U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

SEI ETF Securing Energy Infrastructure Executive Task Force

Reference Architectures as a Means of Influencing Electric Energy Operational Technology/Industrial Control System Security Outcomes

March 2022

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

SEI ETF Securing Energy Infrastructure Executive Task Force

This publication was produced for the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response by the Technical Project Team of the Security Energy Infrastructure Executive

Reference Architectures as a Means of Influencing Electric Energy Operational Technology/Industrial Control Systems Security Outcomes

Technical Project Team: Evaluate Technology and Standards

Sponsoring DOE Office: Cybersecurity, Energy Security, and Emergency Response

Date of Publication: April 2022

Authors: Maurice Martin (lead author), National Renewable Energy Laboratory
Samuel Chanoski, Idaho National Laboratory
Steve Granda, National Renewable Energy Laboratory
Steven Kunsman, Hitachi Energy
Marcus Sachs, Auburn University

Preface

The work presented in this document was performed by a group of senior government, industry, and nonprofit representatives convened to address cybersecurity challenges associated with technology and standards for industrial control systems (ICSs), specifically those supporting the electrical grid. The work is in support of the *National Defense Authorization Act for Fiscal Year 2020*,[1] section 5726 ("Securing Energy Infrastructure"). The group, named the Securing Energy Infrastructure Executive Task Force (SEI ETF), was chartered to:

A. Evaluate technology and standards, in partnership with covered entities, to isolate and defend ICSs of covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities including:
    a. Analog and nondigital control systems
    b. Purpose-built control systems
    c. Physical controls.[2]
B. Develop a national cyber-informed engineering strategy to isolate and defend covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities.[3]
C. Identify new classes of security vulnerabilities of covered entities.[4]

This report focuses on a significant aspect of the first item above: Evaluating technology and standards. It explains the role that the reference architecture and associated profiles can play in this effort, and the work by the SEI ETF in this area.

[1] Inhofe, James M. S. 1790 - 116th Congress (2019-2020): National Defense Authorization Act for Fiscal Year 2020, legislation. December 20, 2019, 2019/2020. https://www.congress.gov/bill/116th-congress/senate-bill/1790.
[2] Inhofe, sec. 5726 (c)(1)(A) and (b)(2).
[3] Inhofe, sec. 5726 (c)(1)(B).
[4] Inhofe, sec. 5726 (b)(1).

List of Acronyms

AOO	asset owner and operator
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
HMI	human machine interface
I&C	instrumentation and control
ICS	industrial control system
IDS/IPS	intrusion detection system/intrusion prevention system
IED	intelligent electronic device
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
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

Executive Summary

There exist more than 60 cybersecurity standards applicable to the electrical grid.[5] Some apply to industrial control systems in general, while others are specific to the energy sector. These standards have been developed by diverse organizations and focus on various aspects of security such as documenting good practices, promoting economic efficiency, and supporting ownership and operation.

Despite the considerable number of standards, there are still gaps corresponding to devices or systems within the electrical grid that are not addressed by a single standard, or standard series. This situation may grow more dire over time as the grid incorporates new digital technologies, advanced automation, and increased distributed generation (including renewables). It cannot be assumed that today's standards address all areas of the current grid, much less the more complicated grid coming into existence. Gaps in cybersecurity standards represent a latent sector-wide weakness in the electricity subsector.

This white paper presents a *reference architecture and associated profiles* as a path forward for asset owners, cybersecurity specialists focused on operational technology (OT) systems, standards organizations, system integrators, third-party original equipment manufacturers, and other grid stakeholders. Reference architectures are sets of documents that provide templates for the design or upgrade of systems in a variety of domains. If system designers work within a reference architecture, they are not starting from scratch—the reference architecture can be adapted for the specific system. In doing so, the design process is accelerated and produces better results.

In this context, reference architectures provide value in two ways. Both assume a collection of reference architectures that address distinct aspects and applications of electrical grid cybersecurity.

First, reference architectures can be used to identify gaps in OT security design and solutions. Comparing the security architecture of a specific system with the most applicable reference architecture can reveal missing security controls, which can then be added to the design. Section 3 of this paper explains an iterative process for refining the design prior to implementation of the design.

Second, reference architectures can reveal gaps in the 60+ cybersecurity standards applicable to the electrical grid. One could map this collection of cybersecurity standards onto reference architectures to determine which parts of the reference architectures are covered by one or more standards. Any part of a reference architecture not addressed would represent a gap that could potentially leave systems vulnerable. Grid stakeholders (as identified above) could come together to discuss these gaps, identify where the standards gaps may correspond to gaps in available solutions, and commence security designs to resolve the gaps.

This white paper describes work already begun to develop the collection of reference architectures needed. This work began with an SEI ETF Reference Architecture for Electric Energy OT from which domain-specific profiles were derived. The Reference Architecture and accompanying profiles presented in this white paper may be considered early iterations, with refinements to follow. The domain-specific profiles under development are:

- Generation
- Transmission and distribution substation

[5] Office of Cybersecurity, Energy Security, and Emergency Response. "Standards to Secure Energy Infrastructure." Accessed 28 March 2022. https://energyicsstandards.inl.gov/.

- Distributed energy resources (DER)
- Regional utility-scale DER
- Control center.

These reference architectures are discussed in this report with an explanation of the variations among them.

Table of Contents

List of Figures

1. Introduction: Standards and Gaps

According to research performed by the Securing Energy Infrastructure Executive Task Force (SEI ETF), there exist more than 60 cybersecurity standards that are applicable to the electrical grid.[6] Some apply to industrial control systems (ICSs) in general, such as the *Guide to Industrial Control Systems (ICS) Security* published by the National Institute of Standards and Technology. Another example is IEC 62443 (formerly ISA 99), an international series of standards that address cybersecurity for operational technology (OT) in automation and control systems. That standard is divided into different sections and describes both technical and process-related aspects of automation and control systems cybersecurity. It divides the cybersecurity topics by stakeholder category/roles, including: the operator, the service providers (service providers for integration and for maintenance), and the component/system manufacturers. Each role follows a risk-based approach to prevent and manage security risks in their activities.[7]

Other standards are specific to the energy sector, such as the IEEE C37.240 *Standard for Cybersecurity Requirements for Substation Automation, Protection, and Control Systems* from the Institute of Electrical and Electronics Engineers (IEEE). These standards have been developed by diverse organizations and focus on various aspects of security, such as documenting good practices, promoting economic efficiency, and supporting ownership and operation.[8] These standards represent the work of hundreds of subject matter experts working across various industries for many years and often in a volunteer capacity. While they deserve much of the credit for advancing grid security, the sheer number of standards creates a new kind of challenge: System operators and manufacturers are left wondering which standards to adopt. Is there a small number (ideally one) that will cover all elements of an individual operator's system? If so, which one? Overlapping standards create another problem: Organizations may attempt to comply with multiple overlapping standards, resulting in security programs that are bloated, thereby consuming valuable security resources without adding security value.

In examining this issue, the Securing Energy Infrastructure Executive Task Force (SEI ETF) identified other concerns. Two standards may offer different guidance in some areas of security, or outright contradict one another. Standards may be out of date, as the process of creating and revising standards is notoriously slow. Standard-making committees may succumb to political or economic pressures.[9] They may produce documents that provide multiple, confusing options for adoption or implementation.

There may also be gaps corresponding to devices or systems within the electrical grid that are not addressed by any standard, or addressed only superficially. This situation may grow more pronounced over time, since the grid is undergoing a radical change as it incorporates new digital technologies, advanced automation and increased distributed generation (particularly renewables). Furthermore, the fact that standards creation systemically lags technological development may exacerbate this issue. The future grid will likely incorporate more communication technology, as digital substations become the norm, supervisory control and data acquisition (SCADA) networks push further toward the grid edge, and the boundary between OT and information technology (IT) blur. It cannot be assumed that today's standards address all areas of the current grid, much less the more complicated grid coming into existence.

Gaps in cybersecurity standards represent a latent sector-wide weakness for the electricity subsector. A well-intentioned utility owner might comply with what they believe are best-in-class standards, yet still have unaddressed, systemic vulnerabilities. This white paper describes a path forward, using reference architectures

[6] SEI ETF.
[7] Wikipedia. "IEC 62443."March 2022. Accessed on 28 March 2022. https://en.wikipedia.org/wiki/IEC_62443.
[8] SEI ETF.
[9] Ferguson, Niels, Bruce Schneier, and Tadayoshi Kohno. 2010. *Cryptography Engineering: Design Principles and Practical Applications*. Indianapolis, Indiana: Wiley Publishing, 318.

as a tool for identifying gaps in cybersecurity standards, and providing a starting point for system design using a risk-based approach to assess potential solution security risks.

2. Reference Architectures

There are many definitions of *reference architecture*. The European Innovation Partnership on Smart Cities and Communities definition reads: "Reference architecture is defined as an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions.[10]" For the purposes of its work in the field of cybersecurity standards for the electricity subsector, the SEI ETF developed the following definition:

- Reference architecture is a system of classification (taxonomy) to establish a common architecture communication platform.
- Typically, a reference architecture includes common architecture principles, patterns, building blocks, and standards.[11]

Reference architectures are used in many different industries. They often serve as a starting point for those wishing to design a system—for instance, an IT system to protect financial transactions. By studying an applicable reference architecture, designers can get ideas on what to include in their financial transaction system. Their design does not need to start from scratch. They can use the reference architecture as a template, adapting it in ways that make sense for the specific system they're building. In doing so, they accelerate the design process and produce better results.

In the cybersecurity domain, reference architectures provide a starting point for developing security implementations. They serve as the "stake in the ground" that starts the conversations around security for a new system, allowing for more efficient and effective discussions between stakeholders (including original equipment manufacturers [OEMs] and asset owners and operators [AOOs]). Reference architectures can guide the discussions that appropriately consider security features and controls.

Shared reference architectures help users focus on risk-based approaches to cybersecurity. They reduce duplicative efforts, provide a mechanism for building consensus around best practices, and are consistently updatable. They provide a means for AOOs to create baselines for their short- and long-term design and engineering practices. This baseline provides OEMs a starting point for design.

In the context of this project, reference architectures provide value in two ways. Both assume a collection of reference architectures that address distinct aspects and applications of electric grid cybersecurity.

First, reference architectures can be used to identify gaps in OT security design and solutions. Comparing the security architecture of a specific system with the most applicable reference architecture can reveal missing security controls, which can then be added to the design. Section 3 of this paper explains an iterative process for refining the design in this way prior to implementation of the design.

Second, reference architectures can reveal gaps in the 60+ cybersecurity standards applicable to the electrical grid. One could map this collection of cybersecurity standards onto reference architectures to determine which

[10] Heuser, Lutz, Jeroen Scheer, Pieter den Hamer, Bart de Lathouwer, Andy Cox, Peter Parslow, Bernhart Kempen, Eva Klien, and Joachim Lonien. Sept. 27, 2017. *Reference Architecture & Design Principles*. European Commission. https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b9a18c76&appId=PPGMS

[11] SEI ETF technical project team meeting.

parts of the reference architectures are covered by one or more standards. Any part of a reference architecture not addressed would represent a gap that could potentially leave systems vulnerable. Grid stakeholders could come together to discuss these gaps, identify where the standards gaps may correspond to gaps in available solutions, and commence security designs to resolve the gaps. This idea is illustrated in Figure 10 below.

The SEI ETF is developing the initial reference architecture and profiles needed to provide these two types of value. This development began with the SEI ETF Reference Architecture for Electric Energy OT, from which domain-specific applications could be derived. These domain-specific applications are referred to as *profiles.* The Reference Architecture and accompanying profiles presented in this white paper may be considered early iterations, with refinements to follow. The domain-specific reference architectures under development are:

- Generation
- Substation
- Distributed energy resources (DER)
- Regional utility-scale DER
- Control center.

Their development and details are explained in Section 5. Reference Architecture and Profiles.

3. Engineered Cybersecurity Process Flow

The process flow for applying reference architecture profiles to improving security is illustrated in Figure 1.

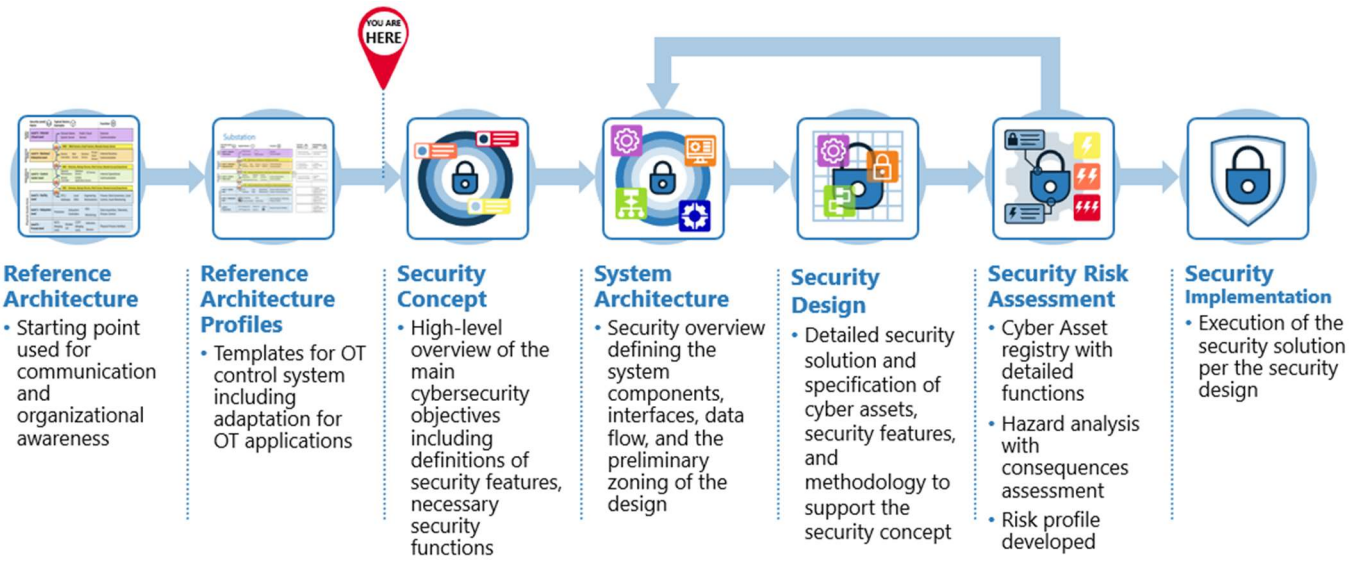

Figure 1. Engineered cybersecurity process flow from reference architecture to security implementation

The two items to the left of the "You are HERE" marker in Figure 1 represent work accomplished by this project. Note that this begins with a single reference architecture (far left), which serves as a baseline for the domain-specific reference architecture profiles (second from left). Items to the right of the marker are tasks undertaken by the AOO as it moves from security concept to implementation.

The security risk assessment may trigger several iterations of refinement for the architecture and design. This is the real value of the process. These iterations (ideally) bring together the OT, IT, and security teams for an

objective evaluation of the design under proposal and trigger discussions on effectiveness, operational impact, practicality, cost, and other factors. The goal is to move as much of the thinking and planning up front, extricate ambiguity, and arrive at the most mature design possible before moving to security implementation.

4. Development: Starting with the Purdue Model

The Purdue Enterprise Reference Architecture, often called the "Purdue Model," was developed in the 1990s to define segmentation between enterprise networks and ICS networks. While the Purdue Model was not designed to be a cybersecurity reference architecture,[12] it does provide a framework for discussing, analyzing, and designing security for ICSs, particularly the touchpoints between OT networks and IT networks. For this reason, the Purdue Model is heavily referenced in the literature for ICS security.

The profiles developed for this effort draw from the Purdue Model. Like the Purdue Model, they 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. However, the profiles presented here also attempt to address some of the Purdue Model shortcomings relative to evaluating standards. Specifically, the Purdue Model:

- Was not designed as a cybersecurity reference architecture
- Was not designed specifically for the electricity subsector
- Assumes localized industrial processes
- Focuses on devices, rather than the properties of information passing between them
- Is approximately 30 years old, and therefore does not reflect advances in technology and design practices.

The Purdue Model has been utilized in the industrial and manufacturing sectors, and thus the levels and zones represent these sectors. The SEI ETF effort leveraged the model but adapted some of the zone and level naming that would be more familiar to an electricity subsector OT system engineer.

It is also acknowledged that the Purdue Model will have challenges as the OT systems evolve and advance (for instance, through the incorporation of virtualization technology). The SEI ETF effort has focused on the typical OT system installed or the digital OT systems that are state of the art today. The virtualization and cloud-based OT systems in development are an identified SEI ETF gap that will require adaption or development of a new reference architecture.

5. Reference Architecture and Profiles

As stated above, this document refers to domain-specific reference architecture application as *profiles*. Besides addressing the shortcomings of the Purdue Model, the profiles presented here include new conceptual elements: *security features* and *participating parties* assigned to each of the six levels of the model. *Security features* are controls recommended for the level or zone to which they are attached. *Participating parties* are humans that are either a part of a level or interact with elements found within that level (for instance, an OT manager at the facility level).

[12] SANS Institute. July 16, 2021. "Introduction to ICS Security Part 2." https://www.sans.org/blog/introduction-to-ics-security-part-2.

5.1 SEI ETF Reference Architecture for Electric Energy OT

The SEI ETF Reference Architecture for Electric Energy OT (referred to below as the Reference Architecture) serves as a baseline for the profiles. Compared to the profiles, it most resembles the Purdue Model. The Reference Architecture introduces elements common to all the profiles, such as the five columns that cut across all levels:

- Security level/name
- Typical device examples
- Function
- Security features
- Participating parties.

In the Reference Architecture, the columns labeled "security features" and "participating parties" are left deliberately blank. (These columns are only populated in the profiles.) As shown in Figure 2, the Reference Architecture includes six security levels spread across four zones: physical assets, operations, enterprise, and public. Zones are separated by demilitarized zones, network segments typically located between two firewalls.

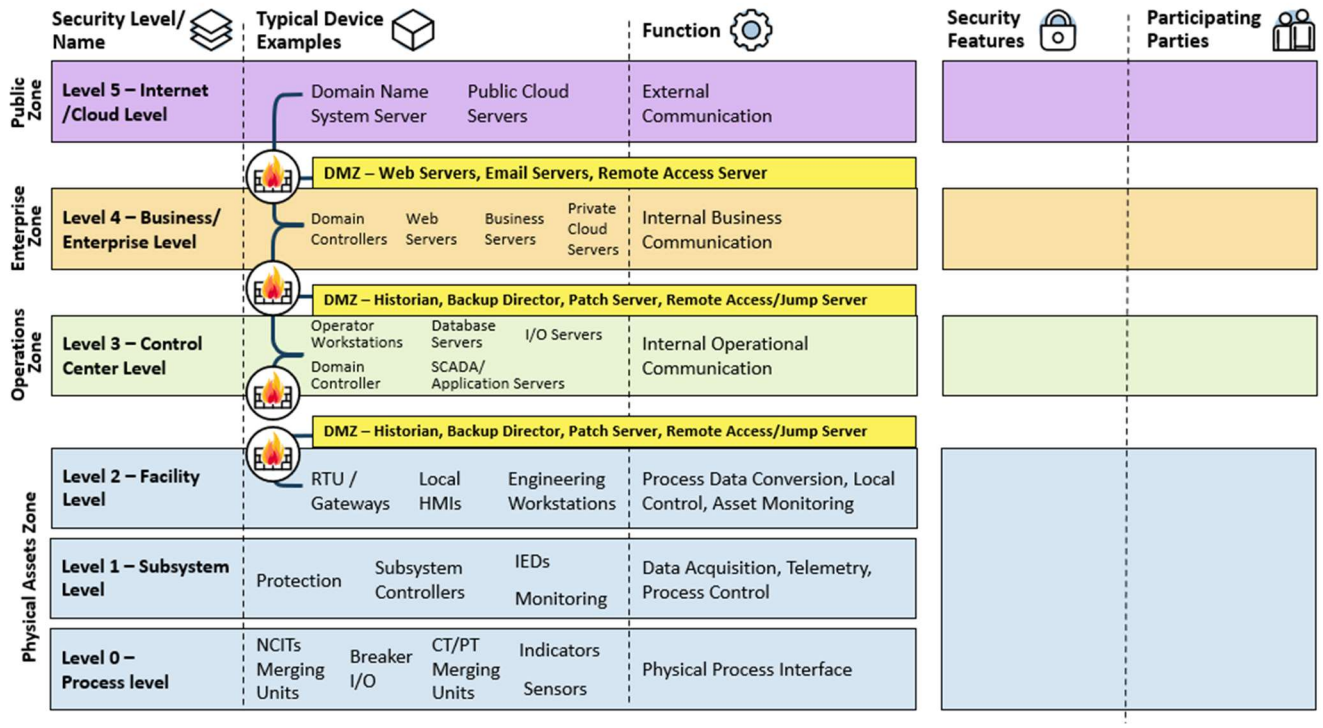

Figure 2. SEI ETF Reference Architecture for Electric Energy OT. Includes the two columns (at right) that will be populated in the profiles. (Abbreviations appearing in tables are expanded in the list of acronyms.)

The Reference Architecture makes no assumptions about the location of processes in Level 0. In an actual grid, you would expect breakers, current transformers, potential transformers, and other Level 0 devices to be spread

across a wide geographic area. Likewise, devices all the way up to Level 2 may be distributed among remote substations or local control stations.

5.2 Generation

The generation profile, as shown in Figure 3, focuses specifically on large-scale, centralized generations facilities.

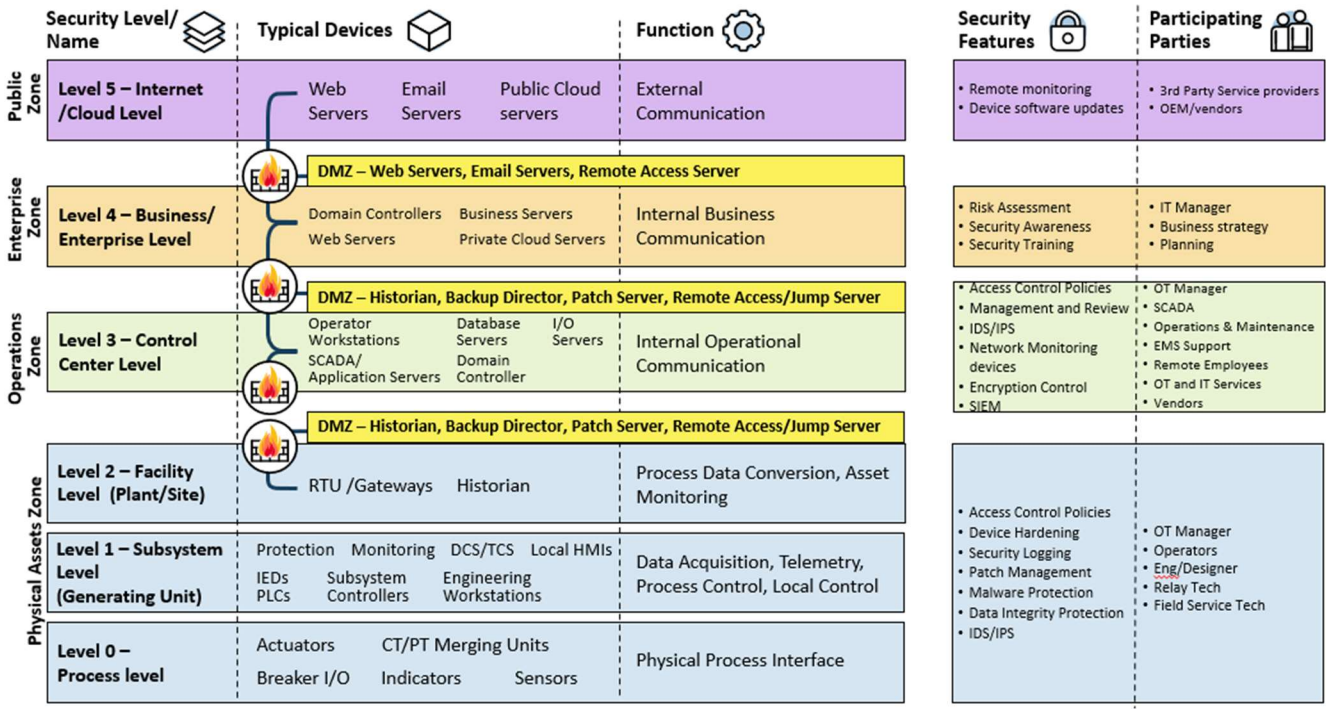

Figure 3. Generation profile

The following list examines the contents of the security features in detail:

- **Level 5**
  - **Remote monitoring:** Securing the touchpoints between the generation facility and external resources (e.g., cloud-based applications).
  - **Device software updates:** Updating software and firmware for devices and systems. Updates might be delivered via Internet connection with the device, requiring some security validation (e.g., checking hashes on the update files).
- **Level 4**
  - **Risk assessment:** Identifying critical assets, vulnerabilities, threats, and potential impact that might result from a cyberattack.
  - **Security awareness:** Knowledge that utility staff possesses about physical assets, information assets, and their protection (e.g., establishing topological, behavioral, and configuration baselines).
  - **Security training:** Educating utility staff regarding issues of security awareness, as well as specific skills they may need to enforce security.
- **Level 3**
  - **Access control policies:** The policies that determine who has access to various devices, information, and systems.

  - **Management and review:** The activity of reviewing the cybersecurity logging against policy and adjusting any access or security settings as needed.
  - **Intrusion detection system (IDS)/intrusion prevention system (IPS):** Those functions that identify a cyberattack in progress and (in the case of IPS), take some action in response to the attack.
  - **Network monitoring devices:** Tools for tracking activity on a network.
  - **Encryption control:** The inclusion of a cryptographic system to protect data.
  - **Security information and event management:** Tools for managing data about system behavior and observed events that may prove helpful in identifying cyber incidents.
- **Levels 2-0**
  - **Access control policies:** The policies that determine access to various devices, information, and systems.
  - **Device hardening:** Setting configurations, turning off unused services, and other actions that reduce the vulnerability or attack surface of a device.
  - **Security logging:** Collecting data useful for identifying security events, either in real time or after the fact.
  - **Patch management:** The ongoing process of keeping software and firmware up to date as new versions are released.
  - **Malware protection:** Defenses against malicious software.
  - **Data integrity protection:** Security controls that prevent the unauthorized injection, modification, or deletion of data.
  - **IDS/IPS:** Those functions that identify a cyberattack in progress and (in the case of IPS) take some action in response to the attack.

Note that there is not a one-to-one correspondence between security features and participating parties that might contribute to their implementation. For instance, the security feature “risk assessment” might be a joint effort between participating parties’ “IT manager” and “business strategy” personnel. Likewise, an “OT manager” might contribute to “access control policies,” “device hardening,” “patch management,” and other security features. Also, job titles vary from organization to organization. Therefore, the “participating parties” entries should be treated as job descriptions (rather than literal job titles).

Profiles can be developed for subsystems within the generation profile. For instance, the physical assets zone of the generation profile may contain multiple subsystems such as the balance of plant distributed control system; generation excitation system; generation protection; and control system. Figure 4 below illustrates the expansion of the generation profile to include several subsystems.

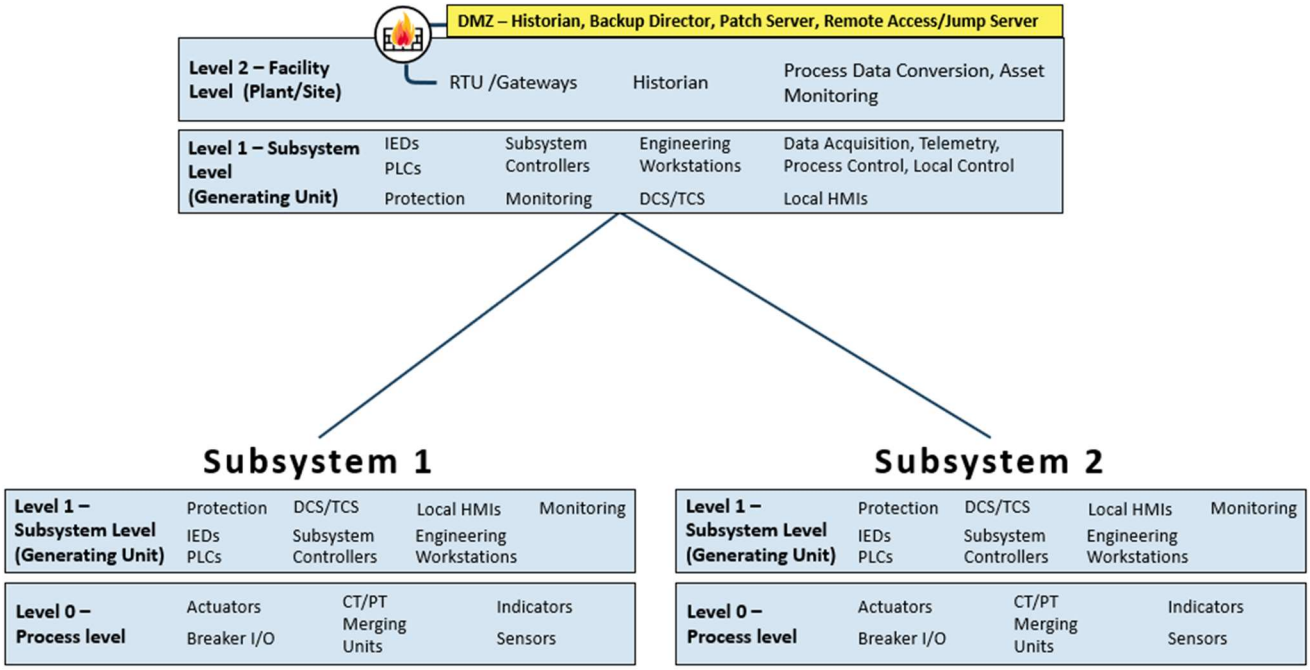

Figure 4. Subsystems of the generation physical assets zone

5.3 Substation

The substation profile, as shown in Figure 5, focus specifically on substations operations.

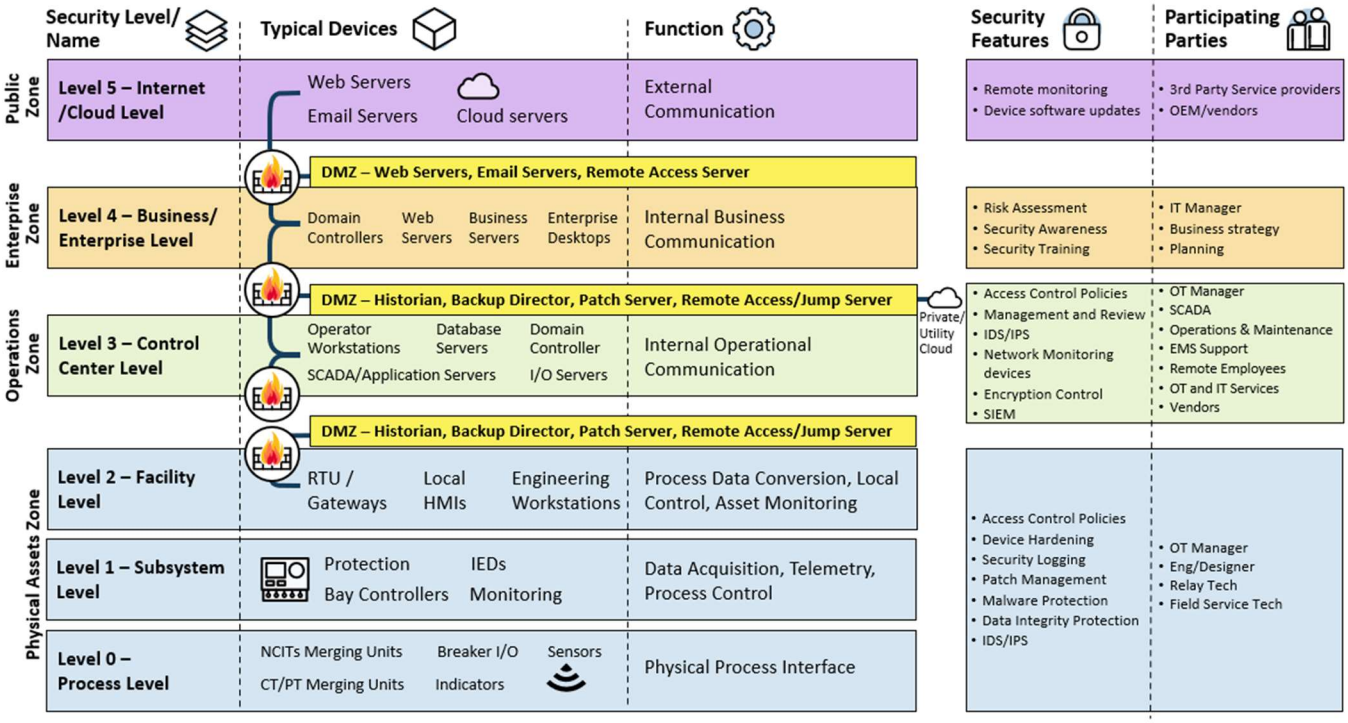

Figure 5. Substation profile

5.4 Distributed Energy Resource (DER)

The DER profile, as shown in Figure 6, must accommodate a large variety of DER technologies including solar, wind, and battery storage. It therefore contains more elements than some of the other profiles discussed here.

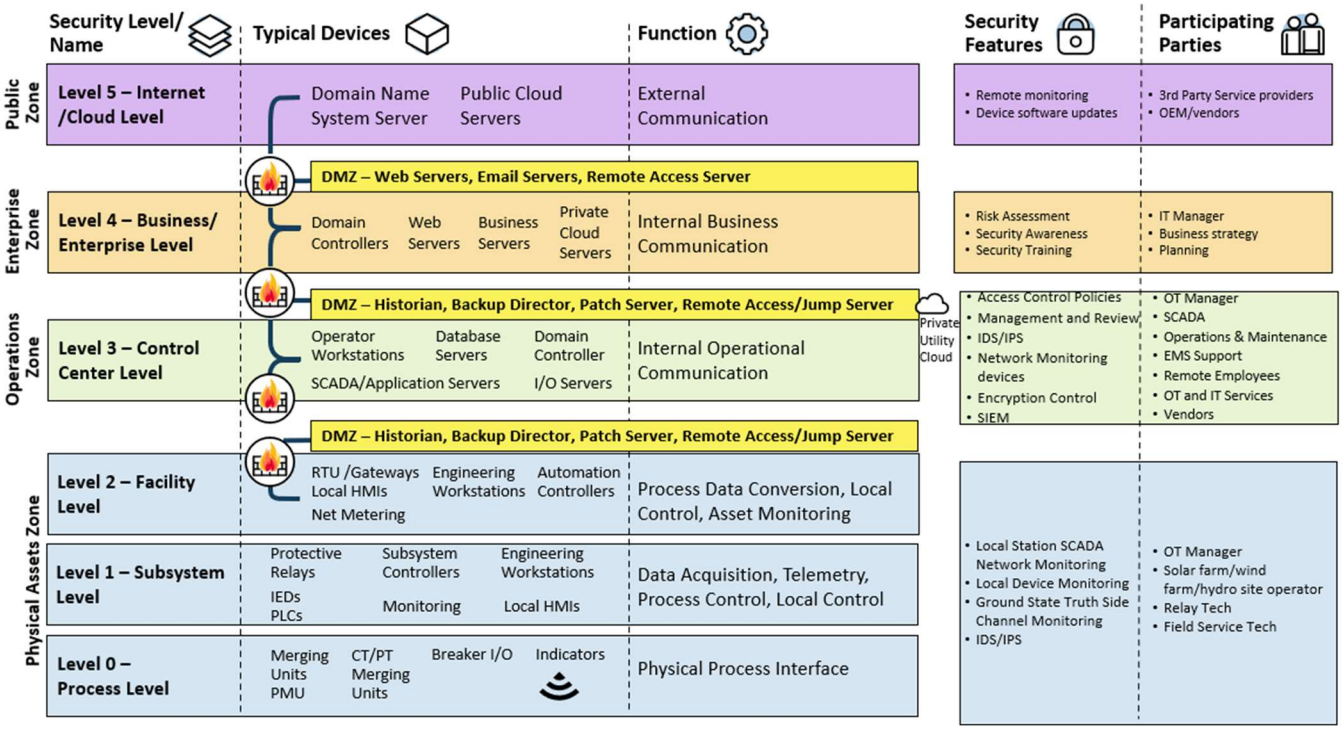

Figure 6. DER profile

5.5 Regional Utility-Scale DER

The regional utility-scale DER profile emphasizes the parallel control structures that may be present in an environment of heterogeneous DER technologies (solar, wind, etc.). Figure 7 illustrates this point, with multiple DER installations controlled from the same Levels 4 and 5. Security features and participating parties are not given for this profile, as they are similar to those in the DER profile for each level. (Note: A more accessible version of Figure 7 can be found at on the SEI ETF website.[13])

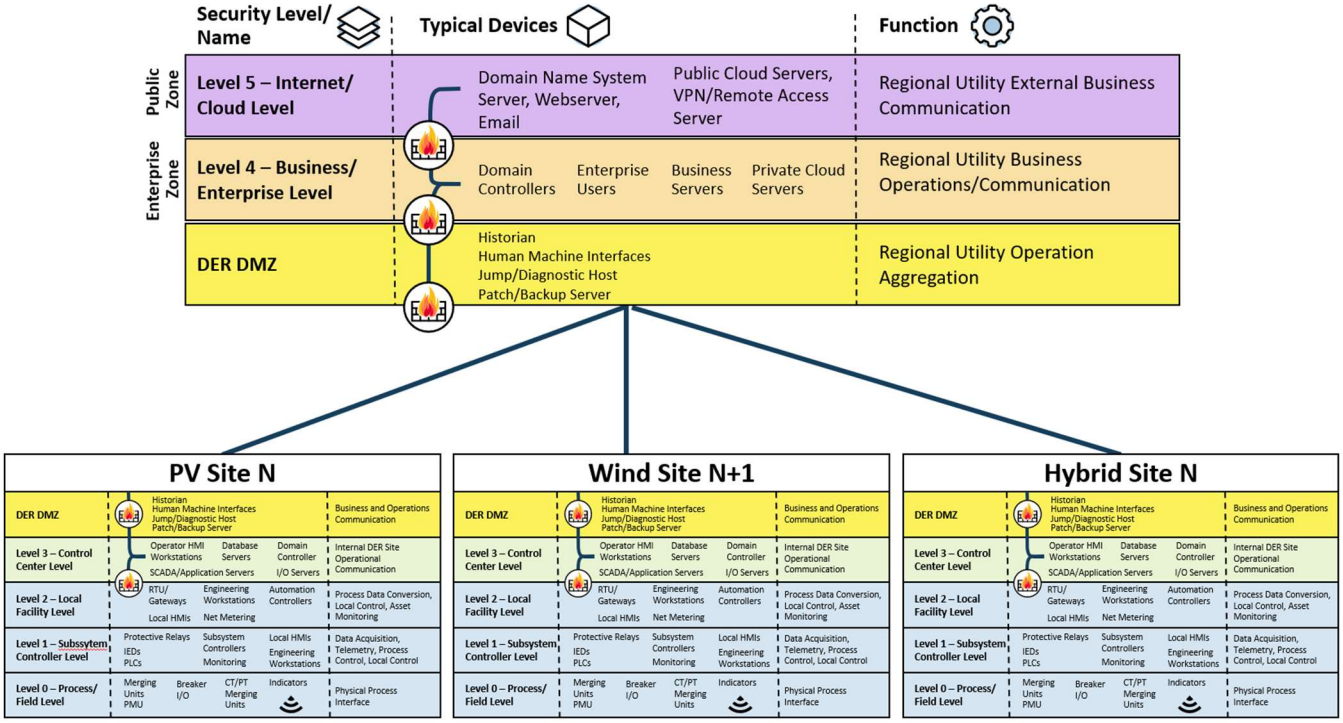

Figure 7. Regional utility-scale DER profile

[13] Office of Cybersecurity, Energy Security, and Emergency Response. March 8, 2022. *Reference Architecture for Electric Energy OT and Accompanying Profile.* https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-Reference-Architecture-for-Electric-Energy-OT-and-Profiles.pdf.

5.6 Control Center

The control center profile, as shown in Figure 8, focuses on Levels 3-5.

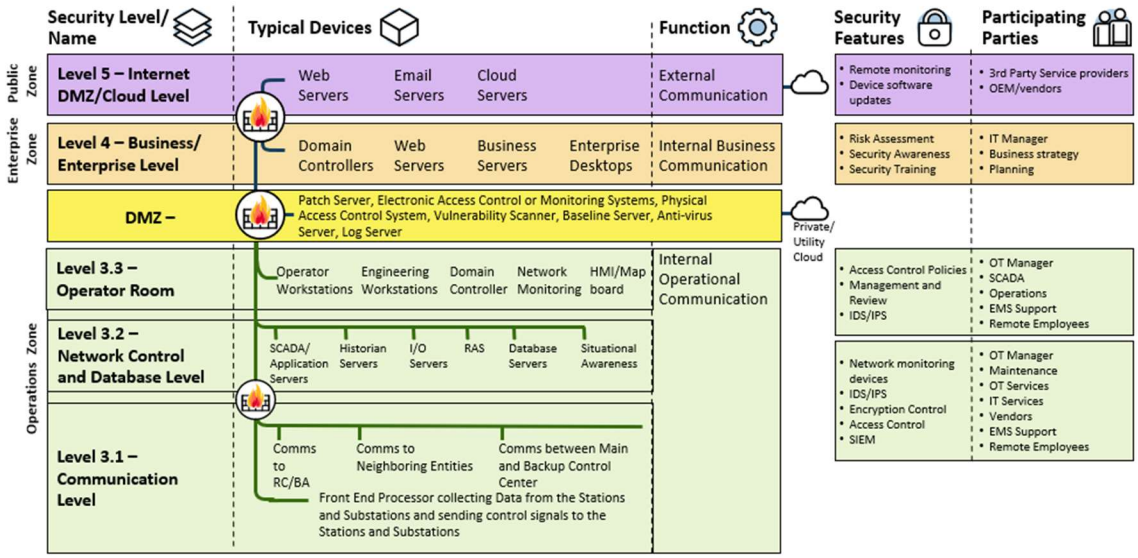

Figure 8. Control center profile

Figure 9 shows how the control center profile can connect to different physical asset zone implementations. (Note: A more accessible version of Figure 9 can be found at the SEI ETF website.[14])

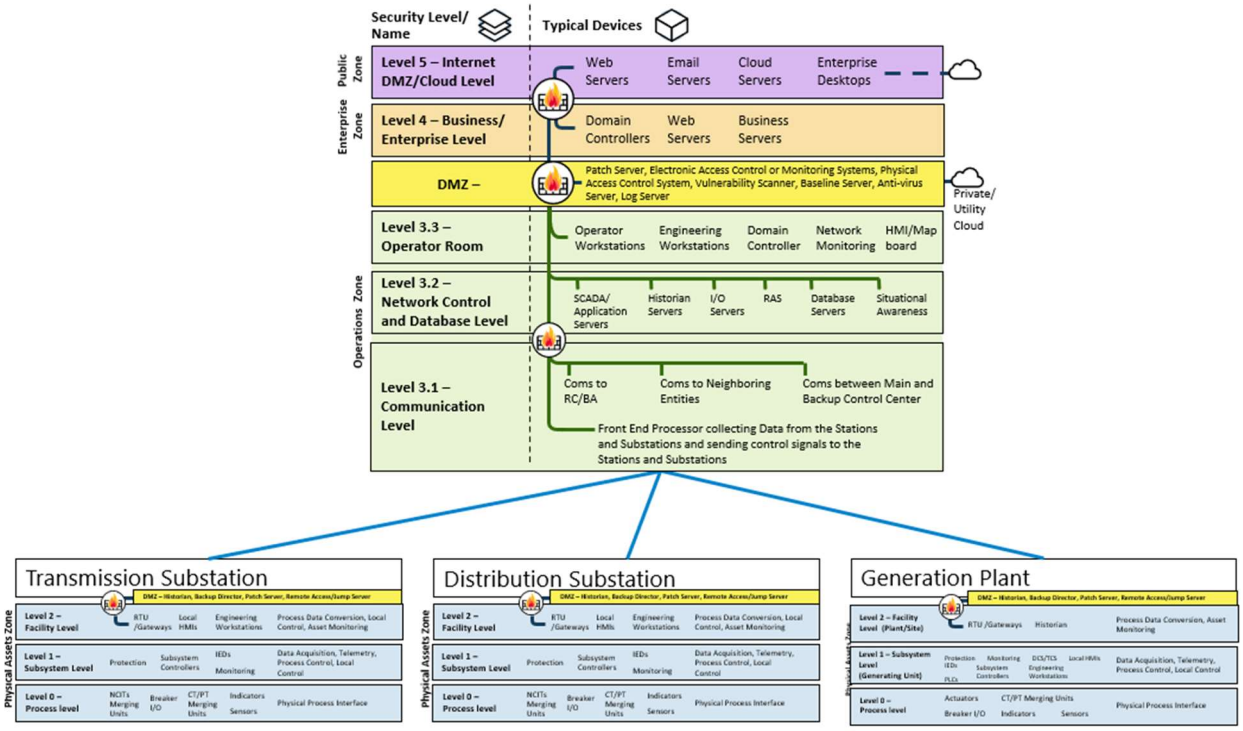

Figure 9. Control center profile with multiple physical zone assets

[14] https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-Reference-Architecture-for-Electric-Energy-OT-and-Profiles.pdf

6. Mapping Standards to the Reference Architecture

As mentioned in Section 2, reference architectures can also be used to assess the coverage of cybersecurity standards for a given part of the electric grid. Graphically overlaying chosen portfolios of standards onto a reference architecture profile illustrates the breadth and depth by which different zones and levels are nominally covered by existing standards. An example of this is shown in Figure 10 below, where several prominent and broadly applicable standards have been overlaid onto the SEI ETF Reference Architecture for Electric Energy OT. All aspects of the profile are covered by at least one standard, and Levels 1 and 2 of the physical assets zone are covered by multiple standards families and individual standards encompassing mandatory and voluntary standards as well as best practices and guides.

While the level of coverage of a chosen set of standards across a particular profile will surely vary, the type of standards matters. Properly applied best practices and guides are generally useful, compliance to voluntary standards is more focused, and mandatory standards with a formal compliance regime should be the most rarely used. It is important to recognize that standards are developed by diverse organizations with different levels of detail and focus on different aspects of security, so more granular analysis (i.e., up to a level of mapping individual requirements or recommendations in each chosen standard to particular devices, functions, security features, and participating parties) is warranted when using this technique to support material security investments.

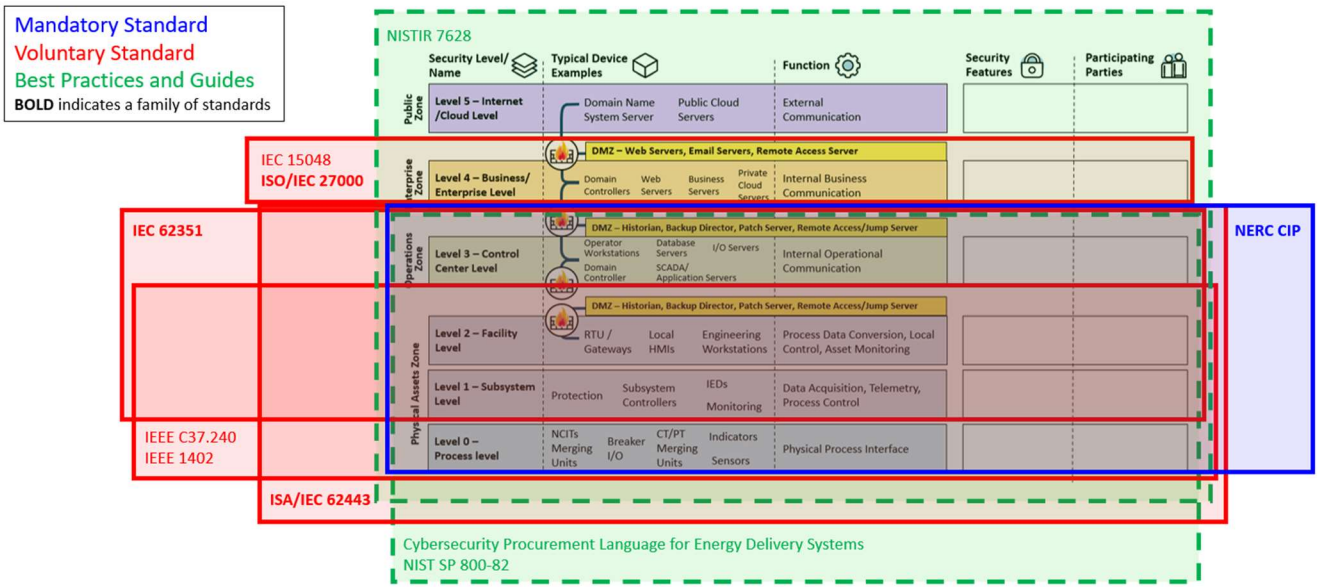

Figure 10. Example mapping of standards onto the Reference Architecture

7. Future Work

This project's work on reference architectures will continue with refinements to the current profiles. SEI ETF would like to have profiles sufficient to cover 95% of today's installed based, while also covering projected future grid systems. For instance, there may be a need for a reference architecture for cloud-based monitoring, control, and security applications and virtualized control systems.

The project will also begin the process of mapping ICS security standards to its reference architectures. After this has been done, the project team will be able to identify any overlaps in standards, as well as insufficient coverage or potentially complete gaps in the standards (those areas of the reference architectures not covered by any standards). This will serve as a basis for discussions regarding the best ways to address these gaps, either by expanding existing standards or by creating new standards to address gaps in current and future systems.