS/IPS	- OT Manager - Operators - Eng/Designer - Relay Tech - Field Service Tech
	Level 1 – Subsystem Level (Generating Unit)	Protection Monitoring DCS/TCS Local HMIs IEDs PLCs Subsystem Controllers Engineering Workstations	Data Acquisition, Telemetry, Process Control, Local Control		
	Level 0 – Process level	Actuators CT/PT Merging Units Breaker I/O Indicators Sensors	Physical Process Interface		

Generation Physical Asset Zone (Expanded Profile)



DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server

Level 2 – Facility Level (Plant/Site)
RTU /Gateways
Historian
Process Data Conversion, Asset Monitoring

Level 1 – Subsystem Level (Generating Unit)
IEDs
PLCs
Protection
Subsystem Controllers
Monitoring
Engineering Workstations
DCS/TCS
Data Acquisition, Telemetry, Process Control, Local Control
Local HMIs

Subsystem 1

Level 1 – Subsystem Level (Generating Unit)
Protection
IEDs
PLCs
DCS/TCS
Subsystem Controllers
Local HMIs
Engineering Workstations
Monitoring

Level 0 – Process level
Actuators
Breaker I/O
CT/PT
Merging Units
Indicators
Sensors

Subsystem 2

Level 1 – Subsystem Level (Generating Unit)
Protection
IEDs
PLCs
DCS/TCS
Subsystem Controllers
Local HMIs
Engineering Workstations
Monitoring

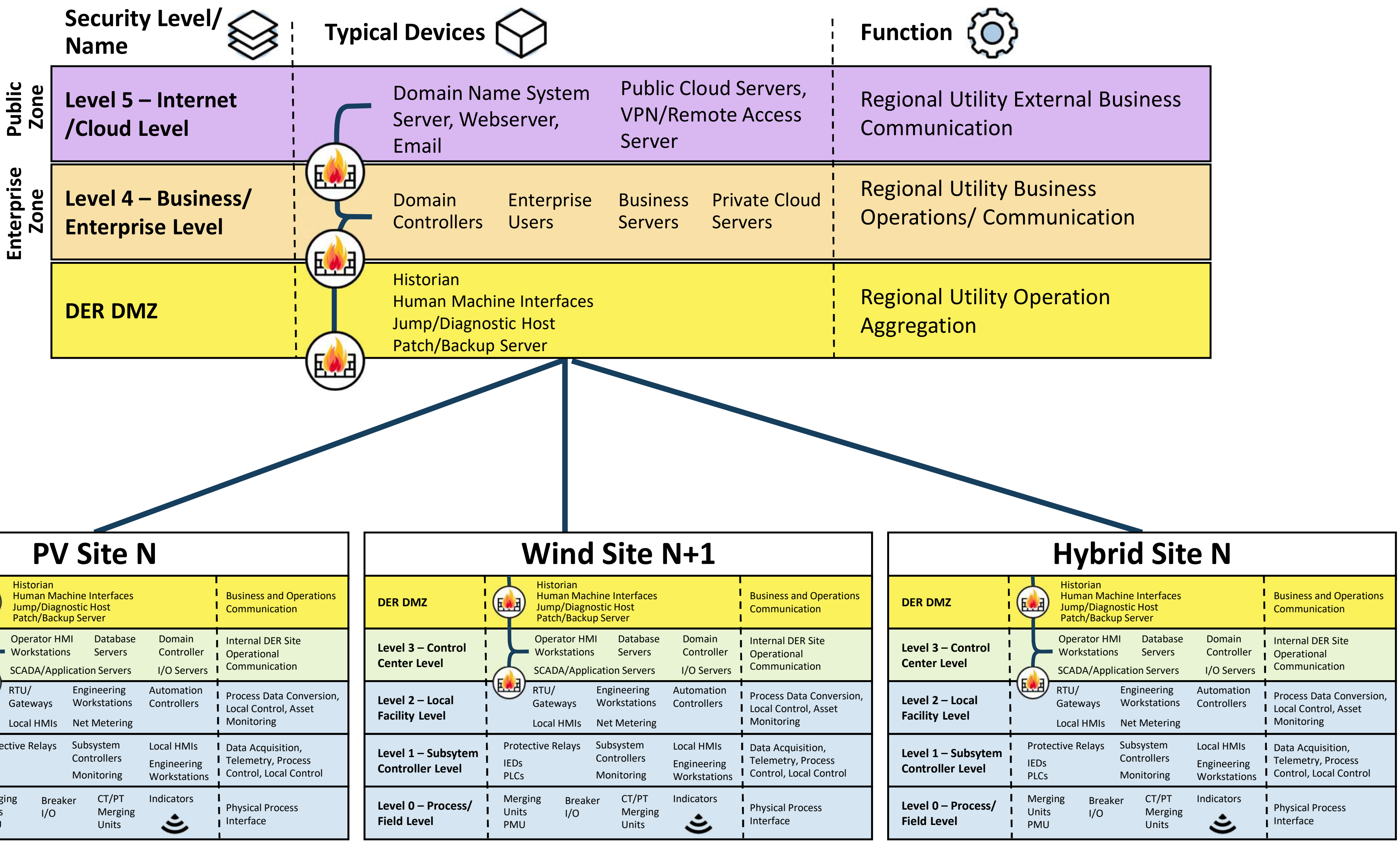
Level 0 – Process level
Actuators
Breaker I/O
CT/PT
Merging Units
Indicators
Sensors

Distributed Energy Resources (DER) Profile

Zone	Security Level/ Name	Typical Devices	Function	Security Features	Participating Parties
Public Zone	Level 5 – Internet /Cloud Level	Domain Name System Server Public Cloud Servers	External Communication	• Remote monitoring • Device software updates	• 3rd Party Service providers • OEM/vendors
	DMZ – Web Servers, Email Servers, Remote Access Server				
Enterprise Zone	Level 4 – Business/ Enterprise Level	Domain Controllers Web Servers Business Servers Private Cloud Servers	Internal Business Communication	• Risk Assessment • Security Awareness • Security Training	• IT Manager • Business strategy • Planning
	DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server	Private Utility Cloud		• Access Control Policies • Management and Review • IDS/IPS • Network Monitoring devices • Encryption Control • SIEM	• OT Manager • SCADA • Operations & Maintenance • EMS Support • Remote Employees • OT and IT Services • Vendors
Operations Zone	Level 3 – Control Center Level	Operator Workstations Database Servers Domain Controller SCADA/Application Servers I/O Servers	Internal Operational Communication		
	DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server				
Physical Assets Zone	Level 2 – Facility Level	RTU /Gateways Local HMIs Engineering Workstations Automation Controllers Net Metering	Process Data Conversion, Local Control, Asset Monitoring	• Local Station SCADA Network Monitoring • Local Device Monitoring • Ground State Truth Side Channel Monitoring • IDS/IPS	• OT Manager • Solar farm/wind farm/hydro site operator • Relay Tech • Field Service Tech
	Level 1 – Subsystem Level	Protective Relays Subsystem Controllers Engineering Workstations IEDs PLCs Monitoring Local HMIs	Data Acquisition, Telemetry, Process Control, Local Control		
	Level 0 – Process level	Merging Units PMU CT/PT Merging Units Breaker I/O Indicators	Physical Process Interface		

Not captured: Parallel control architectures

Regional Utility Scale DER Profile



	Security Level/ Name	Typical Devices				Function
Public Zone	Level 5 – Internet /Cloud Level	Domain Name System Server, Webserver, Email	Public Cloud Servers, VPN/Remote Access Server			Regional Utility External Business Communication
Enterprise Zone	Level 4 – Business/ Enterprise Level	Domain Controllers	Enterprise Users	Business Servers	Private Cloud Servers	Regional Utility Business Operations/ Communication
	DER DMZ	Historian Human Machine Interfaces Jump/Diagnostic Host Patch/Backup Server				Regional Utility Operation Aggregation

PV Site N

DER DMZ	Historian Human Machine Interfaces Jump/Diagnostic Host Patch/Backup Server				Business and Operations Communication
Level 3 – Control Center Level	Operator HMI Workstations SCADA/Application Servers	Database Servers	Domain Controller I/O Servers		Internal DER Site Operational Communication
Level 2 – Local Facility Level	RTU/ Gateways Local HMIs	Engineering Workstations Net Metering	Automation Controllers		Process Data Conversion, Local Control, Asset Monitoring
Level 1 – Subsytem Controller Level	Protective Relays IEDs PLCs	Subsystem Controllers Monitoring	Local HMIs Engineering Workstations		Data Acquisition, Telemetry, Process Control, Local Control
Level 0 – Process/ Field Level	Merging Units PMU	Breaker I/O	CT/PT Merging Units	Indicators	Physical Process Interface

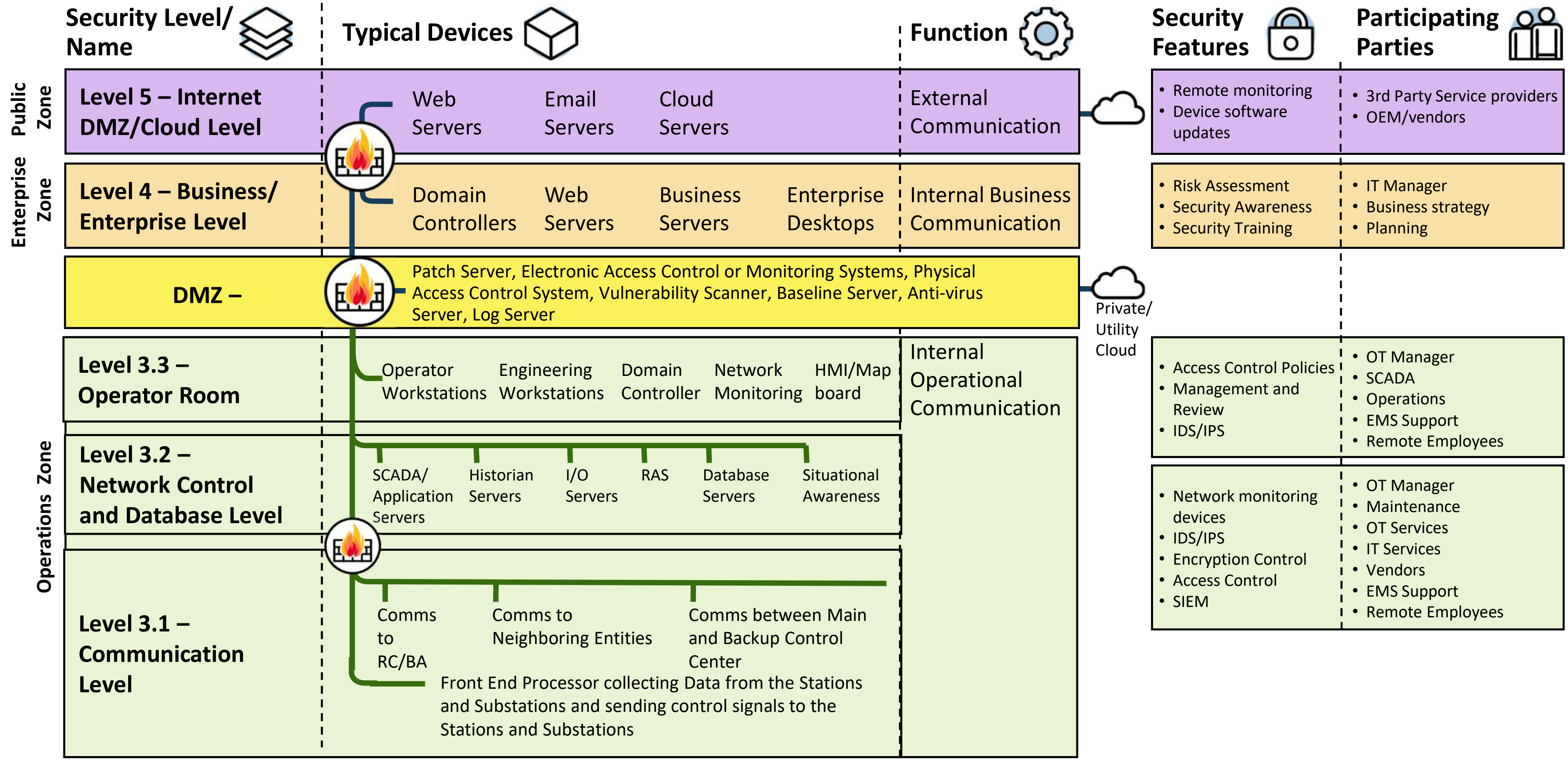
Wind Site N+1

DER DMZ	Historian Human Machine Interfaces Jump/Diagnostic Host Patch/Backup Server				Business and Operations Communication
Level 3 – Control Center Level	Operator HMI Workstations SCADA/Application Servers	Database Servers	Domain Controller I/O Servers		Internal DER Site Operational Communication
Level 2 – Local Facility Level	RTU/ Gateways Local HMIs	Engineering Workstations Net Metering	Automation Controllers		Process Data Conversion, Local Control, Asset Monitoring
Level 1 – Subsytem Controller Level	Protective Relays IEDs PLCs	Subsystem Controllers Monitoring	Local HMIs Engineering Workstations		Data Acquisition, Telemetry, Process Control, Local Control
Level 0 – Process/ Field Level	Merging Units PMU	Breaker I/O	CT/PT Merging Units	Indicators	Physical Process Interface

Hybrid Site N

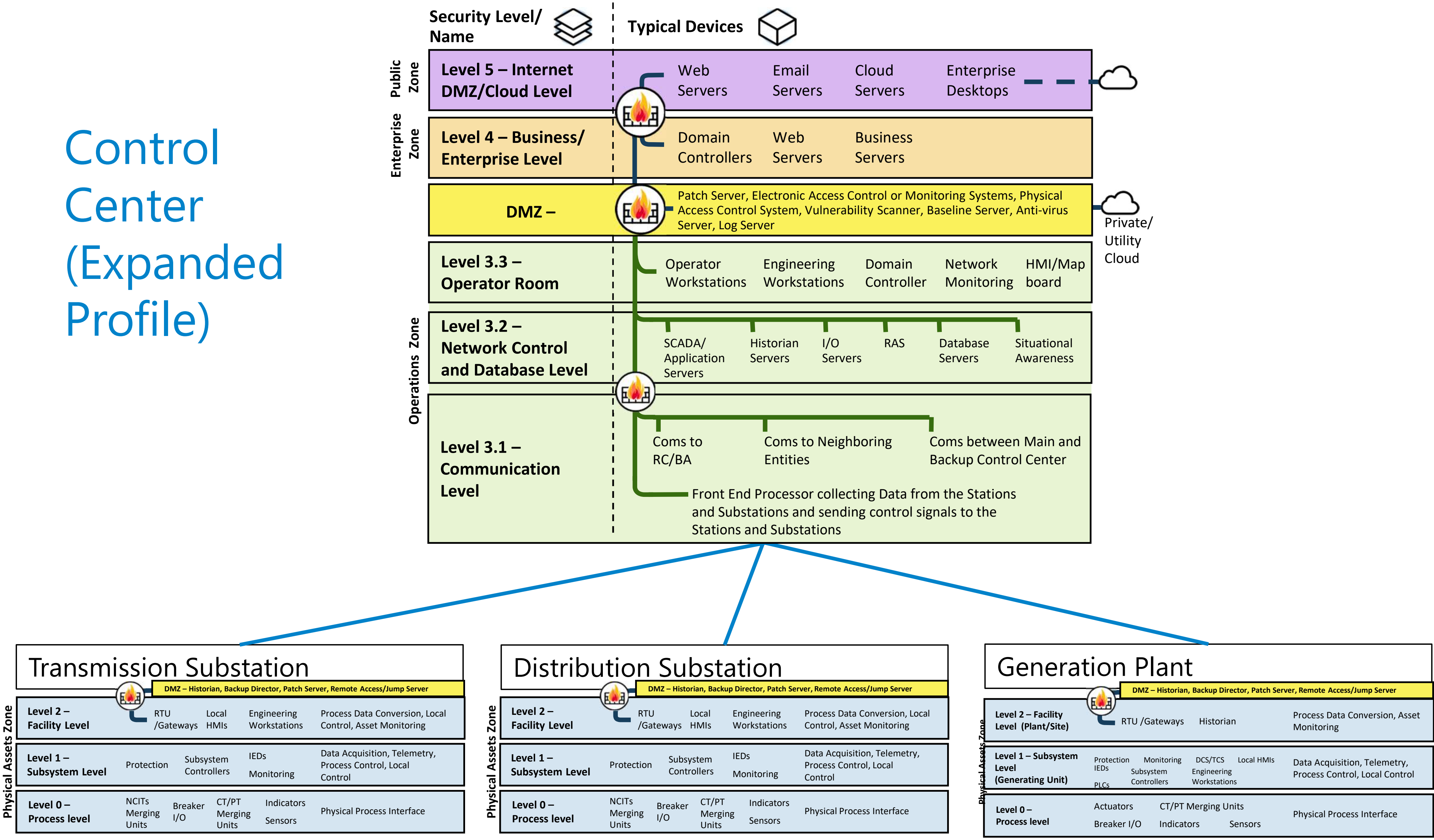
DER DMZ	Historian Human Machine Interfaces Jump/Diagnostic Host Patch/Backup Server				Business and Operations Communication
Level 3 – Control Center Level	Operator HMI Workstations SCADA/Application Servers	Database Servers	Domain Controller I/O Servers		Internal DER Site Operational Communication
Level 2 – Local Facility Level	RTU/ Gateways Local HMIs	Engineering Workstations Net Metering	Automation Controllers		Process Data Conversion, Local Control, Asset Monitoring
Level 1 – Subsytem Controller Level	Protective Relays IEDs PLCs	Subsystem Controllers Monitoring	Local HMIs Engineering Workstations		Data Acquisition, Telemetry, Process Control, Local Control
Level 0 – Process/ Field Level	Merging Units PMU	Breaker I/O	CT/PT Merging Units	Indicators	Physical Process Interface

Control Center Profile



Zone	Security Level/ Name	Typical Devices	Function	Security Features	Participating Parties
Public Zone	Level 5 – Internet DMZ/Cloud Level	Web Servers Email Servers Cloud Servers	External Communication	• Remote monitoring • Device software updates	• 3rd Party Service providers • OEM/vendors
Enterprise Zone	Level 4 – Business/ Enterprise Level	Domain Controllers Web Servers Business Servers Enterprise Desktops	Internal Business Communication	• Risk Assessment • Security Awareness • Security Training	• IT Manager • Business strategy • Planning
	DMZ –	Patch Server, Electronic Access Control or Monitoring Systems, Physical Access Control System, Vulnerability Scanner, Baseline Server, Anti-virus Server, Log Server			
Operations Zone	Level 3.3 – Operator Room	Operator Workstations Engineering Workstations Domain Controller Network Monitoring HMI/Map board	Internal Operational Communication	• Access Control Policies • Management and Review • IDS/IPS	• OT Manager • SCADA • Operations • EMS Support • Remote Employees
	Level 3.2 – Network Control and Database Level	SCADA/ Application Servers Historian Servers I/O Servers RAS Database Servers Situational Awareness		• Network monitoring devices • IDS/IPS • Encryption Control • Access Control • SIEM	• OT Manager • Maintenance • OT Services • IT Services • Vendors • EMS Support • Remote Employees
	Level 3.1 – Communication Level	Comms to RC/BA Comms to Neighboring Entities Comms between Main and Backup Control Center Front End Processor collecting Data from the Stations and Substations and sending control signals to the Stations and Substations			

Control Center (Expanded Profile)



Security Level/ Name

Typical Devices

Public Zone

Level 5 – Internet DMZ/Cloud Level: Web Servers, Email Servers, Cloud Servers, Enterprise Desktops

Enterprise Zone

Level 4 – Business/ Enterprise Level: Domain Controllers, Web Servers, Business Servers

DMZ –: Patch Server, Electronic Access Control or Monitoring Systems, Physical Access Control System, Vulnerability Scanner, Baseline Server, Anti-virus Server, Log Server

Private/ Utility Cloud

Operations Zone

Level 3.3 – Operator Room: Operator Workstations, Engineering Workstations, Domain Controller, Network Monitoring, HMI/Map board

Level 3.2 – Network Control and Database Level: SCADA/ Application Servers, Historian Servers, I/O Servers, RAS, Database Servers, Situational Awareness

Level 3.1 – Communication Level: Coms to RC/BA, Coms to Neighboring Entities, Coms between Main and Backup Control Center, Front End Processor collecting Data from the Stations and Substations and sending control signals to the Stations and Substations

Transmission Substation

DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server

Physical Assets Zone

Level 2 – Facility Level: RTU /Gateways, Local HMIs, Engineering Workstations; Process Data Conversion, Local Control, Asset Monitoring

Level 1 – Subsystem Level: Protection, Subsystem Controllers, IEDs, Monitoring; Data Acquisition, Telemetry, Process Control, Local Control

Level 0 – Process level: NCITs Merging Units, Breaker I/O, CT/PT Merging Units, Indicators, Sensors; Physical Process Interface

Distribution Substation

DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server

Physical Assets Zone

Level 2 – Facility Level: RTU /Gateways, Local HMIs, Engineering Workstations; Process Data Conversion, Local Control, Asset Monitoring

Level 1 – Subsystem Level: Protection, Subsystem Controllers, IEDs, Monitoring; Data Acquisition, Telemetry, Process Control, Local Control

Level 0 – Process level: NCITs Merging Units, Breaker I/O, CT/PT Merging Units, Indicators, Sensors; Physical Process Interface

Generation Plant

DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server

Physical Assets Zone

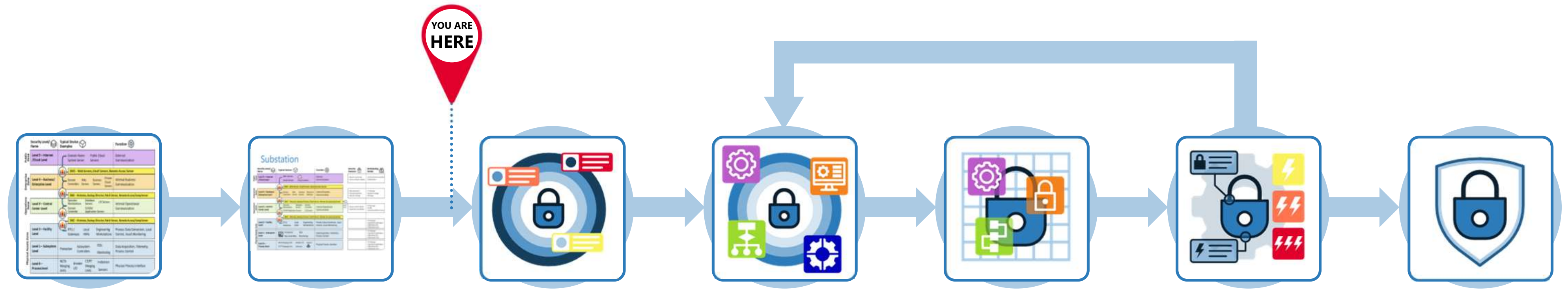
Level 2 – Facility Level (Plant/Site): RTU /Gateways, Historian; Process Data Conversion, Asset Monitoring

Level 1 – Subsystem Level (Generating Unit): Protection IEDs, PLCs, Monitoring, Subsystem Controllers, DCS/TCS, Engineering Workstations, Local HMIs; Data Acquisition, Telemetry, Process Control, Local Control

Level 0 – Process level: Actuators, Breaker I/O, CT/PT Merging Units, Indicators, Sensors; Physical Process Interface

Engineered Cybersecurity Process Flow

Reference Architecture to Security Implementation



Reference Architecture

- Starting point used for communication and organizational awareness

Reference Architecture Profiles

- Templates for OT control system including adaptation for OT applications

Security Concept

- High level overview of the main cybersecurity objectives including definitions of security features , necessary security functions

System Architecture

- Security overview defining the system components, interfaces, data flow and the preliminary zoning of the design

Security Design

- Detailed security solution and specification of cyber assets, security features and methodology to support the security concept

Security Risk Assessment

- Cyber Asset registry with detailed functions
- Hazard analysis with consequences assessment
- Risk profile developed

Security Implementation

- Execution of the security solution per the security design

Appendix A: Acronyms and Abbreviations

- AOO: Asset Owner-Operator
- ICS: Industrial Control System
- CESER: Office of Cybersecurity, Energy Security, and Emergency Response
- CT/PT: Current Transformer/Potential Transformer
- DCS/TCS: Distributed Control System/Transmission Control System
- DER: Distributed Energy Resource
- DMZ: Demilitarized Zone
- EMS: Energy Management System
- ENG: Engineering
- HMI: Human Machine Interface
- I&C: Instrumentation and Control
- IDS/IPS: Intrusion Detection System/Intrusion Prevention System
- IED: Intelligent Electronic Device
- IEEE: Institute of Electrical and Electronics Engineers
- INL: Idaho National Lab
- I/O: Input/Output
- IT: Information Technology
- NCIT: Non-Conventional Instrument Transformers
- NDAA: National Defense Authorization Act
- NIST: National Institute of Standards and Technology
- NREL: National Renewable Energy Laboratory
- O&M: Operations and Maintenance
- OEM: Original Equipment Manufacturer
- OT: Operational Technology
- PLC: Programmable Logic Controller
- PMU: Phasor Measurement Unit
- RAS: Remote Access Server
- RC/BA: Reliability Coordinator/Balancing Authority
- RTU: Remote Terminal Unit
- SCADA: Supervisory Control and Data Acquisition
- SEI ETF: Securing Energy Infrastructure Executive Task Force
- SIEM: Security Information and Event Management
- VPN: Virtual Private Network