SANDIA REPORT
SAND2022-15760
Printed November 2022

Networked Microgrid Cybersecurity Architecture Design Guide - A New Jersey TRANSITGRID Use Case

Fisayo Sangoleye, Jay Johnson, Adrian Chavez, Eirini Eleni Tsiropoulou, Nicholas L. Marton, Charles R. Hentz, and Albert Yannarelli

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185
Livermore, California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	https://classic.ntis.gov/help/order-methods

Networked Microgrid Cybersecurity Architecture Design Guide - A New Jersey TRANSITGRID Use Case

Fisayo Sangoleye
University of New Mexico
Albuquerque, NM
fsangoleye@unm.edu

Jay Johnson
Renewable and Distributed Systems Integration
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-1033
jjohns2@sandia.gov

Adrian Chavez
Autonomous Cyber Systems
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0672
adrchav@sandia.gov

Eirini Eleni Tsiropoulou
University of New Mexico
Albuquerque, NM
eirini@unm.edu

Nicholas L. Marton
New Jersey Transit
Newark, NJ
nmarton@njtransit.com

Charles R. Hentz
New Jersey Transit
Newark, NJ
chentz@njtransit.com

Albert Yannarelli
New Jersey Transit
Newark, NJ
ayannarelli@njtransit.com

ABSTRACT

Microgrids require reliable communication systems for equipment control, power delivery optimization, and operational visibility. To maintain secure communications, Microgrid Operational Technology (OT) networks must be defensible and cyber-resilient. The communication network must be carefully architected with appropriate cyber-hardening technologies to provide security defenders the data, analytics, and response capabilities to quickly mitigate malicious and accidental cyberattacks. In this work, we outline several best practices and technologies that can support microgrid operations (e.g., intrusion detection and monitoring systems, response tools, etc.). Then we apply these recommendations to the New Jersey TRANSITGRID use case to demonstrate how they would be deployed in practice.

Acknowledgment

The team would like to thank the New Jersey Transit for supporting the development of this report, especially Rafi Khan, Chief Information Security Officer, John Franciscone, Senior Director - Cybersecurity Architecture & Engineering, and Miguel Teixeira, Senior Director - Cybersecurity Governance, Risk, and Compliance, who each provided thoughtful reviews of this material.

CONTENTS

LIST OF FIGURES

Nomenclature

ACL Access Control Lists

AGC Automatic Generation Control

AIC Availability, Integrity, Confidentiality

AMI Advanced Metering Infrastructure

ARP Address Resolution Protocol

CCI Control Correlation Identifiers

CETC Central Electrification and Traffic Control

CFE Communication Front End

CIA Confidentiality, Integrity, Availability

CPU Central Processing Unit

CSET Cyber Security Evaluation Tool

CSF Cybersecurity Framework

DCS Distributed Control System

DER Distributed Energy Resources

DERCF Distributed Energy Resources Cybersecurity Framework

DERMS Distributed Energy Resources Management System

DG Distributed Generation

DHCP Dynamic Host Configuration Protocol

DHS Department of Homeland Security

DMZ Demilitarized Zone

DNP3 Distributed Network Protocol 3

DNS Domain Name System

DoD Department of Defense

EDR Endpoint Detection and Response

EMS Energy Management System

ES-C2M2 Electricity Subsector Cybersecurity Capability Maturity Model

FTP File Transfer Protocol

GE General Electric

GMS Generation Management System

HIDS Host-based Intrusion Detection System

HIPS Host-based Intrusion Prevention System

HMI Human-Machine Interface

HSE Health, Safety, and Environment

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

IBN Intent-Based Networking

ICCP Inter-Control Center Protocol

ICS Industrial Control Systems

IDS Intrusion Detection System

IED Intelligent Electronic Device

IIoT Industrial Internet of Things

IM Interdependent Microgrid

IP Internet Protocol

IPS Intrusion Prevention System

IPSec Internet Protocol Security

IT Information Technology

LLC Limited Liability Company

MAC Media Access Control

MCF Microgrid Control Facility

M&E Morrison Essex

MFA Multi-factor Authentication

MODBUS Modicon Communication Bus

MTD Moving Target Defense

NEC Northeast Corridor

NGFW Next-Generation Firewall

NIDS Network-based Intrusion Detection System

NIPS Network-based Intrusion Prevention System

NIST National Institute of Standards and Technology

NJ New Jersey

NJT New Jersey Transitgrid

NM Networked Microgrid

NREL National Renewable Energy Laboratory

OPC Open Process Communications

OSI Open Systems Interconnection

OT Operational Technology

PDP Policy Decision Point

PEP Policy Enforcement Point

PJM Pennsylvania-New Jersey-Maryland

PKI Public Key Infrastructure

PLC Programmable Logic Controller

PMU Phasor Measurement Units

PSE&G Public Service Enterprise Group

PV Photovoltaic

RMF Risk Management Framework

ROC Rail Operations Center

RTU Remote Terminal Unit

SCADA Supervisory Control and Data Acquisition

SDN Software Defined Networking

SDP Software Defined Perimeter

SEM Security Event Monitoring

SFTP Secure File Transfer Protocol

SIEM Security Information and Event Management

SIM Security Information Management

SIRP Security Incident Response Platforms

SMTP Simple Mail Transfer Protocol

SOA Security Orchestration and Automation

SOAR Security Orchestration, Automation and Response

SOC Security Operations Center

SSH Secure Shell

SSL Secure Sockets Layer

SQL Structured Query Language

SYSLOG System Logging Protocol

SYSLOG-NG System Logging Protocol Next-Gen

TCP Transmission Control Protocol

TIP Threat Intelligence Platforms

TLS Transport Layer Security

TTP Tactic, Technique, or Procedure

UDP User Datagram Protocol

UFC Unified Facilities Criteria

UNIX Uniplexed Information and Computing Service

UPS Universal Power Supply

VLAN Virtual Local Area Networks

VMA Virtual Management Appliance

VPN Virtual Private Network

WAF Web application Firewall

WAN Wide Area Network

WEC Windows Event Collector

WEF Windows Event Forwarding

WINRM Windows Remote Management

XDR Extended Detection and Response

XSS Cross-Site-Scripting

ZTA Zero Trust Architecture

1. INTRODUCTION

A microgrid is a group of interconnected loads and distributed energy resources (e.g., wind turbines, diesel or natural gas gen-sets, photovoltaic systems, batteries, flywheels, etc.) within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in both grid-connected or island mode [1]. Microgrids are often designed as a backup source of electricity for critical loads (e.g., hospitals, emergency service centers, etc.) in the event of an emergency (e.g. a power outage or an adversarial attack) [2], and this makes them a target for adversaries looking to cause disruption. Adversarial manipulation of the microgrid industrial control system (ICS) will disrupt control actions and optimization functions, and likely cause microgrid load outages.

Recently, there has been a growing interest in deploying networked microgrids. *Networked Microgrids (NMs)* are two or more microgrids interconnected at the power/physical layer with communication and control capabilities. By taking advantage of control, automation, and communication capabilities, NMs are able to increase reliability, resilience, scalability, and diversity of loads and generation assets [3, 4].

In this work, we introduce a new term, *Interdependent Microgrids (IMs)*, which are two or more microgrids interconnected at the networking/communication layer. As opposed to being electrically coupled like NMs, IMs can operate more efficiently or reliably by exchanging information with other microgrids in the area. One example of this situation is a microgrid that powers a rail line and another that powers a rail station along that line. If the rail line microgrid is de-energized, loads at the rail station will likely be much lower. Similarly, if the station microgrid is unpowered, the rail lines will not stop at this station and this will change the loads expected by the microgrid powering the rail line.

Substantial research has been performed to study the benefits of NMs, including designing resilience into the system [5, 6, 7], energy management, optimization, power sharing, and scheduling [8, 9, 10, 11, 12, 13, 14], voltage and frequency control [15, 16], and restoration [17, 18]. There has also been prior work to create a benchmark system for comparing and testing optimal power flow, energy management, control, stability, and protection [19]. However, there has been less attention to different approaches to secure communications in NMs or IMs.

As shown in Fig. 1-1, NMs represent multiple, dependent microgrids which are controlled with a high-level controller. The microgrids can island during a grid outage individually or as a group to provide additional reliability for the entire islanded system. The microgrid controller maintains stability, protection/control, and energy management by communicating with the DER equipment using a DER management system (DERMS), the protection equipment (e.g., relays) using a protection control system [20], and other Supervisory control and data acquisition (SCADA) equipment

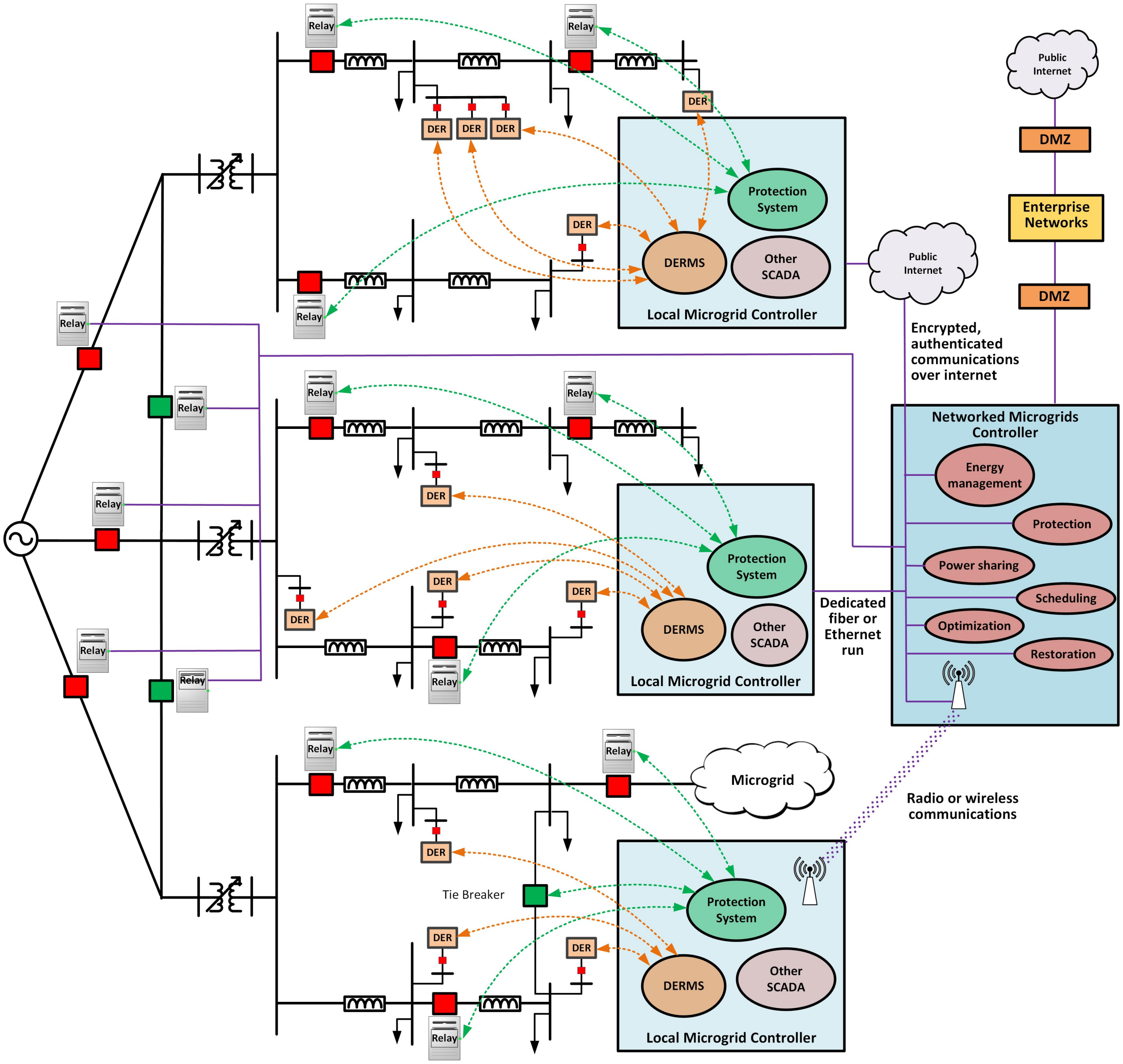


Figure 1-1. Microgrid Network Logical Architecture

like phasor measurement units (PMU) and advanced metering infrastructure (AMI). The same networking architecture would exist for IMs.

At the higher level, control systems for NMs/IMs must have real-time communications to coordinate the individual microgrids for power sharing and economic optimization. The NM/IM controller must also include the ability to dynamically transition to any other NM/IM operating modes and grid topologies by communicating these changes to the individual microgrid controllers and relays that manage microgrid interconnections. Two centralized or distributed NM/IM controller communication design possibilities include client/server architectures or publish/subscribe approaches [21]. In either case, local microgrid DER/Protection/SCADA communications must be secured to the local microgrid controllers [22, 23] and secured upstream to the higher-level NM/IM controller(s).

The challenge is that microgrid and other ICS systems have historically been installed in physically secure areas and disconnected from wide-area networks; as a result, microgrid and networked microgrid control systems are generally not designed with cybersecurity in mind [22]. What makes securing NMs/IMs even more challenging is that the individual microgrid systems may be spread over a larger geographical area–sometimes without dedicated communication lines between the sites–and each microgrid is typically running isolated but poorly-secured industrial control systems running proprietary or legacy control protocols with specialized software and hardware. In some cases, connections to these systems may be performed over the internet using encrypted VPN, SSH, or other connections, as is common for large wind and solar installations today. This requires a zero-trust architecture where all accessible endpoints/assets authenticate and authorize users, as opposed to primarily securing systems with perimeters [24].

NM/IM controllers and facilities will also need to connect with business/enterprise networks in order to facilitate business and administrative operations. Integrating the Operational Technology (OT) system with IT environments provides many benefits including remote access and monitoring, grid interactivity, and cross-enterprise optimization. However, the OT/IT convergence [25] also expands the attack surface of the microgrid, and these new attack vectors must be carefully defended [26]. If the IT systems must be connected to the NM/IM controller, it is possible to establish a DMZ between IT and OT networks to ensure adversaries are prevented from crossing this boundary.

It is also essential to design cyber-hardening technologies into NMs/IMs which provide security operators with visibility, anomaly detection tools, and defensive options to respond to attacks. These technologies may include the NIST Cybersecurity Framework (CSF) functions listed below [27]:

1. **Identification** - Understanding, categorizing, and documenting the control network, systems, data, and assets, in order to effectively manage cybersecurity risks [27].

    - Create Risk Management Framework for the organization.
    - Define a governance program for legal and regulatory requirements.
    - Identify critical functions and document potential risks to them.
    - Document all digital assets (hardware and software) in the IT and OT networks and establish an asset management program.
    - Determine potential threats, vulnerabilities, and response strategies.
    - Create Supply Chain Risk Management strategy with risk tolerances.

2. **Protection** - Network security implementations, policies and procedures designed to protect cyber-physical systems from cyberattacks.

    - Deploy stateful firewalls which track active network connections and intrusion prevention systems to protect against malware.
    - Establish demilitarized zones (DMZs) and network segmentation at different levels of the system.

   - Use dedicated networks for critical applications.

   - Where possible, update communication protocols with enhanced security technologies.

   - Encrypt sensitive data flows.

   - Implement access control with least privileged principles and multi-factor authentication.

   - Implement whitelisting, which is considered more secure than blacklisting [28].

   - Add unidirectional gateways and data diodes to isolate critical components and prevent two-way communication where applicable.

   - Use jump hosts and multi-factor authentication for remote connections and facilities.

   - Disable unused connections, ports, components, and applications which could be used as attack surfaces.

   - Mandate timely and periodic patching of operating systems and applications.

3. **Detection** - This stage involves situational awareness and real-time monitoring of systems and processes in order to identify attacks.

   - Use antivirus and intrusion detection systems (HIDS and NIDS) to detect anomalies and malicious behaviors.

   - Implement continuous, centralized system monitoring and event logging (e.g. SIEM tools).

   - Maintain situational awareness of system operations.

   - Conduct regular threat-hunting activities and update scanning tools based on new threat intelligence.

4. **Response** - This includes plans and processes put in place to respond to attacks and incidents.

   - Implement incident response and cyber-physical remedial action schemes to contain the incident.

   - Manage communications with the internal team, law enforcement, and external stakeholders as appropriate.

   - Create isolation and containment plans for compromised systems/hosts in the case of an attack. As an example, this may include changing the network topology using Software Defined Networking/Moving Target Defense.

   - Perform forensic analysis to identify the source of the attack in order to fully resolve the incident.

   - In the event that a cyberattack impacts the power system or rail, bus, or ferry operations, pre-planned remedial actions should be deployed to get the system operational.

- Where applicable, containerized systems can be quickly reconstructed from known good images.

5. **Recovery** - Measures by which to recover and restore system functionality to the state it was before the attack.

    - Execute the recovery plan, incorporate lessons learned, and update recovery strategies.
    - Manage public relations by communicating internally and externally about recovery activities.

Herein we present a collection of best practices for securing a collection of microgrid OT networks. This primarily focuses on the network devices and topology required to protect the microgrid. Other requirements from the NIST CSF and other best practices, guides, and standards should be consulted to generate comprehensive cybersecurity strategies for specific NM/IM applications. The remainder of the report is structured as follows. Chapter 2 discusses the design of a logical cybersecurity architecture for NMs/IMs, considering defense-in-depth techniques. Chapter 3 describes the New Jersey TRANSITGRID project use case and details the design considerations for the NJT logical cybersecurity architecture. Chapter 4 discusses some key architectural cyber-hardening technologies, Chapter 5 explores some operational cyber-hardening technologies, and Chapter 6 concludes the paper.

2. SECURE NETWORKING DESIGN

This section details our approach to designing a cyber-secure architecture for NMs/IMs. Our cybersecurity architecture for NMs/IMs takes a holistic approach by considering the two primary security zones of the microgrid systems: (a) the Information Technology (IT) networks that include business and enterprise operations and (b) the Operational Technology networks that operate each of the NM control systems, as well as networks providing communications between NMs/IMs. Our design implements the following defense-in-depth measures:

1. Deploying paired firewalls from different vendors, and intrusion detection systems to protect against malware [28].
2. Establishing demilitarized zones (DMZs) and network segmentation at different levels for extra security.
3. Implementing a logically separated microgrid control network.
4. Use of unidirectional gateways and data diodes where necessary, to isolate critical components and prevent two-way communication.
5. Use of jump hosts and multi-factor authentication for remote connections to facilities.

Unfortunately, IT security solutions are not applicable to ICS/OT environments due to the differences in how these systems are designed, their performance and reliability requirements, and their modes of operation. In fact, many IT security tools may disrupt OT environments, e.g., scanning certain control systems may cause them to reboot or misoperate [29]. Therefore, all security measures and technologies have to be carefully configured in the OT environments to prevent control function disruptions or misoperations [30].

2.1. Application of Risk Management Frameworks to Define Security Features

The security of the NM/IM networks should be designed based on the risk tolerance of the owners, operators, and other stakeholders. The question is "How can the appropriate network security features be selected for the NM/IM?". There are multiple approaches for selecting security controls based on the organization's risk tolerance. Risk is a broad measure of the extent to which adverse impacts would arise if an event occurs, and the likelihood of that occurrence [31]. Assessing risk is challenging, but if time is taken upfront to discuss and document the threats and consequences in terms of risk tolerance, assumptions, constraints, priorities, tradeoffs, and uncertainty, the system can be designed with the appropriate security controls. The Department of Defense (DoD) Unified Facilities Criteria (UFC) 4-010-06, *Cybersecurity of Facility-Related Control Systems* [32], describes a Risk Management Framework (RMF) in a five-step process: (1) selecting the impact levels (low, moderate, high) for the confidentiality, integrity, and availability of the control system, (2) selecting the proper NIST SP 800-82 controls, (3) listing the DoD Control Correlation Identifiers (CCIs) [33] for the controls, (4) identifying CCIs that require input from the designer, and (5) including the cybersecurity requirements in the project specification. The NIST RMF (SP 800-37 Rev. 2) has a similar approach, wherein the security controls are selected based on impact analysis of the system and information that is processed, stored, and transmitted [34]. These approaches stretch across the entire lifecycle of the system as opposed to the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) [35], DHS Cyber Security Evaluation Tool (CSET) [36], or NREL's Distributed Energy Resource Cybersecurity Framework (DERCF) [37], which are tools for evaluating as-built installations or as-designed systems. RMFs are especially useful in the design process, where high-level architectural and difficult cost-benefit decisions are made based on the risk profile for the system.

For the following reference NM/IM security architecture, we have not completed the risk management process because this will change site-to-site and stakeholder-to-stakeholder. Instead, we adopted best industry networking practices into a template for NMs/IMs. This design should be modified based on site needs, resources, and risk frame.

2.2. Design Considerations

In the report "Microgrid Cyber Security Reference Architecture (V2)" [38], Stamp *et al.* designed a microgrid cybersecurity reference architecture which leveraged defense-in-depth techniques to secure the data exchanges required for microgrid operations. Defense-in depth is a multi-layered defense approach where security measures are applied at different levels, ensuring that a single compromised or misconfigured component does not compromise the systems [22, 38, 39]. The Microgrid Cyber Security Reference Architecture was an improvement on traditional flat ICS networks because it segmented the microgrid control system network into enclaves, then into functional domains, making it difficult for an attacker who gains access into the control network to move laterally and compromise other systems. This architecture is created to prevent common OT vulnerabilities such as [28]:

1. **Connections to internet and external networks** - Microgrid control network is insecurely interfaced with the enterprise network or internet to facilitate monitoring and administrative functionalities.

2. **Misconfigurations** - Improper internal perimeter configurations, security applications, or other hardware/software. For example, misconfigured firewall rules would allow lateral movement post-breach.

3. **Insecure remote access connections** - Poor management or configuration of remote access to the control system, e.g., lack of authentication, active but unused connections and ports, etc.

Our logical network design builds on the defense-in-depth methodology to prevent these issues by creating a network that is simplistic, segmented, monitored, and independent:

- Simplistic: This involves prioritizing system functionality and operation during security design consideration. While traditional IT systems are designed to ensure Confidentiality, Integrity, and Availability (CIA Triad), in that order of priority, industrial control systems are the opposite, embracing the reverse order of priority - Availability, Integrity, and Confidentiality (AIC Triad). This is because, information technology (IT) security systems are designed with the goal of protecting critical and sensitive information such as users' personal records, financial information, intellectual property, etc., whereas, industrial control systems (ICS) are designed with a focus on enhancing the industrial process, and ensuring maximum availability and integrity. It is important for an industrial control system to stay up and running without interruptions or unexpected downtime (availability), and for information being passed across to be without errors or alterations (integrity), any of which could impact industrial operations negatively. Designing the network infrastructure to be simple makes it easy to implement changes, fix errors, monitor processes and control operations. This means implementing a functionality-based segmentation, and ensuring that while deploying and configuring hardening tools, such as firewalls, intrusion detection and prevention systems (IDS/IPS), and encryption technologies, the smooth operation of the IDS processes is not negatively impacted.

- Segmented: Segmentation involves the separation of systems and components into different logical groups, domains, or enclaves based on properties, such as communication protocols, uniform policies, network traffic, level of trust, functionalities, interdependencies, security requirements, criticality of operations, vulnerabilities, etc. This ensures that a compromised system does not give attackers the freedom of moving through the network and infecting other systems. With proper segmentation in place, security implementations such as authentication, firewalls, intrusion detection and prevention, encryption, system monitoring, event logging, and digital forensics are easier to implement. Segmentation helps to enforce boundaries and minimize access to sensitive information by establishing rules that define how information and communications are allowed through boundaries. According to [28], segmentation can be implemented in the following ways:

  - Logically through Virtual Local Area Networks (VLANs), encrypted Virtual Private Networks (VPNs), and through unidirectional gateways that ensure communication only flows in one direction.

  - Physically through air gaps which completely prevent connection or flow of traffic between network domains.

  - Traffic filtering at the (a) network layer, based on IP and route information, (b) application layer, based on application level firewalls, proxies, and content-based filtering, (c) port/protocol level, based on service type, and (d) state-based filtering, based on operation state and functions.

- Monitored: System monitoring and event logging should be implemented in a way that does not impact industrial operations. Monitoring systems should be designed across different segments of the network, collecting and logging system and process information within the segment they are deployed. This reduces the overhead of logging and processing aggregated information across the whole network by a single monitoring system and the rate of false positives that might arise with the monitoring of unrelated processes by a single system.

- Independent: Systems are segregated into different independent logical groups based on their functions and processes as if they exist alone. This would make the microgrid control system more resilient to attacks. In the event of a compromise of one of the systems, the rest of the control network can continue performing their functions, while the compromised system is isolated until the attack is resolved.

Additionally, since NMs/IMs must operate during power outages, all networking and control equipment must be powered with alternative sources. This generally means that cloud-based assets, Industrial Internet of Things (IIoT), and other devices are not appropriate because, when power is lost, there will be no internet connectivity. Instead, critical connectivity within and between the microgrids must be provided with microgrid power, universal power supplies (UPSs), or other means–depending on the NM/IM design requirements for islanded operations.

2.3. The Networked Microgrids Network Logical Architecture

We design our logical architecture as shown in figure 2-2, based on the Purdue Model for control hierarchy [40]. The Purdue Model is a widely adopted reference model in the industrial control system (ICS) industry [41, 42], which uses the concept of hierarchy to segment devices and systems in the ICS into logical zones based on their functionalities and network requirements. It separates the ICS network from the enterprise network by using a demilitarized zone in-between (Enterprise/ICS DMZ), which limits the degree of connection between both networks, regardless of their interdependencies. The enterprise network, due to its business and administrative functions, allows extensive traffic such as internet (HTTP), file transfers (FTP), email (SMTP), etc., which should not reach the ICS network because of the risk of impacting control operations. If the enterprise and ICS networks must communicate for certain reasons, it is advised that the number of entry points is limited, and there should be no direct connection between both networks [43]. With the implementation of the Enterprise/ICS DMZ, in the event that the enterprise network gets compromised, the systems in the control network will not be affected and will continue with their normal operations uninterrupted. In addition to the separation of the enterprise network from the control network, further hierarchical segregation is employed within the control network, in order to separate different systems and components into logical groups, based on the functions they perform. Several technologies now allow logical grouping like Cisco TrustSec Security Group Tagging, which provides software-defined network segmentation [44], and OpShield from GE Digital [45], which handles OT network flows with hardware or Virtual Management Appliances (VMAs).

2.3.1. The Enterprise DMZ

The enterprise network needs to connect to the internet for e-mail, browsing, remote access, FTP, etc. While this is necessary to facilitate business operations, it is important to ensure that these external communications do not expose the enterprise network to external attacks. To protect the enterprise network, we create an enterprise DMZ [43] as shown in figure 2-3, which acts as an extra

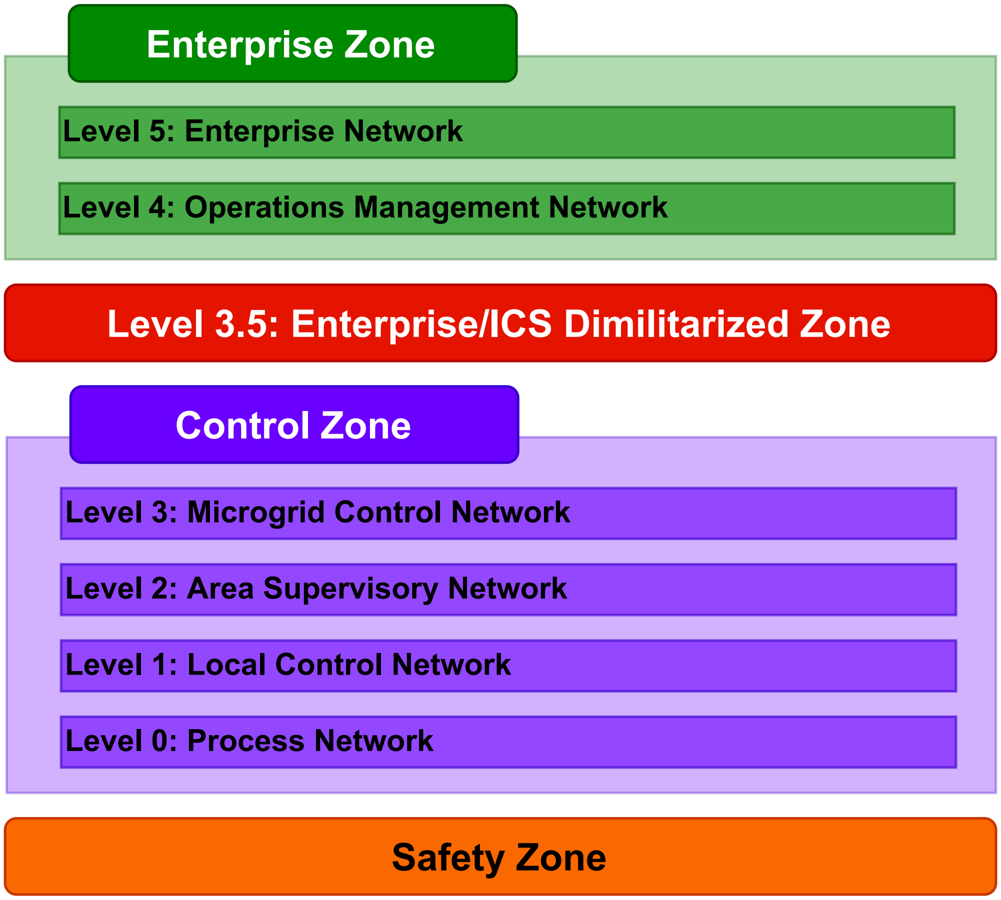

Enterprise Zone
Level 5: Enterprise Network
Level 4: Operations Management Network
Level 3.5: Enterprise/ICS Dimilitarized Zone
Control Zone
Level 3: Microgrid Control Network
Level 2: Area Supervisory Network
Level 1: Local Control Network
Level 0: Process Network
Safety Zone

Figure 2-1. Microgrid Network Logical Architecture

layer of protection between the internet and the enterprise network, which houses bastion hosts that need to be exposed to the internet, such as e-mail gateways, Web, VPN, DNS, and FTP servers, etc. The enterprise DMZ ensures that there is no direct connection between the outside world and the enterprise network which provides access control benefits, foils network reconnaissance, and prevents IP spoofing. Internet traffic that needs to reach the enterprise system (e.g., when hosting the microgrid website) is processed by the servers in the DMZ network. Outgoing traffic is also sent to the DMZ before they are forwarded to the external network. This layered security approach makes it difficult for an intruder to make it past the DMZ and into the enterprise network without being detected. In some cases, the enterprise DMZ may be replaced with a single firewall, if sufficient protections are provided in other ways (e.g., reverse proxies for web servers, safe links, NIDS).

Network design considerations:

- Segregated DMZs: Depending on design requirements, the enterprise DMZ could be further hardened by separating it into smaller independent DMZs based on functionalities [28]. As seen in figure 2-3, each of the DMZs exists independently. This would prevent lateral movement risks by ensuring DMZ assets are individually protected in case one of them gets compromised.

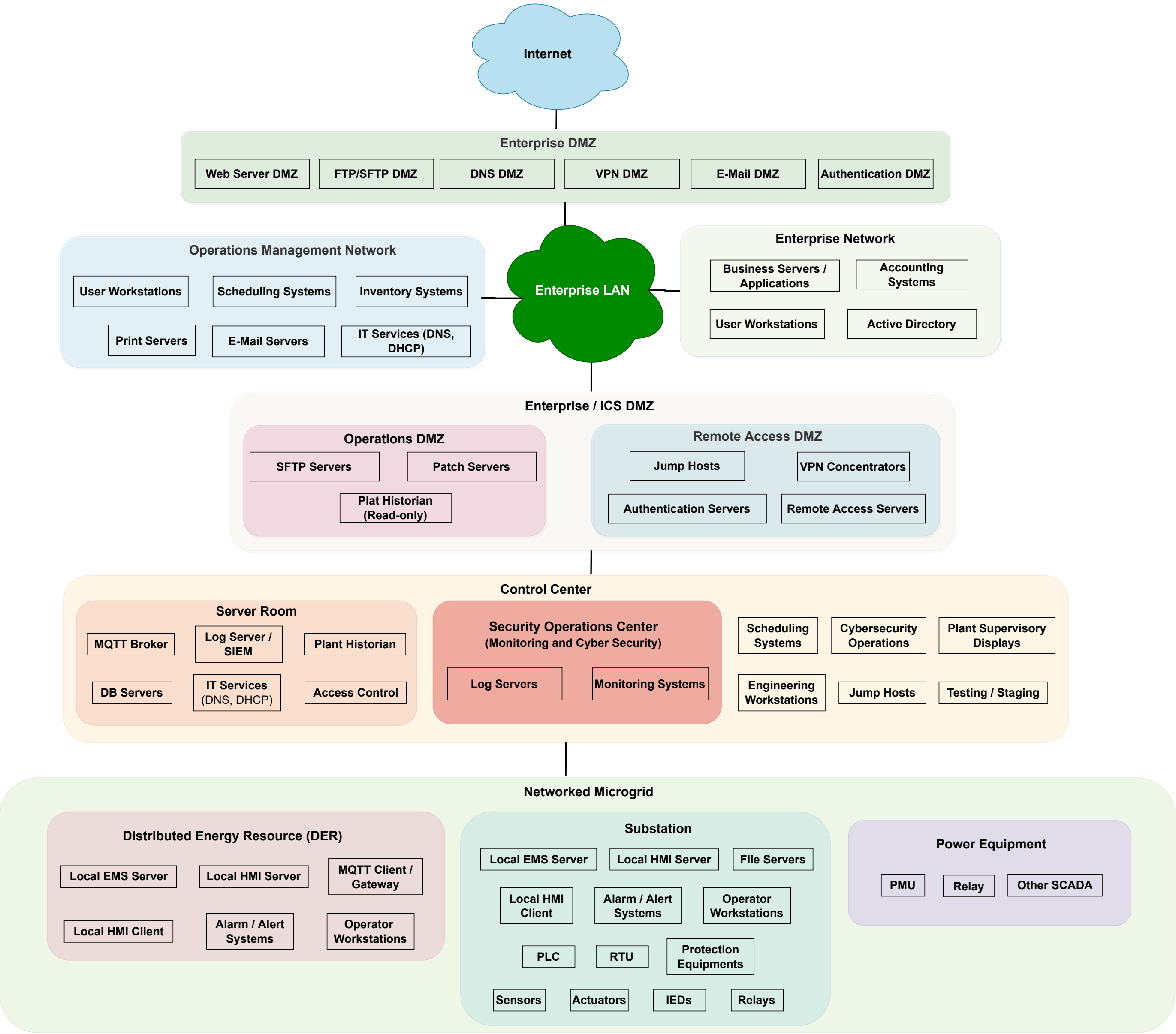


Figure 2-2. Overall Network Overview

- Firewalls: Web application Firewalls (WAFs) could be used to protect web applications on the enterprise network from attacks such as SQL injection, cross-site scripting (XSS), file inclusion, etc. By deploying a WAF in front of a web application, it acts as a shield, filtering and monitoring HTTP traffic between the internet and the web application [46]. A system of layered firewalls could also be used, such as a packet filtering router or firewall followed by a next-generation firewall (NGFW) for different levels of packet inspection. With the high volume of incoming external traffic, the packet filtering firewall could first filter out some easily detectable malicious packets, before the next generation firewall performs a deeper packet inspection on the filtered traffic. This helps reduce the delay or congestion that could occur if the NGFW had to perform deep packet inspection on every single packet that comes from the internet. [28]

- IDS: An intrusion detection system is used in the DMZ as an extra layer of protection.

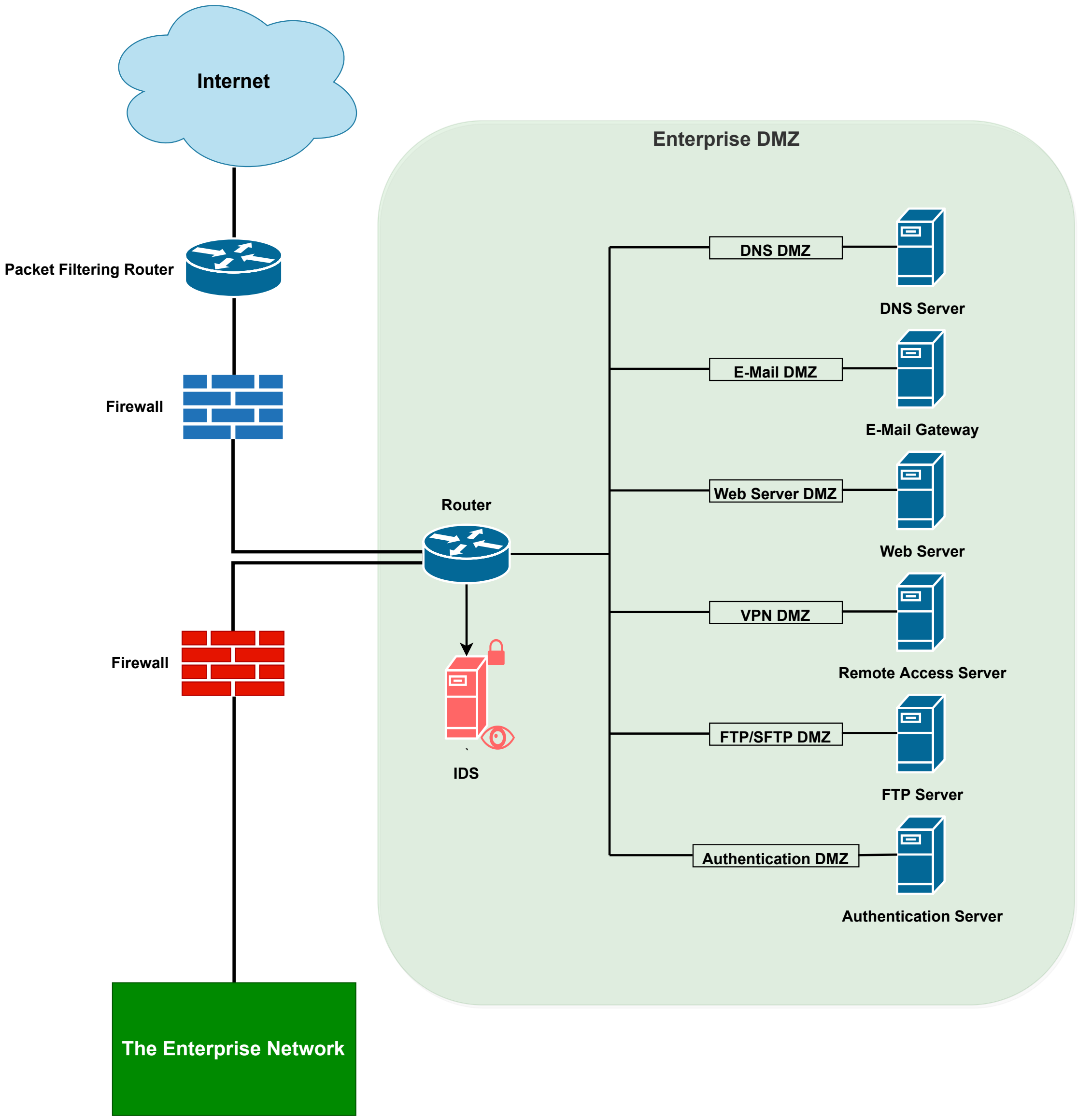


Figure 2-3. The Enterprise DMZ

2.3.2. Enterprise Zone - Levels 4-5

The enterprise zone 2-4, while not part of the ICS, relies on the control network's data for its operations and may need to make changes to OT operations (e.g., adjust generation based on updated fuel prices). The enterprise network houses the corporate IT infrastructure, systems, and applications at Level 5. IT services such as web hosting, email servers, VPN, remote access, active directory, and other enterprise applications exist in this zone. The Security Operations Center

(SOC) is located at Level 5 because it needs to collect real-time threat intelligence from the internet, acquire evolving information on attacks, reach out to external parties (law enforcement), etc. The SOC also helps to monitor control systems by gathering network and process data from the control network in order to provide quick detection and response during security incidents. Since the SOC receives information from both the internet and the control network, strict security measures (such as the use of DMZs, unidirectional gateways, etc.) must be taken to ensure that the SOC does not introduce a security vulnerability into the control network.

Level 4 is the operation management network, where administrative and business operations are performed. Some of them include usage monitoring and reporting, billing, inventory management, scheduling, capacity planning, e-mail, printing, etc. IT monitoring and logging operations are also performed in this zone.

Network design considerations:

- Boundary Firewalls: Firewalls are recommended as enforcement boundaries or gateways between the enterprise network and the upstream and downstream DMZs. This ensures that communication flowing in and out of the enterprise zone is checked and controlled.

- It is also recommended to separate the enterprise network into different functional sub-nets using VLANs or firewalls. This ensures extra protection for essential systems like monitoring and logging, databases, authentication servers, etc.

- Intrusion detection systems (Host-based and Network-based) are used as an extra layer of detection and defense.

2.3.3. The Enterprise/ICS DMZ - Level 3.5

While designing the microgrid control system network, it is important to ensure that the control network is well isolated from the enterprise network. The enterprise network operates differently from the control network and their requirements are different. The enterprise network has to communicate with external systems through the internet, e-mail, etc. Generally, enterprise computers are modern, patched Windows and Mac computers, well-equipped for interacting with external environments. Control system devices on the other hand are typically running Linux, Unix, or other operating systems continuously for 10+ years and must be protected from enterprise network traffic [47]. Attacks on industrial control systems and machines could cause life-threatening or other high-consequence events, hence, it is critical to ensure that direct communication between the enterprise and control networks is managed. This is implemented using a demilitarized zone (DMZ) 2-5 between the IT and OT networks. The system could be configured in a way that ensures all traffic from either side terminates at the servers in the DMZ, with no direct connection between both networks. The DMZ would typically be comprised of shared historian servers, remote access servers, jump-hosts, authentication servers, patch servers, FTP/SFTP servers, etc.

Network design considerations:

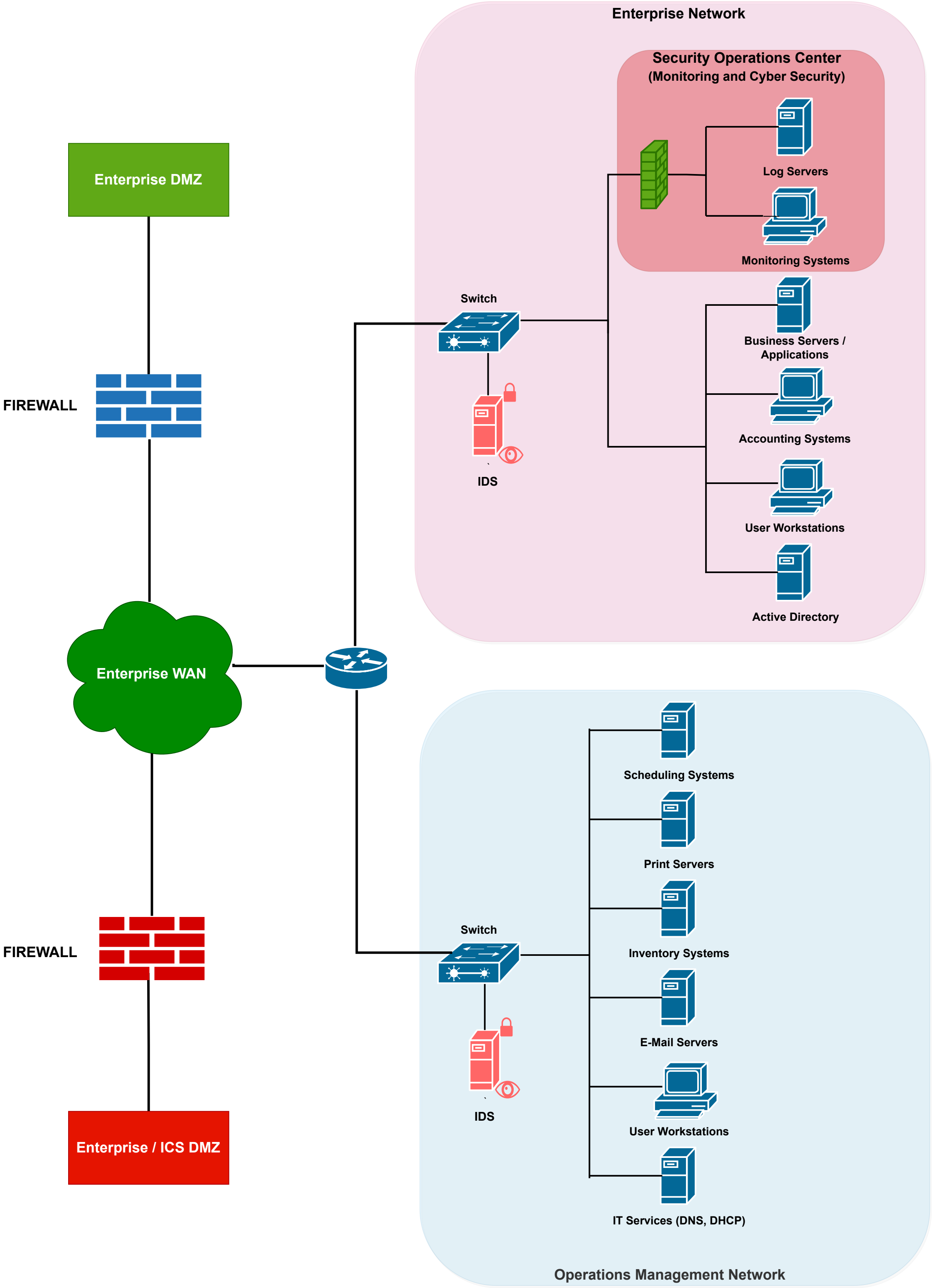


Figure 2-4. The Enterprise Zone

- Boundary Firewalls: Firewalls are recommended as enforcement boundaries or gateways between the DMZ and the connected networks. This ensures that communication flowing in and out of the DMZ is filtered. A good practice to improve security could be to use firewalls from different manufacturers. Since firewalls from different vendors would have different security technologies and vulnerabilities, an attacker would need to exploit vulnerabilities common to both firewalls in order to get past them without being detected, and this would make the system more resistant to attacks.

- It is also recommended to separate the DMZ into different sub-DMZs. This ensures added protection for systems in the DMZ. An example could be to have a separate DMZ for remote access, and a separate DMZ for master servers and historians [28].
- The DMZs could also be implemented as separate unidirectional networks. One could be for ICS-to-enterprise connections and another could be for enterprise-to-ICS connections. This ensures that an attacker who gains access to the control network through the DMZ is unable to retrieve information from the control network through that same connection since it is unidirectional. Unidirectional connections could also be used for process monitoring, information logging, and reporting. An example could be in cases where the enterprise network needs process information from the control network - a read-only historian server could be placed in the DMZ, which periodically pulls information from the control network for the enterprise network's usage, without allowing communication in the opposite direction.
- The DMZ could also be implemented using disjoint protocols. An example is using Modbus/TCP on the controller side of the DMZ and HTTPS on the enterprise for specific communication. With this setup in place, an attacker would have to use two different exploits for the two different protocols in order to be successful, and this would be more challenging than if both communications used the same protocol. This would also act as an extra layer of security [28].
- Jump-hosts could be placed in the DMZ to provide remote access to vendors or employees and unused connections should always be terminated [28, 43, 47].

2.3.4. The Control Zones - Levels 0-3

In each microgrid control zone shown in 2-6, there is a plant-wide microgrid control network (Level 3), the area supervisory networks (Level 2), the local control networks (Level 1), and the process network (Level 0). The control zone is very important to the smooth functioning of the microgrid because it features all the devices, systems, and applications used in monitoring and controlling the microgrid operations. It is therefore critical to ensure that this zone is logically separated from the enterprise network and protected from possible attacks. Proper segmentation and segregation should also be employed within the control zone, in order to protect the systems and devices in this zone.

The microgrid control network (Level 3) performs management operations of the control system. Systems at this level may communicate and share data with systems at the enterprise through a DMZ, and also communicate with systems in lower levels for monitoring and control purposes [47]. Some of the systems and applications found at this level include:

- Monitoring and reporting systems

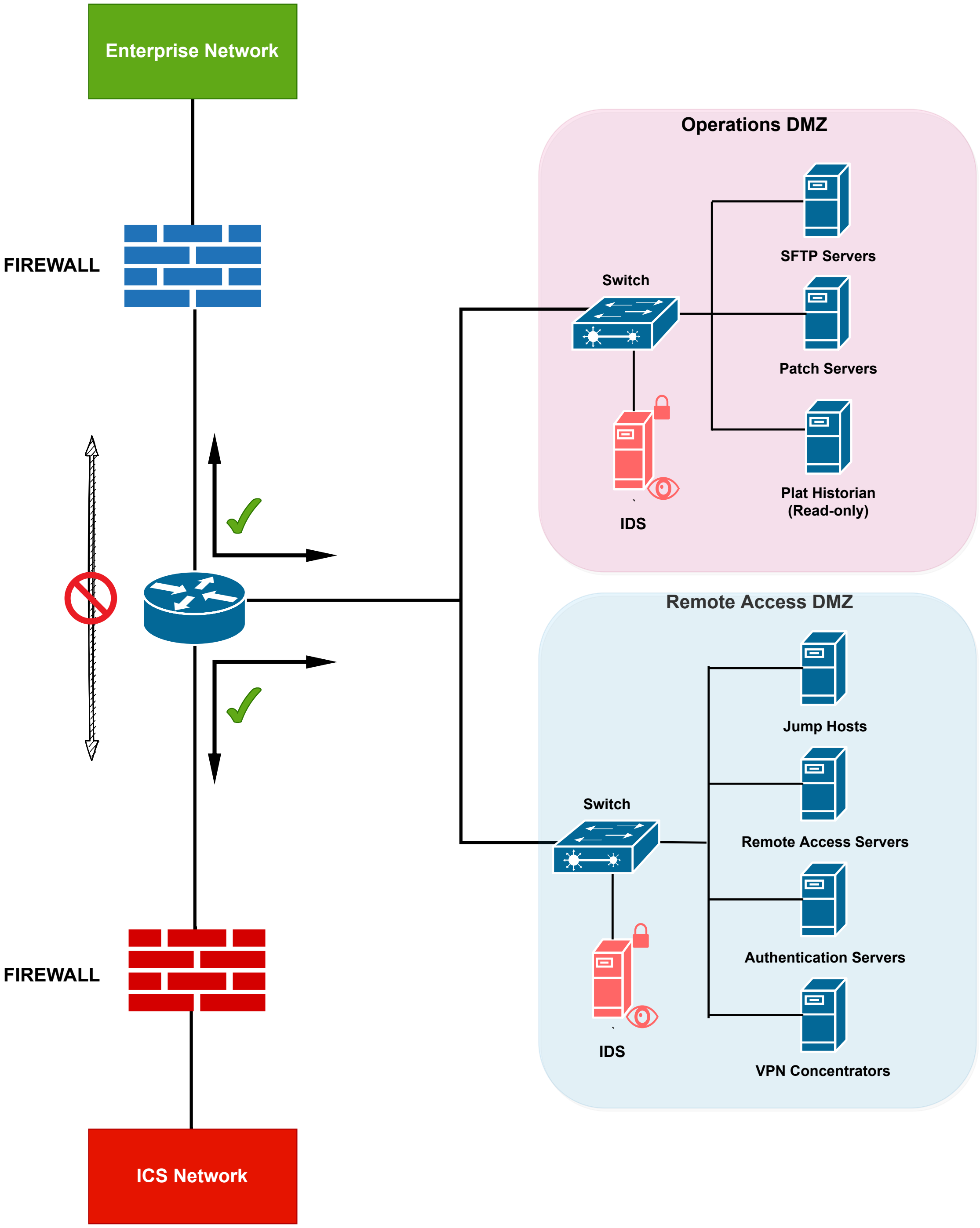


Figure 2-5. The Enterprise/ICS DMZ

- Testing and staging area
- Patch servers
- Plant historian
- Production scheduling systems

- Jump hosts and remote access support
- Network file servers
- Engineering workstations
- IT services such as Active Directory, DHCP, DNS, etc.

The area supervisory network (Level 2) includes systems and applications responsible for controlling and supervising a cell/area. Some of the systems found at this level include:

- Human Machine Interfaces (HMI)
- Control room workstations
- Alarms/Alert systems

Systems at this level may interface with systems in levels 1 and 0 for control and monitoring operations, as well as systems above (levels 3, 4, 5) for reporting operations [47].

The Local control network (level 1) is made up of controller systems and devices that interface with the sensors, actuators, analyzers and other field devices in level 0. The devices typically found at this level include Programmable Logic Controllers (PLC), Distributed Control Systems (DCS), and Remote Terminal Units (RTU), with some of them running vendor-specific operating systems. It is common for the devices found at this level to coordinate with each other and exchange information in order to facilitate their operations, while also communicating with HMIs and control systems at higher levels (2 and 3) [47].

The Process network (Level 0) includes systems such as actuators, sensors, Industrial Internet-of-Things (IIoT) devices, Intelligent Electronic Devices (IEDs), and field devices, which are used to directly control physical processes. These devices receive control instructions and update their status information to the level 1 control devices, and are responsible for operations such as sensing, measurement, speed control, etc. [47].

Systems in the control zone communicate using different protocols, such as the Modicon Communication Bus (Modbus), Distributed Network Protocol 3 (DNP3), Open Process Communications (OPC), Inter-Control Center Protocol (ICCP), etc., possessing different network requirements and specific vulnerabilities which must be considered while implementing security. Security at the control zone should be implemented with a strong consideration for availability and latency requirements. It is desired that the systems stay up and running with no interruptions to processes or introduction of too much latency as a result of security. It is therefore essential that security implementation is as simple and non-intrusive as possible, bearing in mind that availability is prioritized in ICS networks over integrity and confidentiality.

Network design considerations:

- Boundary Firewalls: Firewalls are recommended as enforcement boundaries or gateways between the control center and the lower levels. This helps to have control over the communications across the control zone levels.

- Logical Hierarchical Separation: The control zone is logically separated into different functional and hierarchical levels using firewalls, VLANS, software-defined networks, etc. This helps to ensure control over the communications across the systems and devices in the control zone.
- It is advised that logging, monitoring, and alert systems are separated and protected using firewalls and IDS to reduce the risk of compromise.
- Intrusion detection systems (Host-based and Network-based) are used as an extra layer of detection and defense.

2.3.5. The Safety Zone

The safety zone consists of systems designed to ensure health, safety, and environmental (HSE) protection by alerting operators and placing control systems in a 'safe state' in the event of a system malfunction, component failure, or a potentially hazardous mode of operation. While safety systems cannot prevent cyber-attacks from occurring, they help prevent unsafe conditions during attacks by bringing control systems to a safe state. They are designed to be highly reliable during safety events, with redundancy and self-diagnostics capabilities employed where necessary. Safety systems are either interfaced with the local and process control systems (levels 1 and 0) on the same network or logically isolated (air-gapped) using data diodes and unidirectional gateways. In cases where they coexist with control systems on the same network, extra care should be taken to ensure that an attacker who compromises the control systems is unable to compromise the safety systems–such as in the Triton/Trisis attacks [48]. A successfully coordinated attack on control systems and safety systems could make the safety systems unable to provide fail-safe shutdowns to the control systems, which could be very disastrous. Compromised safety systems could also be tricked to shutdown systems despite the absence of attacks, thereby disrupting operations of the control system [47, 43, 49]

Special considerations:

- Principle of Least Privilege should be used to minimize the potential attack surfaces of the safety systems.
- Air gaps, data diodes, and unidirectional gateways should be used to ensure that the safety systems are isolated from the control systems. This helps protect them in the event of cyber attacks on the control systems.

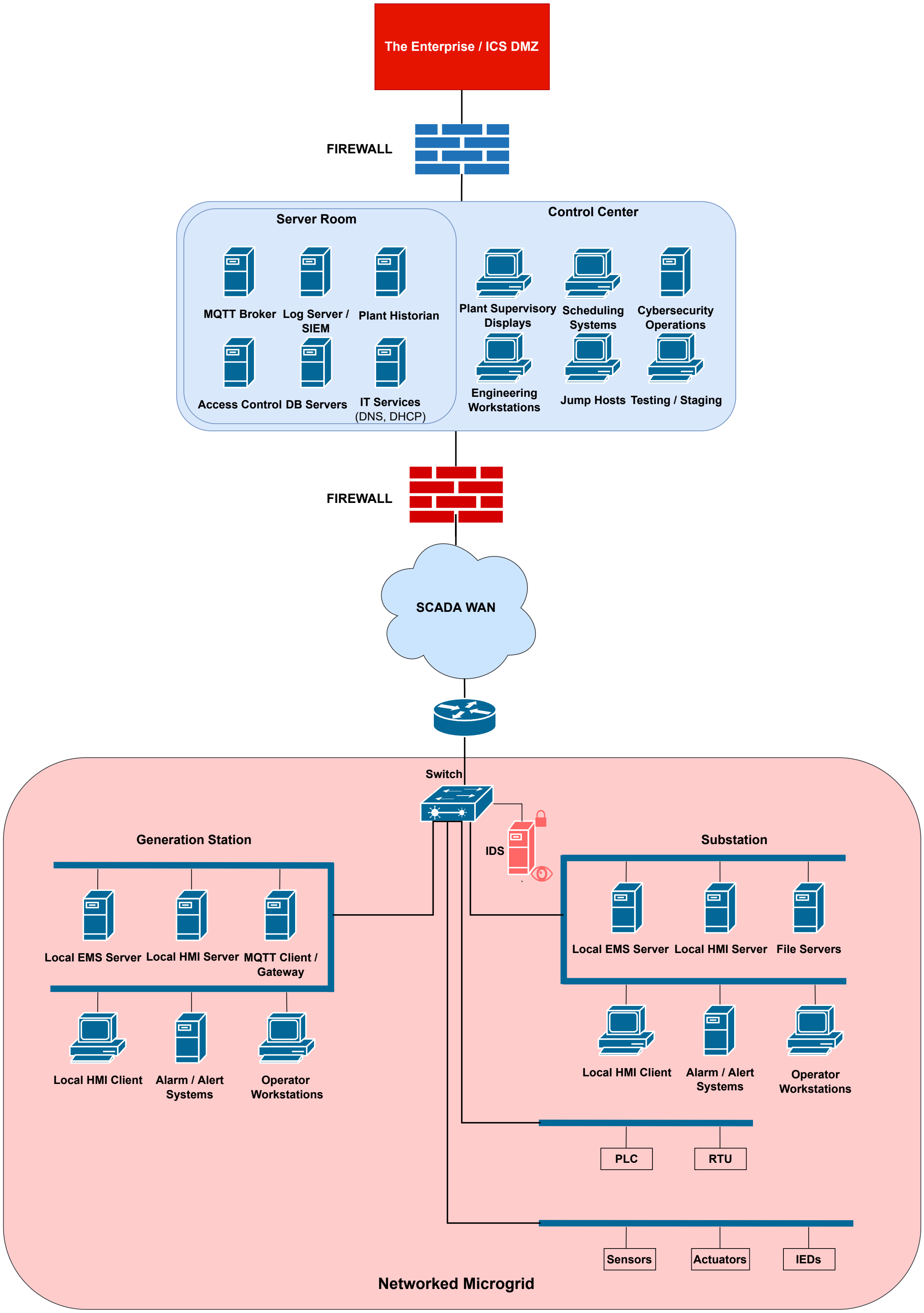


Figure 2-6. The Control Zone

3. NETWORK SEGMENTATION TECHNOLOGIES AND BEST PRACTICES

In this chapter, we highlight some cyber-hardening technologies for networked-microgrid control system environments which segment the network into different subnets. Segmentation divides networks into smaller units and security domains, making it easier to manage networks and enforce security controls. Some common means of establishing segmentation and segregation include:

- **Physical Segmentation:** Networks are completely isolated (air-gapped) with no physical interconnection between them. This could involve the use of separate network devices to establish different networks, ensuring complete isolation of each individual network.

- **Logical segmentation:** Networks are separated through the use of logical network functions e.g. VLANs, unidirectional gateways, firewalls, etc. Logical segmentation can be implemented at any layer of the Open Systems Interconnection (OSI) model.

  - Physical Layer (OSI Layer 1): This involves the separation of networks at the physical layer of the network (different from physical segmentation), using data diodes, unidirectional gateways, etc.

  - Data link Layer (OSI Layer 2): Segmentation at this layer occurs through the use of Virtual Local Area Networks (VLANs). Networks are separated using Layer 2 switches, and their broadcast domains are restricted through the use of VLANs.

  - Network Layer (OSI Layer 3): Segmentation at this layer is performed using routers, layer 3 switches, or firewalls on systems that utilize the Internet Protocol (IP) directly or through encapsulation. Routing also provides security through the use of Access Control Lists (ACLs). Firewalls can also help provide segmentation through state-based filtering, restricting communication between systems based on their current session and state of operation (State-based filtering also involves information at layer 4).

  - Transport, Session, Presentation, and Application Layers (OSI Layers 4-7): Segmentation can exist above the network layer using application payload information, rather than just IP information. This can be implemented through content filtering or deep packet inspection on application-level firewalls e.g., Next Generation Firewalls (NGFW), proxies, content filters etc. Port and protocol level filtering can also be used to restrict the type and number of services that systems use to communicate with each other, thereby ensuring more flexibility and control in defining how information is passed across the network [49, 28].

3.1. Firewalls

Firewalls are able to operate at various layers of the OSI model, using different kinds of rule sets to prevent unauthorized access to systems and networks operating within the industrial control environment. There are three main groups of firewalls:

- Packet Filtering Firewalls: These firewalls, otherwise called stateless firewalls, operate at Layer 3. They possess access control functionality, and filter packets based on basic information such as IP address and protocols. They are faster than more advanced firewalls but can be bypassed by attackers due to their stateless mode of operation [50].
- Stateful Inspection Firewalls: These firewalls keep track of active sessions and filter packets based on their session information. They also check the transport layer content of packets. They are more expensive to implement than packet-filtering firewalls.
- Application-level Firewalls: These firewalls perform deep packet inspection up to the application layer and filter packets based on their application layer information (such as application type or protocols). While they provide an extra level of security, they could introduce delay to the ICS environment.

3.2. Unidirectional Gateways and Data Diodes

Unidirectional gateways are hardware devices or software technologies that allow connections in only one direction (either incoming or outgoing), whereas, a Data diode is a hardware device that allows a one-way transfer of information between segmented networks. They help maintain a closed unidirectional connection by establishing a physical and electrical separation of networks, making it difficult for attackers to establish malicious communications with devices on the other end of the diode since most attacks require two-way communications [51]. One disadvantage of data diodes is the lack of feedback for packets sent. There is no way to tell that a packet was successfully received on the other end since connections only travel in one direction. Data diodes are also expensive to implement, and they require special personnel [52].

3.3. Virtual Local Area Networking

A Virtual Local Area Network (VLAN) is a switched logical network domain with a restricted or controlled broadcast area. With VLANs, systems and devices can be grouped based on their functionalities or other characteristics, and communications such as broadcasts can be restricted to each group, thereby adding a layer of security to the network system. VLANs can be implemented using a single switch, and they can also span multiple switches for larger networks. VLANs provide segmentation by isolating systems and devices based on their functionalities or other characteristics. Broadcast and multicast communications are confined within each group, adding a layer of security to the network [47]. Separate VLANs can be inter-connected (inter-Cell/Area communication) using routers or switches with Layer 3 capabilities or by connecting to access ports. Some common

VLAN vulnerabilities include VLAN hopping, flood attacks, spanning tree protocol attacks, ARP poisoning, etc. VLAN hopping can be mitigated by putting restrictions on the number of allowed VLANs on the trunk or by disabling VLAN trunking on the switch [49].

3.4. Software Defined Networks

Software Defined Networks (SDN) allow a network controller to set up and reconfigure the network based on the needs of the organization. This allows the network team to dynamically make changes to a software-defined perimeter (SDP) or internal routing. In the OT environment, an SDN is a programmable provisioning architecture affording the automation engineer to engineer their Ethernet network as they do the rest of the control systems. SDN control abstracts the control plane from the data plane of an Ethernet network for the traffic engineering of the circuits to prescribe only what is allowed communication and to failover with control system performance needs of less than 100 µsec. In a proactive flow installation mode, network flows can be installed on each of the SDN switches to allow only the specified traffic to traverse the network, while all other traffic is denied. Alternatively, a reactive flow installation mode is possible where flow rules are installed dynamically as traffic is observed, similar to a traditional network switch. There are benefits and drawbacks to both approaches, but in general, SDN provides the ability for network administrators to program the flow rules that control routing decisions for each packet without having to modify existing routing protocols already deployed.

3.5. Remote Access to Microgrids

Remote access has become an essential solution for most industrial facilities due to a limited number of skilled and experienced personnel physically on-site, or with quick access to the site. Remote access exposes control systems and applications to new attack vectors and increases the possibility of an attacker intercepting ICS network data. However, if done correctly, it provides greater security by enabling quick troubleshooting, diagnostics, forensics, and corrective actions.

In fact, there is a significant movement within the security industry to move away from perimeter security and adopt more *zero trust* principles [24]. With zero trust architecture (ZTA), there is no implicit trust, and instead, all subjects must authenticate and authorize actions regardless of location. The NM/IM security team would continuously analyze the risks to assets and operational functions, and respond to protect the system when appropriate. In this case, access to resources is tightly controlled and only permitted when a subject authenticates and authorizes–which happens continually while performing work on the microgrid resources. In the NIST ZTA guidance, there are a couple of approaches that may be applicable to NMs/IMs. As shown conceptually in Fig. 3-1, the subject (e.g., power engineer) authenticates (proves their identity) and is authorized (permitted to perform actions on the resources), based on the Policy Enforcement Point (PEP) rules established by the Policy Decision Point (PDP).

There are techniques to securely enable remote access to sites that do not rely on external systems. Some options include:

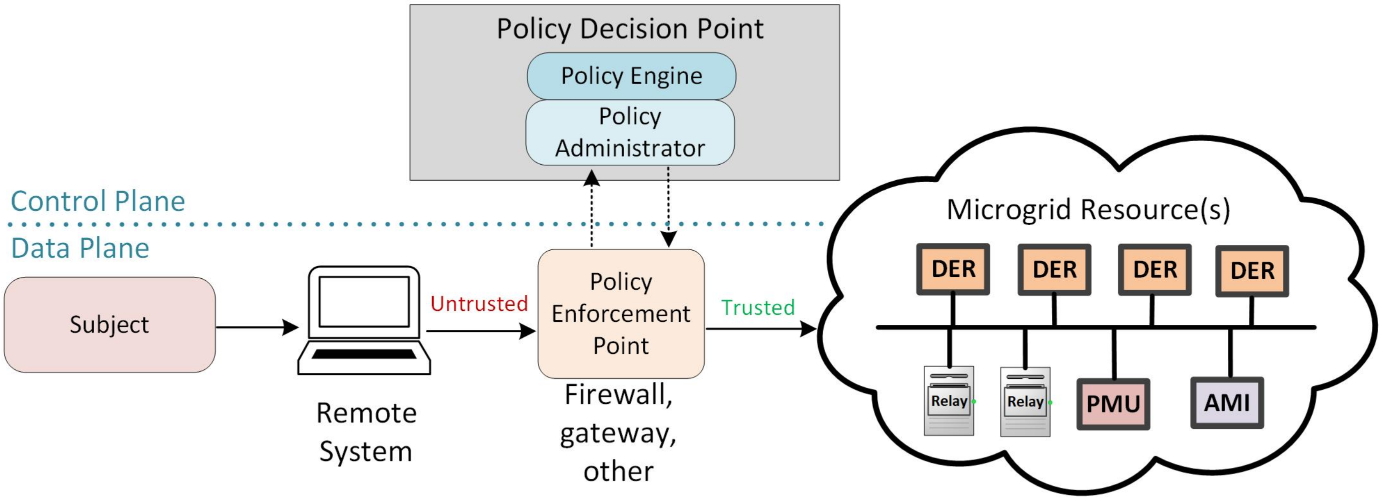


Figure 3-1. Zero Trust Architecture components with control and data planes.

1. Deploy an enterprise-managed Public Key Infrastructure (PKI) responsible for issuing and revoking certificates for devices and end users/subjects. Intermediate certificates are issued from the same enterprise root certificate authority. This would enable mutual TLS to authenticate the subject and resources.

2. Remote personnel first authenticate to an enterprise VPN server using dedicated remote access accounts and multi-factor authentication (MFA). Once on the VPN, the subject then authenticates to an OT DMZ jump host–e.g., using SSH keys–before using OT applications to authorize particular actions on the microgrid equipment. This approach would also work for microgrids connected to the internet or untrusted networks if access to the OT DMZ used whitelisted the public IP of the enterprise network.

3. ZTA using micro-segmentation, wherein the subject is granted access to resources using firewalls, device gateways, or host-based software that acts as the PEP [53].

Here are some recommendations for implementing remote access:

- Ensure proper authentication, authorization, monitoring, and logging of IT and OT access.

- Access to jump hosts should be role-based, and jump hosts for each role should only be allowed to connect to devices managed by the role. Software and applications needed to perform remote functions should be pre-installed on each jump host, and remote users should never be allowed to run software or transfer data from their remote devices [54].

- Use DMZs. No direct traffic should be allowed into the control zone. All remote connections should terminate at the DMZ, from where they are given limited access to the control environment. Patch servers should also be installed in the DMZ in order to enable the initial download of patches before they are deployed on systems in the control zone.

- Control network protocols should be contained in the control zone and not used outside the network, due to their vulnerabilities and limited security capabilities.

- Establish strict remote access rules and controls. Ensure that proper access control is utilized and least-privilege principles are used for remote personnel.

- Use of common protocols on either side of the DMZ is discouraged. It is a good security practice to ensure that different protocols are used on separate sides of a connection. This reduces the attack surface because an attacker would need to exploit vulnerabilities common to both protocols in order to be successful. It helps protect against worms. Security devices (e.g., firewalls) from different manufacturers should also be used on separate sides of connections.

- If possible, separate unidirectional connections should be established for remote access - one for download and another for upload. This would make it more difficult for attackers to gain access to the control network since most attacks require two-way traffic.

- The use of TeamViewer or other cloud-hosted remote access systems is discouraged because it introduces insider threat risks from these other organizations, and in the event of 3rd-party or internet outages, there is no way to access the site.

- Access control systems should be used to ensure that only authorized personnel have access to controlled systems and facilities.

- Access control systems should be designed to be reliable, but not interfere with routine tasks or emergency duties of plant personnel [28].

- Context-based access control policies should be employed. Such contexts include user roles (role-based), device type, time of access, location of user or device, etc. This gives the admin more flexibility and granularity of access control [55].

3.6. Segmentation Best Practices

Some segmentation practices:

- Implement segmentation based on functions and security requirements (e.g. grouping systems based on common vulnerabilities and risks).

- Use least-privilege network access principles, to ensure that just the needed access is given to each system or network that needs to communicate with another network [49].

- Firewall guidance:

  - Use whitelists instead of blacklists.

  - Keep a record of connections and information flowing through the firewall for traffic monitoring and analysis.

  - Ensure secure authentication of all requesting connections before access is granted.

  - Block connections except authorized connections using rules such as source and destination IP addresses or protocols, connection session or state information, etc. [28]

- Unidirectional gateways or data diodes may be used to limit physical network traffic, but many TLS or TCP connections require bi-directional traffic to acknowledge the receipt of data. In certain situations, "bi-directional" data diodes that consist of a pair of individual diodes can be used to solve this issue, but they are more prone to compromise.
- When using VLANs, carefully configure the switches to prevent *switch spoofing* and *double tagging* VLAN hopping attacks [56].

4. OPERATIONAL CYBER-HARDENING TECHNOLOGIES AND BEST PRACTICES

Security monitoring, data collection, and analysis are some of the major challenges of ICS environments. These capabilities should be designed into the system architecture from the beginning to provide the greatest situational awareness without expensive retrofits. The issue is that, generally, not a lot of attention is placed on developing monitoring and data collection technologies for ICS. Focus is largely placed on IT systems instead. Some of these challenges are due to (a) the distributed nature of ICS facilities, which makes data aggregation difficult, (b) the use of legacy systems and poorly documented protocols, (c) the use of proprietary logging technologies instead of standardized ones, and (d) high availability and integrity requirements. The following technologies and concepts provide situational awareness, detection, and response capabilities for OT cybersecurity practitioners.

Layered detection and response security technologies make up part of a comprehensive, defense-in-depth security approach to detecting and recovering from attacks. Over the last few years, power system operators have been improving Security Operation Centers (SOCs) for their OT systems. A SOC is made up of people, processes, and technology that monitor network and endpoint systems for anomalies in order to detect and respond quickly to security incidents. SOCs are often physical locations where security professionals monitor operational activities using data from several tools including:

- Security Information and Event Management (SIEM) software that ingests data from different security monitoring and detection tools, and provides the cybersecurity team with a single interface with detailed information,
- Network-based Intrusion Detection Systems (NIDSs), which use network data to alert on adversary actions,
- Network-based Intrusion Prevention Systems (NIPSs) that block malicious traffic before reaching its target,
- Host-based Intrusion Detection Systems (HIDSs), which track actions on endpoints (e.g., user logins, account creation/modification, binary execution, etc.),
- Host-based Intrusion Prevention Systems (HIPSs), which are a form of Endpoint Detection and Response (EDR) that monitor for system changes and take actions to stop suspicious activity, and
- Security Orchestration, Automation, and Response (SOAR) technologies that use automated response playbooks fed with one or more data streams to defend the network and assets based on pre-programmed rules. (Note: SOAR should not be mistaken for an Extended Detection

and Response (XDR) technology which is similar, but represents a lighter-weight platform, requiring no coding or playbook generation.)

As shown in Fig. 4-1, the SIEM and SOAR are deployed in the SOC, whereas the IDS/IPS tools are deployed on all networks and hosts/endpoints that support them. Aggregating log data in a SIEM platform is a recommended practice, as it would enable a detailed and more efficient log data analysis.

Data from the IT environment may be pertinent to OT SOC analysis, because any adversary actions on the IT side may indicate their tactics, techniques, or procedures (TTPs) for gaining access to the OT network. However, in a case where an integrated IT-OT SOC is to be implemented, efforts should be made to ensure that the data collection process from both environments (IT and OT) are separated, in order not to introduce IT vulnerabilities to the OT environment [57]. IT and OT systems have unique data sources, operations and cyber threats, hence they require unique security solutions. In an OT SOC, there are several data sources that may not exist in traditional IT environments, such as OT alarms, controller events, operational data from DERs, PMUs, PLCs, RTUs, etc. It is therefore critical to provide specialized OT incident monitoring and analysis, in order to efficiently investigate and respond to security incidents. Not all equipment will have the ability to support HIDS/HIPS technologies, as shown in Fig. 4-1.

4.1. Security Information and Event Management (SIEM)

Centralized situational awareness of OT systems is critical for debugging, threat hunting, and forensics. Security Information and Event Management (SIEM) is a combination of Security Event Monitoring (SEM) and Security Information Management (SIM) systems. SEM systems are responsible for real-time monitoring and event correlation, while SIM systems are concerned with the storage, analysis and presentation of collected security data. SIEM systems are essential to ICS environments because they help provide cybersecurity functions such as real-time monitoring, time-based event network and host/endpoint logging, data aggregation from multiple sources, centralized information processing and analysis, event correlation, security alerting and reporting, information presentation and management, data storage, etc. [58, 59]. SIEM systems should be implemented with consideration for different ICS zone requirements, however. Common logging protocols are suitable for high levels of the ICS environment (e.g., level 3), but passive network monitoring should be used for systems running in lower levels (levels 0, 1 and 2) in order not to disrupt their operations [60, 61].

4.2. Security Monitoring and Logging Tools

Security monitoring and logging involve the collection of security event logs in order to provide visibility of activities occurring in various systems and facilities, and enable effective investigation and incident response. It is a traditional IT security practice which is applicable to OT environments as well. Security logging in OT is different from that of IT environments due to their differences in uptime, operation, and safety requirements. Logging can also be quite challenging

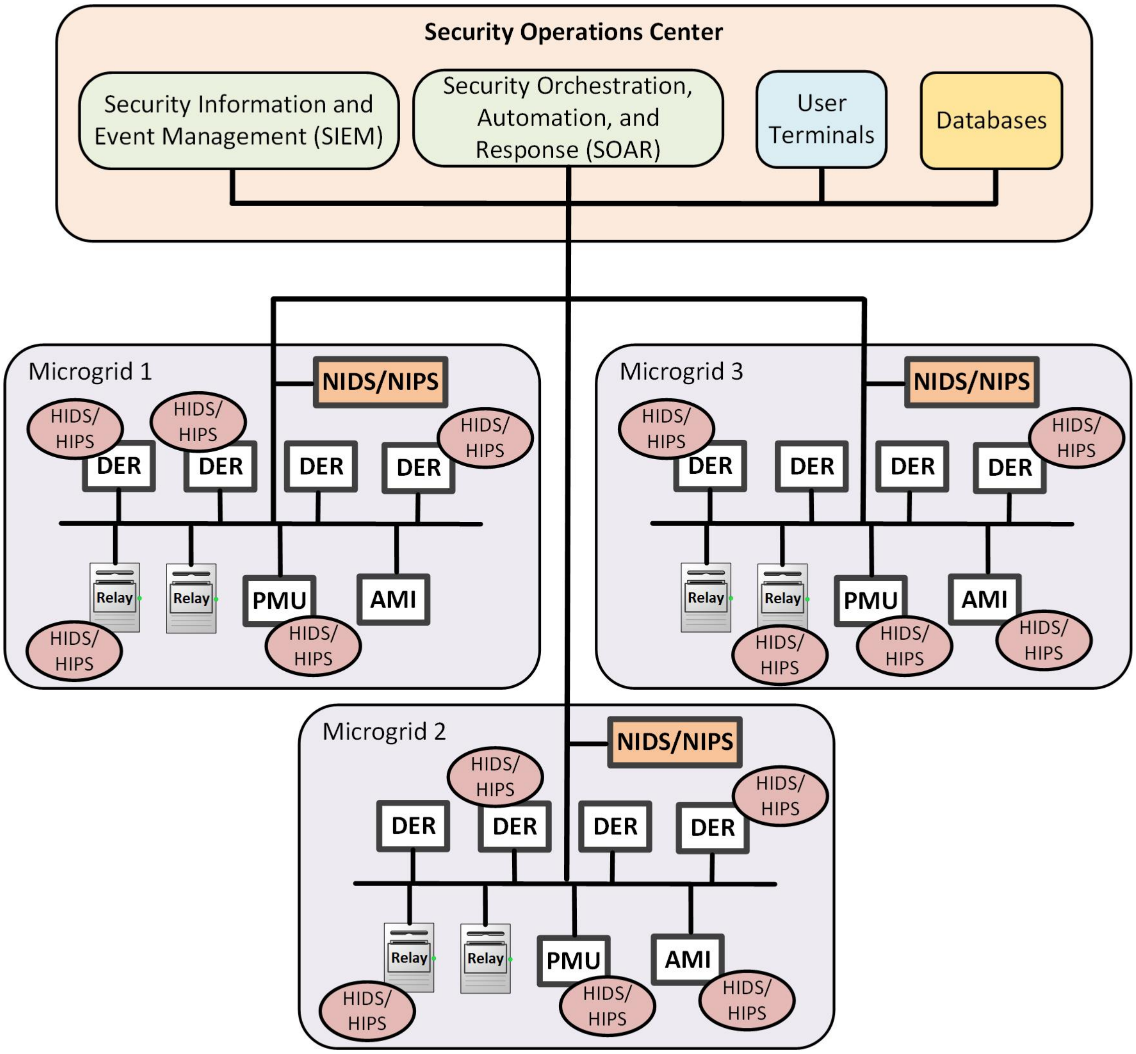

Security Operations Center
Security Information and Event Management (SIEM)
Security Orchestration, Automation, and Response (SOAR)
User Terminals
Databases
Microgrid 1
NIDS/NIPS
HIDS/HIPS
DER
Relay
PMU
AMI
Microgrid 3
Microgrid 2

Figure 4-1. Locations of cyber-hardening technologies in the networked microgrids.

in OT environments as a result of different vendor restrictions and requirements, which makes it difficult to establish a standardized logging architecture across the entire environment [62].

While logging is an essential security practice, it is important that log sources are carefully selected and configured. Collecting logs from every log source available on the network could be expensive in terms of storage. It could also lead to a risk of critical security incidents being overlooked, due to the high volume of false positives and false negatives arising from large log data [63]. Categorizing log sources by functions makes it easier to manage logs. Such sources could include endpoints (servers, computers, PLCs, IEDs, RTUs, etc.), network devices (switches, routers, firewalls, etc.), applications, etc.

Two primary sets of host-based logs are Syslog for UNIX-like environments and Windows Event Forwarding (WEF) for Windows computers.

4.2.1. Syslog

Syslog is a logging protocol used to send event logging information to a log server. It runs natively on UNIX and UNIX-like environments, and can be supported on Microsoft Windows through various open-source and commercial libraries. Syslog features three main layers - Content, which is the information contained within a Syslog message; Application, which is responsible for generating, interpreting, routing, and storing event messages; and Transport, which is responsible for transmitting the message over the network. Syslog operates over a network using a client-server architecture [64]. On the server side, Syslog uses a Listener to gather log messages sent over the network, a database to store Syslog data and management software that helps process, filter, and manage log data. It is commonly used in network devices such as routers, switches, firewalls, etc., and ICS devices such as Programmable Logic Controllers (PLC), Intelligent Electronic Devices (IED), Remote Terminal Units (RTU), etc., provided that they support Syslog functionality [62].

Some drawbacks include data being stored in clear text, making it possible for an intruder to read or modify Syslog data, and Syslog not providing mechanisms for authenticating received log data, making it possible for data to be intercepted or sent from an illegitimate source with no way to verify. Data integrity is also a concern with Syslog since it relies on UDP transport which provides no way to verify if messages are successfully received or not.

The confidentiality problem in Syslog could be solved by encrypting log data during transit. This could be done using Secure Shell (SSH) port forwarding or encrypting the data using a Secure Sockets Layer (SSL) or IP Security (IPSec) protocol. In cases where Syslog data has to be transferred over insecure networks, a Virtual Private Network (VPN) could be created between source and destination to encrypt the log data during transmission [65]. The data integrity problem could be solved by using Nsyslog, Syslog-ng, or Secure Syslog. These are newer versions of Syslog that use TCP as a transport protocol instead of UDP. Lastly, the authentication drawback could be mitigated by using Secure Syslog, which hosts certificates that help provide authentication during data transfer. Secure Shell (SSH) forwarding could also provide authentication services for Syslog data [66].

4.2.2. Windows Event Forwarding (WEF)

Windows Event Forwarding is a feature of Windows Remote Management (WinRM) which helps to transfer logs from ICS environments to a Security Information and Event Management (SIEM) system. It can be deployed using a pull or push configuration. In the pull configuration a Windows Event Collector (WEC) server pulls event logs from clients, while in the push configuration, clients push their event logs to the WEC server. The push configuration, however, is the recommended configuration, according to Microsoft. Windows Event Forwarding facilitates log aggregation from multiple WEC servers in large networks, or across multiple windows domains, making log collection in ICS environments easier. Windows Remote Management (WinRM) communicates using HTTP or HTTPS over TCP and uses Kerberos authentication to encrypt communication by default. WEF provides flexibility in log collection by using a subscription technology, making it possible to configure which WEC servers clients push their log to, and enabling hierarchical log aggregation and management. While configuring WEF subscription, it is recommended that the communication is optimized for latency, in order to ensure that logs are forwarded quickly enough, but with a minimal strain on network resources [62].

4.3. Intrusion Detection and Prevention Systems (IDS/IPS)

Intrusion detection systems monitor networks and systems in order to identify successful and unsuccessful attempts to gain unauthorized access to the system. Unusual activity such as unusual traffic patterns, unauthorized file access, changes to system configurations, suspicious network scanning, etc., are constantly looked out for, and alerts are made when such events are detected on the network. Intrusion detection systems should be tuned for the environment in which they are deployed, in order to make them more efficient and reduce false positive alerts. Special attention must be paid to ICS-specific protocols when deploying ICS in OT environments [28, 67].

Network-based Intrusion Detection Systems (NIDS) passively monitor and analyze network traffic in order to detect and report possible intrusions, while Intrusion Prevention Systems (IPS) actively monitor and analyze network traffic, with the ability to deny suspicious network traffic based on some defined network traffic filtering rules and mechanisms. NIDS should be strategically installed within a network in order to monitor inbound and outbound traffic, as well as communications between systems within the zone where it is installed [43].

Host-based IDS are endpoint software that monitor system characteristics such as CPU usage, log file entries, configuration changes, file accesses, etc., and create alerts when unusual activities are detected on the system. Both host-based and network-based IDS should be deployed in ICS environments, in order to have more efficient intrusion detection.

IDS systems can also be classified in terms of detection mechanisms as signature-based and behavior/anomaly-based [68]. Signature-based IDSs use specified rules to identify intrusions with well-known intrusion patterns. Behavior-based IDS are trained to recognize normal system behavior and classify deviations from normal behavior as anomalies. Thus, they are able to detect new and unknown intrusion types. Both signature-based and anomaly-based IDS should be deployed in ICS environments for improved detection efficiency.

4.4. Security Orchestration, Automation and Response (SOAR)

Security Orchestration, Automation and Response (SOAR) is a combination of three distinct security solutions - Security Orchestration and Automation (SOA), Security Incident Response Platforms (SIRP) and Threat Intelligence Platforms (TIP). It provides the platform that makes it possible to coordinate and synchronize several security technologies through automation [69, 70]. By using automation and machine learning techniques, SOAR systems are able to learn patterns and automate repetitive tasks, reducing manual processes, in order to provide quick and efficient responses to incidents. They also provide centralized comprehensive reporting of events. One publication [70] lists and describes some existing SOAR vendors, solutions and features.

4.5. Moving Target Defense

We implemented and evaluated IP randomization Moving Target Defense (MTD) techniques within a laboratory environment at Sandia National Laboratories. The laboratory environment is shown in 4-2. The MTD defense we developed focuses on randomizing IP addresses at user-configurable frequencies to evade adversarial discovery. One of the goals of IP randomization is to create uncertainty and increase the difficulty for an adversary to discover and track the systems existing within a computer network. IP randomization is implemented using an SDN-based approach with the flow rules installed at each switch controlling the randomization intervals. The randomization algorithms reside at the network layer, transparent to the end devices themselves, for both usability and scalability purposes. Improved usability comes from the fact that the randomization algorithms are managed at the network level and do not need to be deployed at every end device. The algorithms are built into the SDN fabric, which consists of several SDN-capable switches and a management controller system. The SDN architecture provides a scalable solution where any new end device introduced into the network will automatically have the IP randomization MTD defense activated and enabled, without the end user necessarily having any knowledge that the MTD defense is deployed.

When using an SDN-based approach, routing and switching logic can be customized to control the frequency at which source and destination IP addresses are randomized. The customized logic can also account for the periods of time when a packet is traversing the network and new randomized source and destination IP addresses are installed on each of the switches in the network. The random IP address mappings are programmed by flow rules that are managed by a centralized controller. Each flow rule has a “match” specification and an associated “action” to perform depending on if the match criteria are satisfied. The flow rules for this implementation match a packet based on a combination of the source IP address, the destination IP address, and the incoming physical port of the switch that the packet was received on. If the incoming physical port and source IP address that the packet was received on corresponds to a host that is directly connected to the switch, then the action taken within the flow rule is to rewrite the source and destination IP addresses with a set of newly generated random source and destination IP addresses. Otherwise, if the host is not directly connected to the switch (but rather to an interior switch interface), the packet is forwarded to the next hop switch. The location of the next hop switch is specified within the flow rules that matched the randomized source and destination IP addresses for that particular

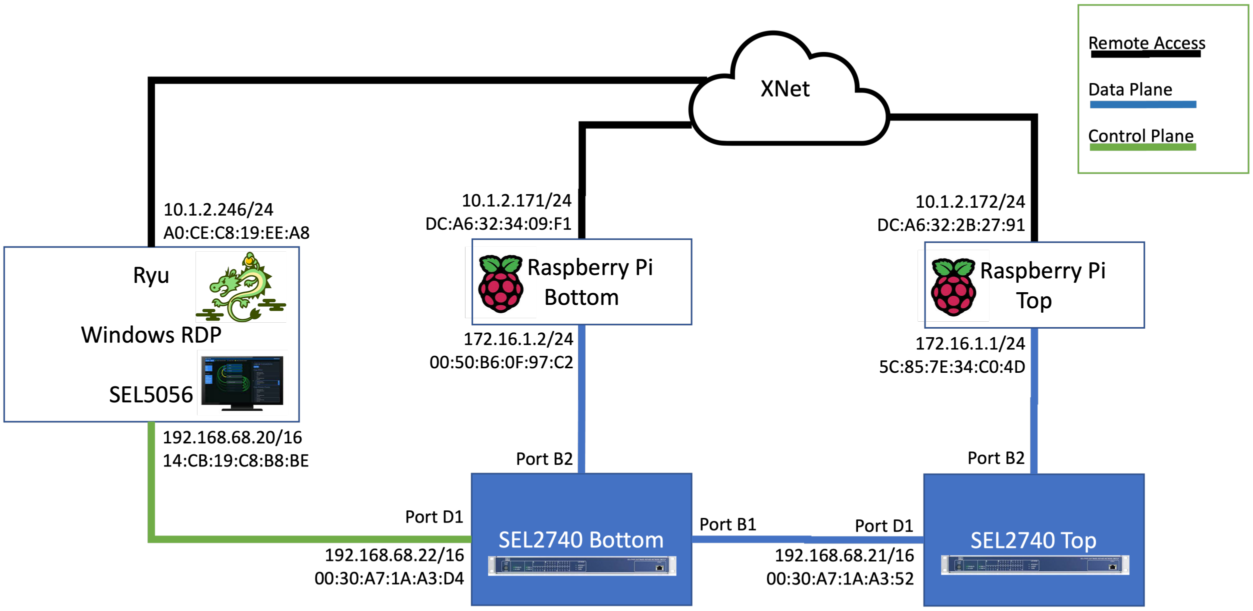
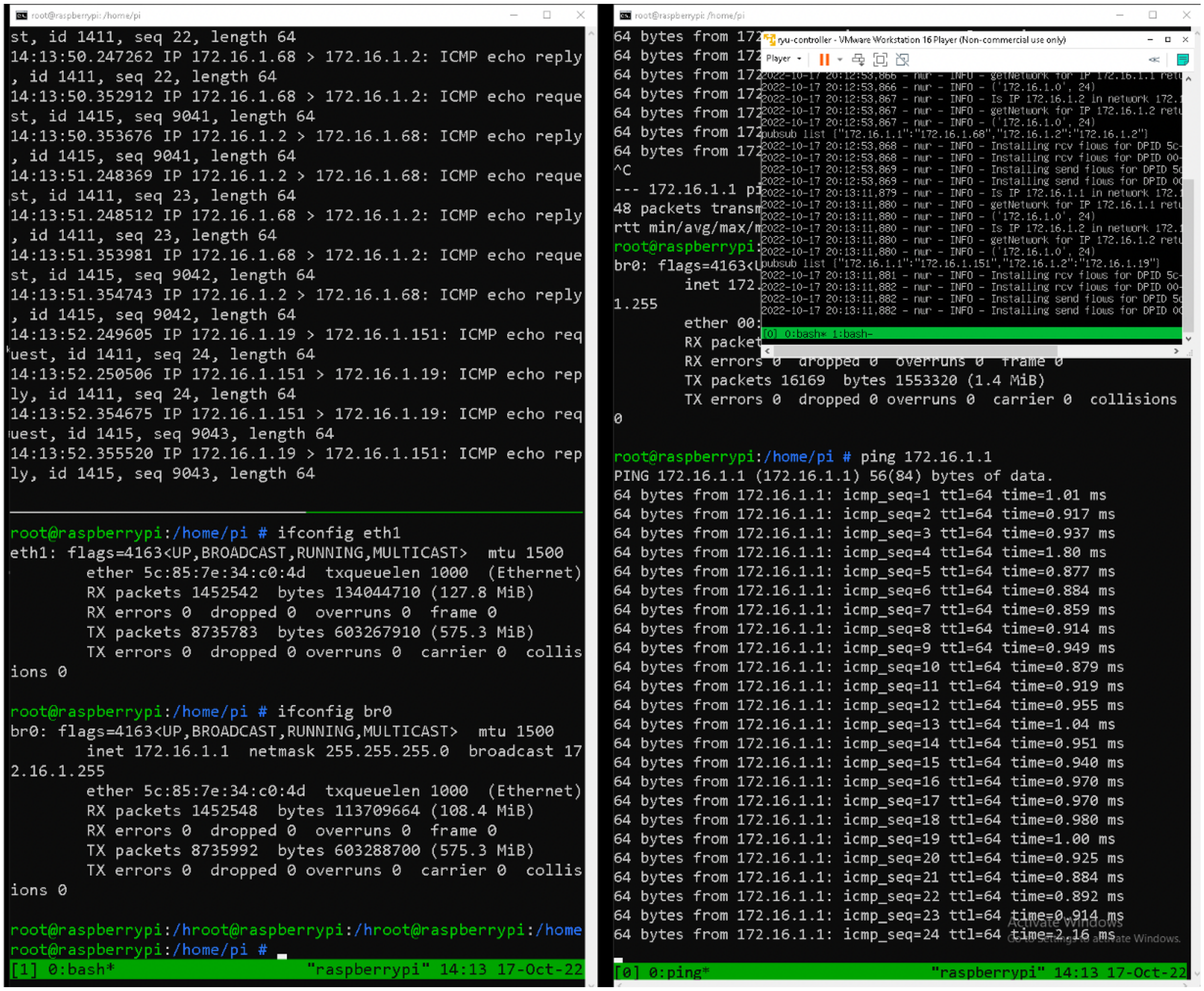


Figure 4-2. The laboratory environment with IP randomization enabled between the two SEL2740 SDN switches.

MTD reconfiguration interval. The random mappings are communicated to the SDN controller via a Python wrapper script that updates the mappings based on predefined user configurable randomization intervals desired.

Once the packet reaches the edge switch that is directly connected to the destination host, the original source and destination IP addresses are restored within the packet back to the original source and destination IP addresses. The result of this approach is that an adversary passively observing traffic on an interior non-SDN capable network switch, will no longer automatically learn the true IP addresses of the end hosts simply by observing network traffic passively. In this scenario, the adversary would instead observe a pair of pseudo-random IP addresses traversing the network. The pseudo-random IP addresses that are managed by the controller are continuously changing at user-configurable time intervals and the random mappings are generated using a pseudo-random number generator. For this implementation, the host bits of the 32-bit IP address are randomized although all 32-bits can be randomized since our laboratory environment consisted of a flat network that contains only layer 2 switches. If routers are included in the topology, only the host bits of the IP address can be randomized so packets can continue to be routed correctly. This solution would allow layer 3 devices to appropriately route packets without having to modify the underlying routing protocols within those devices. A similar approach could have also randomized MAC addresses or even set all MAC addresses to the same value since the match criteria of the SDN flow rule does not depend on MAC addresses. Manipulation of MAC addresses was not performed in this research but can easily be adapted to do so.

Figure 4-3 shows a screenshot of the MTD actively updating IP addresses between two endpoints communicating through the SEL SDN network switches. SSH sessions between the two endpoints are shown in the terminals on the left and on the right of the screen. The system in the right terminal is pinging the system on the left terminal. The left terminal shows a packet capture of the ICMP ping messages that are being received and sent from the system on the right terminal. As



root@raspberrypi: /home/pi
root@raspberrypi: /home/pi
ryu-controller - VMware Workstation 16 Player (Non-commercial use only)
Player

```
st, id 1411, seq 22, length 64
14:13:50.247262 IP 172.16.1.68 > 172.16.1.2: ICMP echo reply
, id 1411, seq 22, length 64
14:13:50.352912 IP 172.16.1.68 > 172.16.1.2: ICMP echo reque
st, id 1415, seq 9041, length 64
14:13:50.353676 IP 172.16.1.2 > 172.16.1.68: ICMP echo reply
, id 1415, seq 9041, length 64
14:13:51.248369 IP 172.16.1.2 > 172.16.1.68: ICMP echo reque
st, id 1411, seq 23, length 64
14:13:51.248512 IP 172.16.1.68 > 172.16.1.2: ICMP echo reply
, id 1411, seq 23, length 64
14:13:51.353981 IP 172.16.1.68 > 172.16.1.2: ICMP echo reque
st, id 1415, seq 9042, length 64
14:13:51.354743 IP 172.16.1.2 > 172.16.1.68: ICMP echo reply
, id 1415, seq 9042, length 64
14:13:52.249605 IP 172.16.1.19 > 172.16.1.151: ICMP echo req
uest, id 1411, seq 24, length 64
14:13:52.250506 IP 172.16.1.151 > 172.16.1.19: ICMP echo rep
ly, id 1411, seq 24, length 64
14:13:52.354675 IP 172.16.1.151 > 172.16.1.19: ICMP echo req
uest, id 1415, seq 9043, length 64
14:13:52.355520 IP 172.16.1.19 > 172.16.1.151: ICMP echo rep
ly, id 1415, seq 9043, length 64

root@raspberrypi:/home/pi # ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 5c:85:7e:34:c0:4d  txqueuelen 1000  (Ethernet)
        RX packets 1452542  bytes 134044710 (127.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8735783  bytes 603267910 (575.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collis
ions 0

root@raspberrypi:/home/pi # ifconfig br0
br0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.1.1  netmask 255.255.255.0  broadcast 17
2.16.1.255
        ether 5c:85:7e:34:c0:4d  txqueuelen 1000  (Ethernet)
        RX packets 1452548  bytes 113709664 (108.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8735992  bytes 603288700 (575.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collis
ions 0

root@raspberrypi:/hroot@raspberrypi:/hroot@raspberrypi:/home
root@raspberrypi:/home/pi # _
[1] 0:bash*                         "raspberrypi" 14:13 17-Oct-22
```

```
2022-10-17 20:12:53,866 - nur - INFO - getNetwork for IP 172.16.1.1 retu
2022-10-17 20:12:53,866 - nur - INFO - ('172.16.1.0', 24)
2022-10-17 20:12:53,867 - nur - INFO - Is IP 172.16.1.2 in network 172.1
2022-10-17 20:12:53,867 - nur - INFO - getNetwork for IP 172.16.1.2 retu
2022-10-17 20:12:53,867 - nur - INFO - ('172.16.1.0', 24)
pubsub list {"172.16.1.1":"172.16.1.68","172.16.1.2":"172.16.1.2"}
2022-10-17 20:12:53,868 - nur - INFO - Installing rcv flows for DPID 5c-
2022-10-17 20:12:53,868 - nur - INFO - Installing rcv flows for DPID 00-
2022-10-17 20:12:53,869 - nur - INFO - Installing send flows for DPID 5c
2022-10-17 20:12:53,869 - nur - INFO - Installing send flows for DPID 00
2022-10-17 20:13:11,879 - nur - INFO - Is IP 172.16.1.1 in network 172.1
2022-10-17 20:13:11,880 - nur - INFO - getNetwork for IP 172.16.1.1 retu
2022-10-17 20:13:11,880 - nur - INFO - ('172.16.1.0', 24)
2022-10-17 20:13:11,880 - nur - INFO - Is IP 172.16.1.2 in network 172.1
2022-10-17 20:13:11,880 - nur - INFO - getNetwork for IP 172.16.1.2 retu
2022-10-17 20:13:11,880 - nur - INFO - ('172.16.1.0', 24)
pubsub list {"172.16.1.1":"172.16.1.151","172.16.1.2":"172.16.1.19"}
2022-10-17 20:13:11,881 - nur - INFO - Installing rcv flows for DPID 5c-
2022-10-17 20:13:11,882 - nur - INFO - Installing rcv flows for DPID 00-
2022-10-17 20:13:11,882 - nur - INFO - Installing send flows for DPID 5c
2022-10-17 20:13:11,882 - nur - INFO - Installing send flows for DPID 00
[0] 0:bash* 1:bash-
```

```
64 bytes from 172
64 bytes from 172
64 bytes from 172
64 bytes from 172
64 bytes from 172
64 bytes from 172
64 bytes from 172
^C
--- 172.16.1.1 pi
48 packets transm
rtt min/avg/max/m
root@raspberrypi:
br0: flags=4163<U
        inet 172.
1.255
        ether 00:
        RX packet
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16169  bytes 1553320 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

root@raspberrypi:/home/pi # ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=1.01 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=0.917 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=0.937 ms
64 bytes from 172.16.1.1: icmp_seq=4 ttl=64 time=1.80 ms
64 bytes from 172.16.1.1: icmp_seq=5 ttl=64 time=0.877 ms
64 bytes from 172.16.1.1: icmp_seq=6 ttl=64 time=0.884 ms
64 bytes from 172.16.1.1: icmp_seq=7 ttl=64 time=0.859 ms
64 bytes from 172.16.1.1: icmp_seq=8 ttl=64 time=0.914 ms
64 bytes from 172.16.1.1: icmp_seq=9 ttl=64 time=0.949 ms
64 bytes from 172.16.1.1: icmp_seq=10 ttl=64 time=0.879 ms
64 bytes from 172.16.1.1: icmp_seq=11 ttl=64 time=0.919 ms
64 bytes from 172.16.1.1: icmp_seq=12 ttl=64 time=0.955 ms
64 bytes from 172.16.1.1: icmp_seq=13 ttl=64 time=1.04 ms
64 bytes from 172.16.1.1: icmp_seq=14 ttl=64 time=0.951 ms
64 bytes from 172.16.1.1: icmp_seq=15 ttl=64 time=0.940 ms
64 bytes from 172.16.1.1: icmp_seq=16 ttl=64 time=0.970 ms
64 bytes from 172.16.1.1: icmp_seq=17 ttl=64 time=0.970 ms
64 bytes from 172.16.1.1: icmp_seq=18 ttl=64 time=0.980 ms
64 bytes from 172.16.1.1: icmp_seq=19 ttl=64 time=1.00 ms
64 bytes from 172.16.1.1: icmp_seq=20 ttl=64 time=0.925 ms
64 bytes from 172.16.1.1: icmp_seq=21 ttl=64 time=0.884 ms
64 bytes from 172.16.1.1: icmp_seq=22 ttl=64 time=0.892 ms
64 bytes from 172.16.1.1: icmp_seq=23 ttl=64 time=0.914 ms
64 bytes from 172.16.1.1: icmp_seq=24 ttl=64 time=2.16 ms
_
[0] 0:ping*                         "raspberrypi" 14:13 17-Oct-22
```

Figure 4-3. The laboratory environment with IP randomization enabled between the two endpoints. The left terminal and right terminal are the two communicating endpoints. The virtual machine near the top-middle of the image is the SDN controller. The left terminal shows IP addresses randomizing from 172.16.1.2->172.16.1.68 updating to 172.16.1.19->172.16.1.151.

can be seen in the packet capture of the left terminal, the IP addresses are re-randomized from 172.16.1.2 communicating with 172.16.1.68 to the updated IP addresses of 172.16.1.19 communicating with 172.16.1.151. The SDN controller is also shown in the virtual machine window on the top right of the screen capture. The SDN controller is the system responsible for issuing the IP re-randomization flow rules into the SEL SDN switches. As a result, an adversary who had gained reconnaissance information about the system communicating on the network would have an outdated understanding of the systems communicating after re-randomization occurred.

5. NJ TRANSITGRID USE CASE

New Jersey Transit (NJT) started the $570 million NJ TRANSITGRID project in response to 'Superstorm Sandy' [71], which caused $65 billion [72] in damage and disrupted critical passenger-rail and other transportation systems throughout New York and New Jersey. The NJ TRANSITGRID project was designed to power limited passenger-rail, bus, and ferry service within the New York City and New Jersey area during natural or man-made disasters, e.g., a future occurrence of 'Superstorm Sandy'. The NJ TRANSITGRID project features several components: the Microgrid Central Facility (MCF)+rail microgrid and seven microgrid facilities that operate rail substations, bus terminals, and ferry ports.

5.1. The NJT Facilities

There are a total of eight *Interdependent Microgrids* that NJT will operate as part of this project. The first is the Microgrid Central Facility (MCF) coupled to rail loads. The other seven are distributed generation (DG) microgrids. The MCF is anticipated to be completed in 2028, Newark Penn Station in 2027, and the other IM sites (often referred to as Distributed Generation (DG) sites) in 2026.

These microgrids can be classified as IMs because operations of each will affect the loads and generation needs of the other microgrids. During an emergency situation, if the rail station, bus terminals, or ferry ports DG microgrids experience an outage, this will impact rail loads and therefore MCF generation requirements. Similarly, if the rail operations are reduced or cancelled because of MCF+rail microgrid generation limitations, the rail station, bus terminal, and ferry port DG IMs will be impacted as transit patterns are modified. Exchanging power data, fuel levels, alarms, and other status information across all the microgrids will improve situational awareness, transportation efficiency, and emergency operations planning.

5.1.1. The Microgrid Central Facility (MCF) and Rail Loads

The original Microgrid Central Facility (MCF) was designed to include six 20 MW gas generators and 150 kW of PV generation. As the central facility, it is responsible for powering NJT rail lines in the event of a utility outage. The MCF can also be operated in a grid-connected mode to provide power to the regional transmission organization, PJM Interconnection LLC when it is financially advantageous. The selection of power generation technologies is currently under revision to accommodate greater use of renewable energy technologies.

5.1.2. Distributed Generation Stations

Each of the seven DG microgrids will include loads and distributed energy resources which may include generators, energy storage systems, solar, bi-directional electric vehicle chargers, etc.

The NJ TRANSITGRID project features seven DG microgrids, which include the Newark Penn Station, Broad Street Station, Secaucus Station, Wayne Bus Garage, Meadowlands Bus Garage, Greenville Bus Garage, and the Port Imperial Ferry Terminal, as described here:

- **Newark Penn Station** is a rail station located in Newark, NJ. This is a four-story building with more than 217,000 square feet of space for waiting rooms, offices, platforms, etc. This facility hosts a number of rail and bus operators. This facility operates on a 24/7/365 schedule. Going by the number of passengers using a facility, this is the busiest of the stations in the TRANSITGRID project.

- **Broad Street Station** is a rail station also located in Newark, NJ. This is a two-story building with 65,000 square feet of space for offices, retail spaces, and island platforms for passenger waiting and entry. This facility hosts both commuter rail and light rail. The commuter rail operates on a 24/7/365 schedule, while the light rail runs from 5:00 a.m. to midnight daily.

- **Secaucus Station** is a rail station in Secaucus, NJ. This is a three-story building with approximately 321,000 square feet of space for waiting rooms, retail spaces, offices, and utility rooms. This facility hosts both passenger rail and bus operations. The facility operates on a 24/7/365 schedule.

- **Wayne Bus Garage** is a bus maintenance facility located in Wayne, NJ. This is a single-story building with approximately 197,000 square feet of space for offices, maintenance/refuelling/storage spaces, and utility rooms. This facility operates on a 24/7/365 schedule. Approximately 100 full-time staff and 300 drivers are employed at this facility.

- **Meadowlands Bus Garage** is a bus maintenance facility in Secaucus, NJ. This is a single-story building with over 266,000 square feet of space for offices, maintenance/refuelling/storage spaces, and utility rooms. This facility operates on a 24/7/365 schedule. Approximately 100 full-time staff and 300 drivers are employed at this facility.

- **Greenville Bus Garage** is a bus maintenance and storage facility in Jersey City, NJ. This is a two-story building with approximately 85,000 square feet of space for offices, maintenance/refuelling/storage spaces, and locker rooms. This facility also includes a separate parking lot across the street large enough to park 25-30 buses. This facility operates on a 24/7/365 schedule.

- **Port Imperial Ferry Terminal** is located in Weehawken, NJ. This is a multimodel station supporting ferry, light rail, and bus services. This facility operates 16 hours per day; with the parking area open 24/7.

Each of these facilities will be modified to possess its own generation and/or storage systems, with natural gas generators and PV systems, where appropriate, as the main sources of power generation, and select facilities may employ chemical battery systems and flywheel energy storage as their main energy storage systems. The expected generation at each of the microgrids is presented in

Microgrid	Generation
Microgrid Central Facility (MCF) + Rail Loads	Originally six 20 MW natural gas generators and 150 kW PV plant, but new design will have more renewables
Newark Penn Station	200 kW natural gas generator
Broad Street Station	200 kW/250 kVA natural gas generator
Secaucus Station	Two 1035 kW natural gas generators
Wayne Bus Garage	1000 kW natural gas generator, 675 kW rotary UPS flywheel, 75 kW carport canopy solar PV system
Meadowlands Bus Garage	Two 785 kW natural gas generators
Greenville Bus Garage	500 kW natural gas generator
Port Imperial Ferry Terminal	250 kW generator

Table 5-1. NJ TRANSITGRID Networked Microgrid generation assets based on the 10% or 20% designs.

Table 5-1 and represented in Figure 5-1. The relative locations of several of these sites is included in Figure 5-2.

5.1.3. Rail Operations Center

The Rail Operations Center (ROC) will act as the primary OT data aggregation and control location for the MCF and seven DG-Networked Microgrid (NM) facilities connected to it. The ROC includes engineering Work stations, E-mail servers, IT services, inventory systems, scheduling systems, etc. This location will also act as the Security Operational Center (SOC) for the MCF and IMs. All the sites will be programmatically connected to the ROC to provide several centralized services:

1. Power system monitoring and control using supervisory control and data acquisition (SCADA).
2. Emergency operations communications and operational alerts to communicate between the IMs and ROC.
3. Cybersecurity information from NIDS/HIDS and other tools to perform threat hunting and detect adversary operations.

5.2. Power, Emergency Operations, and Cybersecurity Communications

5.2.1. SCADA Power Data

The MCF must interface with three remote rail entities that are not owned by NJT:

1. Amtrak rail connected through Substation 41. Power information is exchanged with the Central Electrification and Traffic Control (CETC) facility. MCF power will be interconnected with Amtrak at Substation 41. Power operations with Amtrak will be coordinated using

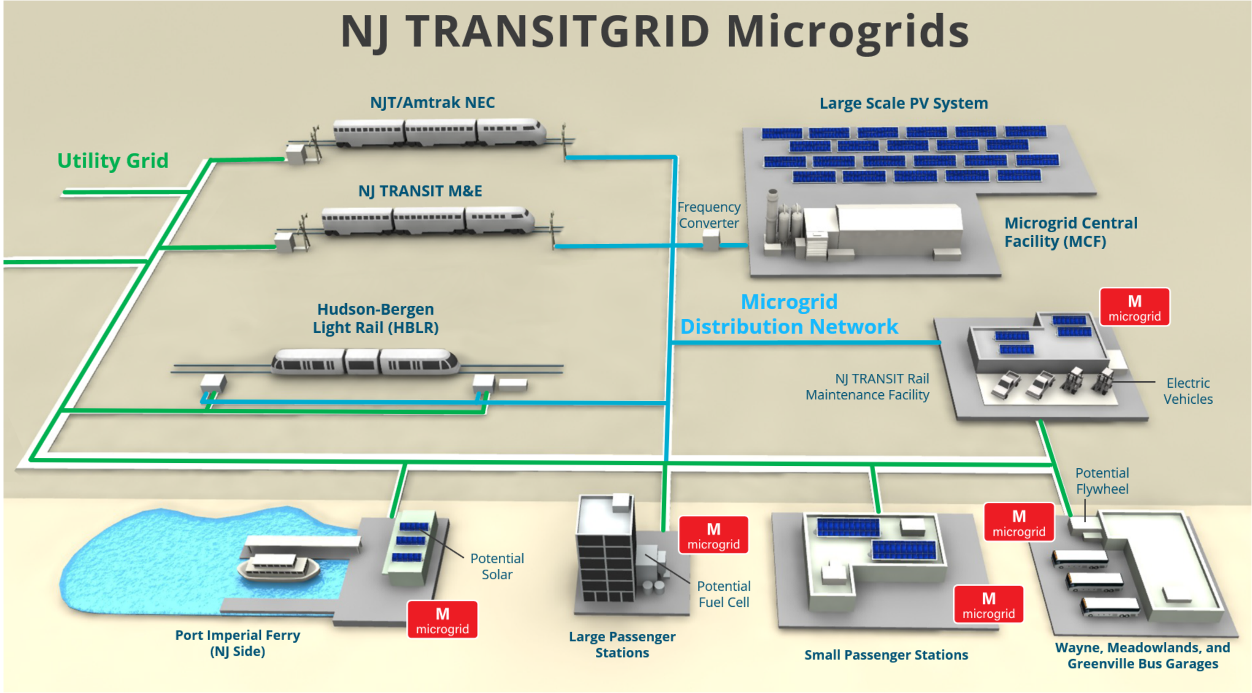

NJ TRANSITGRID Microgrids
Utility Grid
NJT/Amtrak NEC
NJ TRANSIT M&E
Hudson-Bergen Light Rail (HBLR)
Large Scale PV System
Frequency Converter
Microgrid Central Facility (MCF)
Microgrid Distribution Network
M microgrid
NJ TRANSIT Rail Maintenance Facility
Electric Vehicles
Potential Flywheel
Potential Solar
Potential Fuel Cell
Port Imperial Ferry (NJ Side)
Large Passenger Stations
Small Passenger Stations
Wayne, Meadowlands, and Greenville Bus Garages

Figure 5-1. Representation of the MCF feeding rail loads and the smaller DG IMs powering rail, bus, and ferry facilities

SCADA data–including breaker states, voltage, and frequency conversion status (25 Hz for Amtrak, 60 Hz for Transit)–run over fiber optic cable from the MCF to Substation 41. Based on the MCF power generation levels, Amtrak will coordinate emergency mode operations (i.e., reduce service).

2. NJT Morrison Essex (M&E) powered through Mason Substation owned by PSE&G. Two lines run from MCF to PSE&G's Mason Substation. In order to power that system during an outage, PSE&G must isolate two breakers from the utility which are close under normal operations. This will be coordinated via phone and SCADA data from the Mason Substation.

3. Hudson-Bergen Light Rail (HBLR). MCF will provide power to the Hoboken East substation that provides power to HBLR in its northern segments. A nanogrid provides power directly to the southern segments utilizing two onsite generation units at the HBLR yard shop. The nanogrid will be monitored and controlled by the MCF.

Each of these entities requires SCADA data to be fed to the ROC power control system in order to know which stations are energized. The ROC communicates with all NJT rail systems and Amtrak, potentially with additional information from the light rail systems. Although station loads (except for Hoboken) are not provided by the MCF generators, the MCF will be aware of any DG microgrid station outages through status information data because it drives generation requirements. There will be no rail control from the MCF.

To bid into PJM markets (e.g., day-ahead wholesale or ancillary markets), secure bids from the MCF to PJM would be placed. PJM would communicate back to the MCF production schedules. In the case of providing PJM Balancing Operations [73], the MCF will need to communicate with

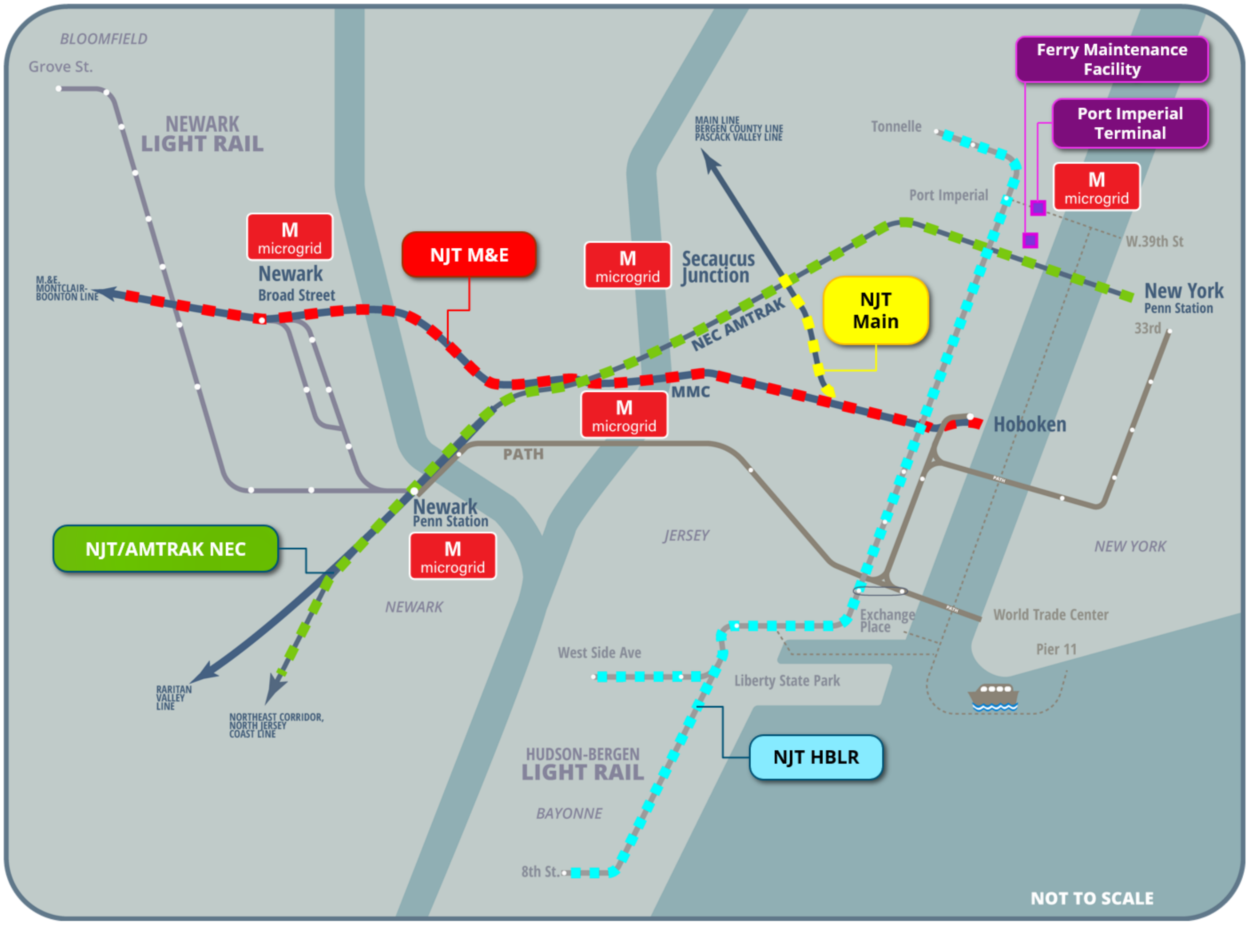


Figure 5-2. Locations of IMs and rail lines

PJM with a 2-second scan rate to get the Automatic Generation Control (AGC) signal value for the traditional signal (RegA) and the dynamic signal (RegD), and provide the current MCF generation level back to PJM. Regulation signal path communications with PJM will use Inter-Control Center Communication Protocol (ICCP) to communicate from an MCF Communication Front End (CFE) to the PJM Energy Management System (EMS) or Generation Management System (GMS).

5.2.2. Rail Data

In the first 2 hours of any outage, the MCF must power Amtrak rail systems to provide safe haven for Amtrak equipment and passengers, e.g., tunnel evacuation. Amtrak communications will be made from the Rail Operations Center (ROC) to Amtrak. NJT will also receive real-time, read-only Northwest Passage rail data (e.g., switching signals, traffic routing, designation of safe-harbor locations, etc.). Similar information is provided to Amtrak so that the same screens are available at the ROC and Amtrak's Central Electrification and Traffic Control (CETC) facility in Penn Station, New York. While rare, freight railroads (Norfolk Southern, CONRAIL) are permitted to operate diesel trains up to the Jersey Portal tunnel, but these communications are anticipated to be via telephone or radio. These communications would alert the freight operators that they cannot use the Northeast Corridor (NEC) during the emergency.

5.2.3. Communications during Emergencies

Different communication systems may fail depending on the type and severity of the emergency. Fiber connections may be severed during underground maintenance work, or entire cellular networks could be down from high winds during a superstorm. Ideally, the ROC would maintain visibility and control of the MCF and DG IMs, but local, fallback control functionality should be available for all sites in the event of communication failures. To coordinate operations of field teams with NJT leadership, it is recommended to have redundant communication options (e.g., local Ethernet-based messaging, cellular voice and text, radios, etc.) to coordinate power system and transportation operations during emergencies. Externally, NJT would communicate with law enforcement, local fire departments, the Department of Homeland Security, and other emergency communications using land or cellular phone systems.

5.2.4. Cybersecurity Data

The ROC will act as the SOC for both the MCF and DG IMs as shown in Fig. 4-1. Each of the IMs will include network- and host-based intrusion detection/prevention systems, logging tools, and other data collectors which will be aggregated at the ROC for processing and analysis. The SOC will include a SIEM, and potentially, a SOAR, or other remediation systems that can change the firewall rules and network topology, or take other actions. SOC analysts will perform threat hunting and organize incident response operations.

5.3. Architecture Design

NJT cybersecurity architecture was designed using the Purdue model discussed above. The OT Security features are concentrated in the Control Zone, as shown in Fig. 5-3.

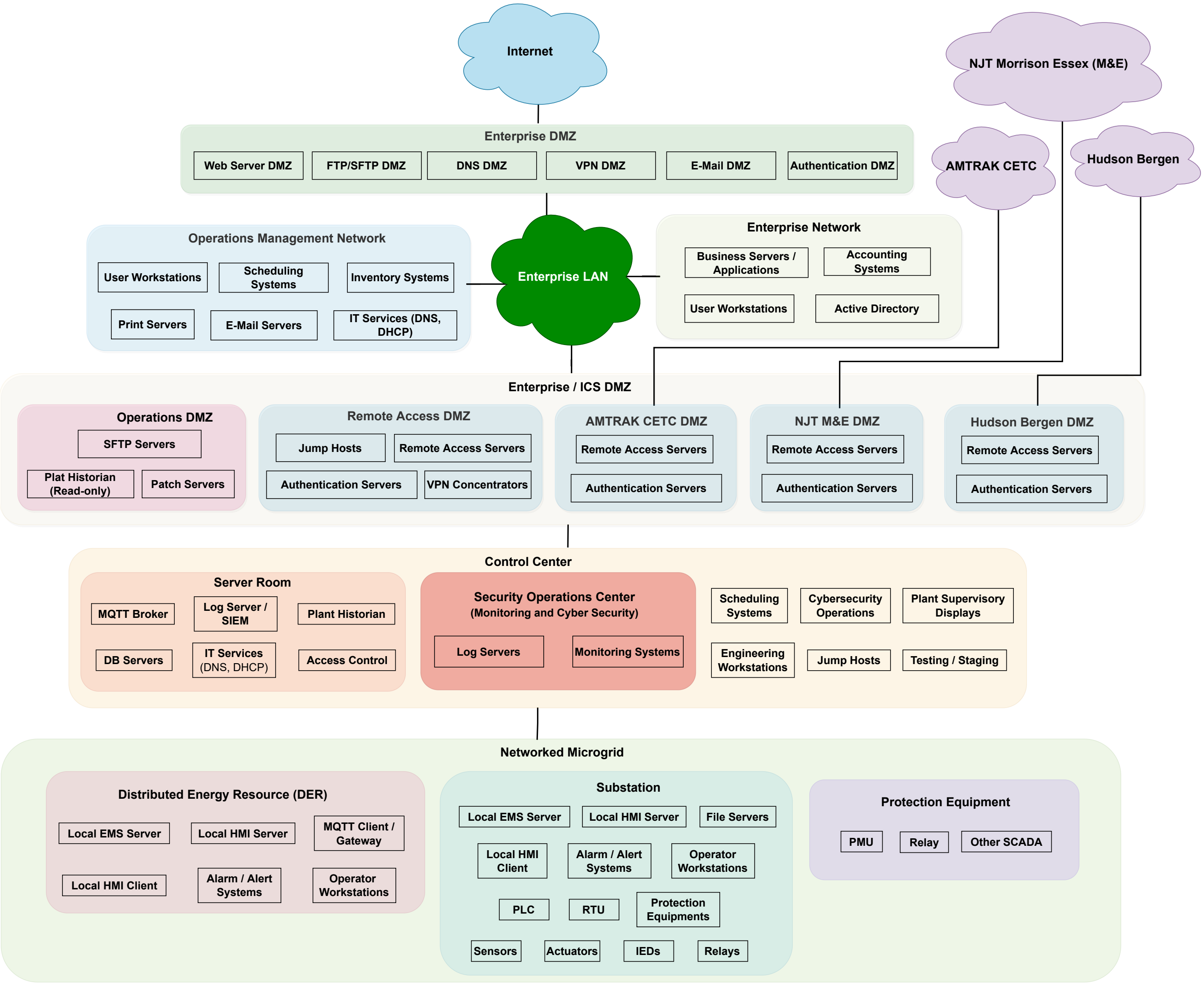


Figure 5-3. NJT IT/OT Network Overview

Since some enterprise/IT assets need to communicate with the control network, they are connected through a DMZ. Some IT resources that need OT data could include websites providing real-time data on trains, ridership levels, or billing operations. The DMZ acts as a barrier between the control network and the business/IT network. The DMZ also acts as a landing place for all the external connections to PJM and Amtrak/M&E/Hudson Bergen Light Rail. As a defense-in-depth measure, each entity connected to the control network is given a separate isolated DMZ, as recommended in [54]. This ensures that proper control is established between the control network and external networks, and in case of a compromise to one of the DMZs, other systems and connections would not be affected. This architecture is shown in Fig. 5-4. The connections would also be in compliance with security frameworks and regulatory standards, such as the use of least-privilege principles, and multi-factor authentication. These would ensure that authorized personnel and processes gain just the required amount of access to the control network, in order to perform their operations.

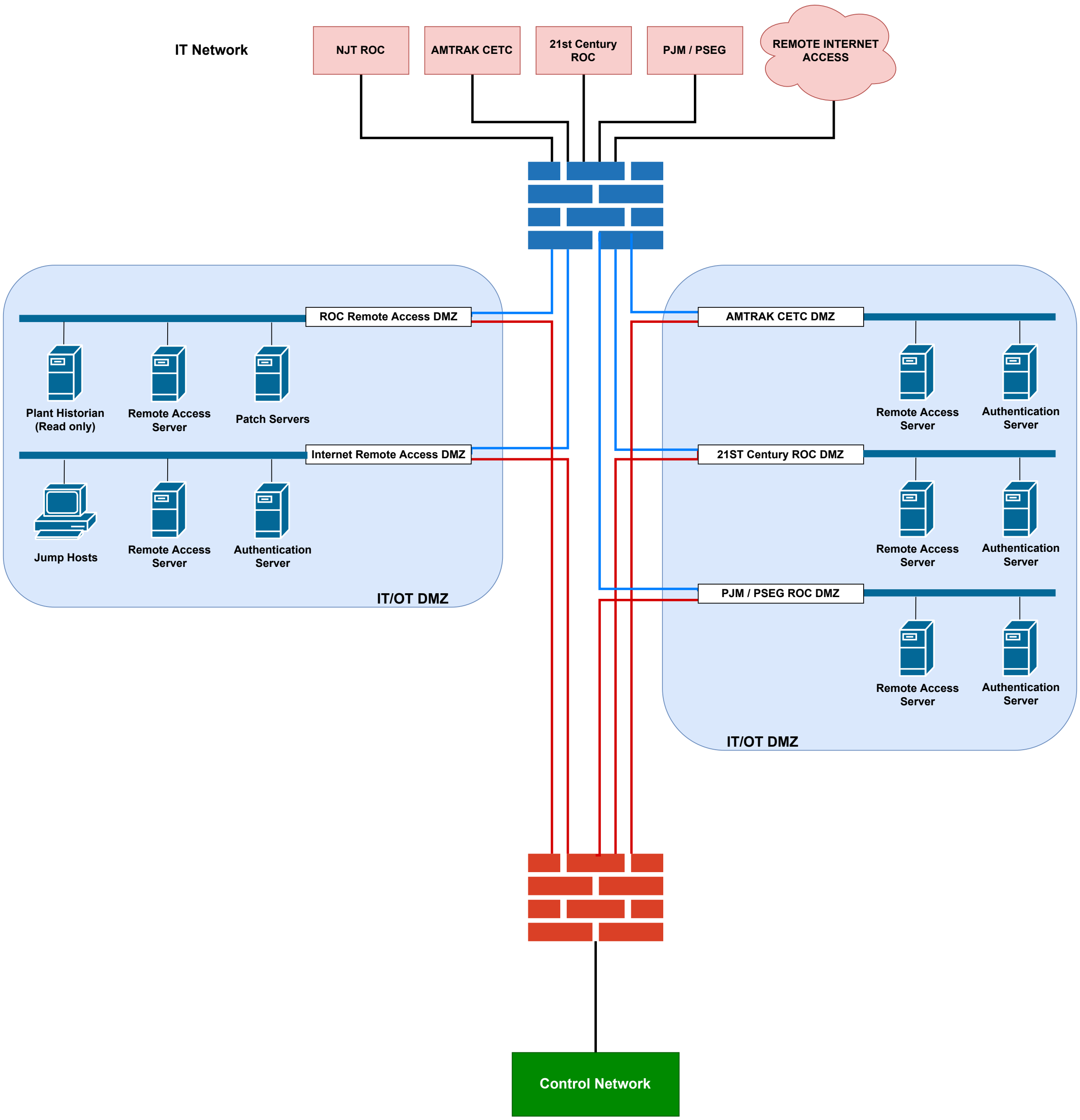


Figure 5-4. The IT/OT DMZ

The NJT OT/control network is responsible for power, rail, and security operations, including those at the MCF and DG IMs. It will gather data from the IMs, PJM, Amtrak/M&E/Hudson Bergen Light Rail, and other resources to run NJT's business. This system is shown in Fig. 5-5. Additionally, the ROC Operations Center (shown in Fig. 5-4) will house the SOC, SIEM, security team, HMIs, databases, etc.

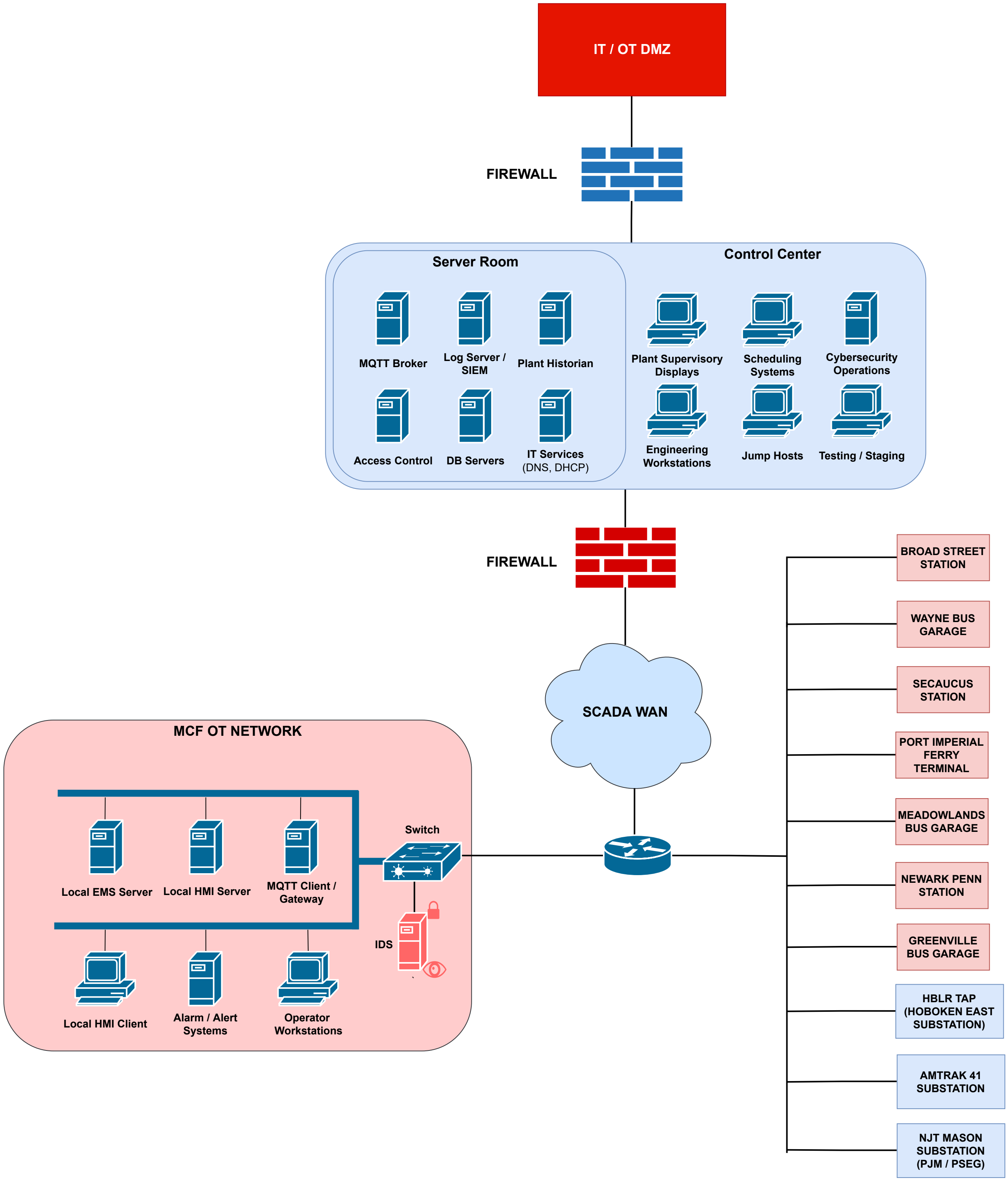


Figure 5-5. The NJT Control Network Logical Design

6. CONCLUSION

This report proposes a cyber-secure reference network architecture for networked and interdependent microgrids. The approach uses traditional perimeter defenses with zero-trust architecture concepts to provide remote access, while defending the IT and OT systems from a range of threats. The segmented topology includes IDS/IPS, SIEM, and SOAR technologies to provide situational awareness for cybersecurity analysts, threat hunters, and forensic teams. To demonstrate the concepts, a reference network design was created for the NJ TRANSITGRID project, which included the IT and OT networks for eight interdependent microgrids with several cyber-hardening features and tools to detect and respond to adversary actions.

REFERENCES

[1] H. Bevrani, B. François, and T. Ise, *Microgrid dynamics and control*. John Wiley & Sons, 2017.

[2] J. E. Stamp, "Spiders: Smart power infrastructure demonstration for energy reliability and security," Oct 2011.

[3] F. Flores-Espino, J. Giraldez Miner, and A. Pratt, "Networked microgrid optimal design and operations tool: Regulatory and business environment study," tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States), 2020.

[4] J. Giraldez Miner, A. Pratt, and F. Flores-Espino, "Networked microgrid optimal design and operations tool: Regulatory and business environment study," tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States), 2020.

[5] W. Yuan, J. Wang, F. Qiu, C. Chen, C. Kang, and B. Zeng, "Robust optimization-based resilient distribution network planning against natural disasters," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2817–2826, 2016.

[6] Z. Wang, B. Chen, J. Wang, and C. Chen, "Networked microgrids for self-healing power systems," *IEEE Transactions on smart grid*, vol. 7, no. 1, pp. 310–319, 2015.

[7] K. P. Schneider, F. K. Tuffner, M. A. Elizondo, C.-C. Liu, Y. Xu, S. Backhaus, and D. Ton, "Enabling resiliency operations across multiple microgrids with grid friendly appliance controllers," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4755–4764, 2017.

[8] Z. Liang, Q. Alsafasfeh, and W. Su, "Proactive resilient scheduling for networked microgrids with extreme events," *IEEE Access*, vol. 7, pp. 112639–112652, 2019.

[9] M. N. Alam, S. Chakrabarti, and A. Ghosh, "Networked microgrids: State-of-the-art and future perspectives," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1238–1250, 2018.

[10] A. Ouammi, H. Dagdougui, and R. Sacile, "Optimal control of power flows and energy local storages in a network of microgrids modeled as a system of systems," *IEEE Transactions on Control Systems Technology*, vol. 23, no. 1, pp. 128–138, 2014.

[11] P. Tian, X. Xiao, K. Wang, and R. Ding, "A hierarchical energy management system based on hierarchical optimization for microgrid community economic operation," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2230–2241, 2015.

[12] Z. Wang, B. Chen, J. Wang, *et al.*, "Decentralized energy management system for networked microgrids in grid-connected and islanded modes," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 1097–1105, 2015.

[13] S. Mojtahedzadeh, S. N. Ravadanegh, and M.-R. Haghifam, "Optimal multiple microgrids based forming of greenfield distribution network under uncertainty," *IET Renewable Power Generation*, vol. 11, no. 7, pp. 1059–1068, 2017.

[14] L. Ren, Y. Qin, Y. Li, P. Zhang, B. Wang, P. B. Luh, S. Han, T. Orekan, and T. Gong, "Enabling resilient distributed power sharing in networked microgrids through software defined networking," *Applied Energy*, vol. 210, pp. 1251–1265, 2018.

[15] R. Zamora and A. K. Srivastava, "Multi-layer architecture for voltage and frequency control in networked microgrids," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 2076–2085, 2016.

[16] M. S. Golsorkhi, D. J. Hill, and H. R. Karshenas, "Distributed voltage control and power management of networked microgrids," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 6, no. 4, pp. 1892–1902, 2017.

[17] Z. Wang and J. Wang, "Service restoration based on ami and networked mgs under extreme weather events," *IET Generation, Transmission & Distribution*, vol. 11, no. 2, pp. 401–408, 2017.

[18] A. Arif and Z. Wang, "Networked microgrids for service restoration in resilient distribution systems," *IET Generation, Transmission & Distribution*, vol. 11, no. 14, pp. 3612–3619, 2017.

[19] M. N. Alam, S. Chakrabarti, and X. Liang, "A benchmark test system for networked microgrids," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6217–6230, 2020.

[20] M. J. Reno, S. Brahma, A. Bidram, and M. E. Ropp, "Influence of inverter-based resources on microgrid protection: Part 1: Microgrids in radial distribution systems," *IEEE Power and Energy Magazine*, vol. 19, no. 3, pp. 36–46, 2021.

[21] G. Liu, M. R. Starke, B. Ollis, and Y. Xue, "Networked microgrids scoping study," *ORNL, TN. Available at https://info.ornl.gov/sites/publications/files/Pub68339.pdf*, pp. 0093–9994, 2016.

[22] A. Ellis, "Improving microgrid cybersecurity," in *Workshop Presentation on Microgrid Design. Sandia National Laboratories, November*, vol. 24, 2016.

[23] H. Farhangi and G. Joós, *Microgrid Planning and Design: A Concise Guide*. John Wiley & Sons, 2019.

[24] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," *NIST Special Publication 800-207*, 2020.

[25] O. ICEFAL, "The legacy of "insecure by design" and its implications for certifications and risk management." Available at https://www.forescout.com/resources/ot-icefall-report/.

[26] G. Ericsson, O. Torkilseng, G. Dondossola, T. Jansen, J. Smith, D. Holstein, A. Vidrascu, and J. Weiss, "Security for information systems and intranets in electric power systems," *Tech. Brochure (TB)*, vol. 317, 2007.

[27] L. Shen, "The NIST cybersecurity framework: Overview and potential impacts," *Scitech Lawyer*, vol. 10, no. 4, p. 16, 2014.

[28] K. Stouffer, J. Falco, K. Scarfone, *et al.*, "Guide to industrial control systems (ICS) security," *NIST special publication 800-82*, 2011.

[29] G. Hale, "Key challenges facing it/ot: Hear from the experts." Available at https://www.belden.com/blogs/key-challenges-facing-it-and-ot-in-the-next-five-years (2021).

[30] IEC, "IT vs. OT: Differing security requirements in the informational technologies (IT) environment and technologies in operational (OT) environment." Available at https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/it-vs-ot/ (2022).

[31] R. M. Blank, "Guide for conducting risk assessments," 2011.

[32] J. Dalton, "Unified facilities criteria (ufc)-cybersecurity of facility-related control systems," tech. rep., Naval Facilities Engineering Command, Alexandria, VA, 2016.

[33] D. C. Exchange, "Control correlation identifier (cci)." Available at https://public.cyber.mil/stigs/cci/.

[34] R. S. Ross *et al.*, "Risk management framework for information systems and organizations: A system life cycle approach for security and privacy," 2018.

[35] J. Stevens, "Electricity subsector cybersecurity capability maturity model (ES-C2M2) (case study)," tech. rep., Carnegie-Mellon, Univ. Pittsburgh PA Software Engineering Inst, 2014.

[36] CISA, "DHS cyber security evaluation tool (CSET)." Available at https://www.cisa.gov/uscert/ics/Downloading-and-Installing-CSET.

[37] C. Powell, K. Hauck, T. Reynolds, A. Sanghvi, M. Touhiduzzaman, and J. Van Natta, "Distributed energy resources cybersecurity framework: Applying the nist risk management process," tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States), 2020.

[38] J. E. Stamp, C. K. Veitch, J. M. Henry, D. H. Hart, and B. Richardson, "Microgrid cyber security reference architecture (v2).," tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2015.

[39] Z. Li and M. Shahidehpour, "Defense-in-depth framework for microgrid secure operations against cyberattacks," in *2017 IEEE Power & Energy Society General Meeting*, pp. 1–5, IEEE, 2017.

[40] T. J. Williams, "The purdue enterprise reference architecture," *Computers in industry*, vol. 24, no. 2-3, pp. 141–158, 1994.

[41] U. DOE, "Reference architectures as a means of influencing electric energy operational technology/industrial control system security outcomes." Available at https://inl.gov/wp-content/uploads/2022/04/SEI-ETF-Reference-Architecture-for-EEOT.pdf (2022/03/09).

[42] U. DOE, "Reference architecture for electric energy ot and accompanying profiles." Available at https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-Reference-Architecture-for-Electric-Energy-OT-and-Profiles.pdf (2022/03/08).

[43] L. Obregon, "Secure architecture for industrial control systems," *SANS Institute InfoSec Reading Room*, vol. 2, 2015.

[44] CISCO, "Cisco trustsec for pci scope reduction—verizon assessment and validation." Available at https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec_pci_validation.pdf.

[45] GE, "Opshield from ge digital protection for industrial controls and critical infrastructure networks." Available at https://www.ge.com/digital/sites/default/files/download_assets/opshield-2-4-from-ge-digital.pdf.

[46] Cloudfare, "What is a WAF? | web application firewall explained." Available at https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/.

[47] Rockwell Automation, "Converged plantwide ethernet (cpwe) design and implementation guide," *Design and implementation guide, Rockwell Automation*, vol. 9, 2011.

[48] M. Giles, "Triton is the world's most murderous malware, and it's spreading," *MIT Technology Review*, 2019.

[49] E. D. Knapp and J. Langill, *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

[50] G. Belding, "Firewalls for ICS/SCADA environments." Available at https://resources.infosecinstitute.com/topic/firewalls-for-ics-scada-environments/ (2020/04/28).

[51] D. Crum, "What is a data diode how do data diodes work?." Available at https://owlcyberdefense.com/blog/what-is-data-diode-technology-how-does-it-work/ (2018/06/25).

[52] A. Scott, "Tactical data diodes in industrial automation and control systems," *SANS Institute InfoSec Reading Room*, pp. 1–32, 2015.

[53] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," tech. rep., National Institute of Standards and Technology, 2020.

[54] S. Mathezer, "Introduction to ICS security part 3." Available at https://www.sans.org/blog/introduction-to-ics-security-part-3/ (2021/10/01).

[55] T. Olzak, "ICS/SCADA access controls." Available at https://resources.infosecinstitute.com/topic/ics-scada-access-controls/ (2019/08/19).

[56] Pam, "Vlan hopping: How to mitigate an attack." Available at https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation (2019/12/09).

[57] I. World, “Two sides of IT vs. OT security and ICS security operations.” Available at https://iiot-world.com/ics-security/cybersecurity/two-sides-of-it-vs-ot-security-and-ics-security-operations/ (2019/05/06).

[58] INCIBE, “SIEM deployment in OT environments.” Available at https://www.incibe-cert.es/en/blog/siem-deployment-ot-environments (2019/11/14).

[59] G. Belding, “SIEM for ICS/SCADA environments.” Available at https://resources.infosecinstitute.com/topic/siem-for-ics-scada-environments/ (2020/04/28).

[60] S. Subramoni, “Integrate IT and OT security operations to protect the purpose of a business.” Available at https://www.tcs.com/content/dam/tcs/pdf/perspectives/integrated-it-ot-soc-approach.pdf (2021/02/01).

[61] Dragos, “Insights into building an industrial control system security operations center.” Available at https://www.dragos.com/wp-content/uploads/Dragos-Insights-into-Building-an-ICS-Security-Operations-Center.pdf (2017/03/01).

[62] M. Hoffman, “Gaining endpoint log visibility in ICS environments.” Available at https://csiac.org/articles/gaining-endpoint-log-visibility-in-ics-environments/ (2019/09/19).

[63] T. Sweeney, “Back to basics with log management, siems mssps.” Available at https://www.darkreading.com/edge-articles/back-to-basics-with-log-management-siems-mssps (2019/07/12).

[64] IT Perfection, “Syslog.” Available at https://www.itperfection.com/network-security/network-monitoring/syslog-server-network-monitoring0security-cybersecurity-protocol/.

[65] McAfee, “Protecting industrial control systems using mcafee firewall enterprise,” tech. rep., 2009.

[66] K. E. Nawyn, “A security analysis of system event logging with syslog,” *SANS Institute, As part of the Information Security Reading Room*, 2003.

[67] M. Horkan, “Challenges for ids/ips deployment in industrial control systems,” *SANS Institute reading room*, 2015.

[68] C. Lai, A. R. Chavez, C. B. Jones, N. Jacobs, S. Hossain-McKenzie, J. Johnson, and A. Summers, “Review of intrusion detection methods and tools for distributed energy resources,” tech. rep., Sandia National Laboratories, Albuquerque, NM, 2021.

[69] Redscan, “What is SOAR?.” Available at https://www.redscan.com/news/what-is-security-orchestration-automation-and-response-soar-and-how-does-it-improve-threat-detection-and-remediation/ (2022/04/06).

[70] A. W. Mir and R. K. Ramachandran, “Implementation of security orchestration, automation and response (soar) in smart grid-based scada systems,” in *Sixth International Conference on Intelligent Computing and Applications*, pp. 157–169, Springer, 2021.

[71] K. Sheppard, “Report warns that superstorm sandy was not ’the big one’.” Available at https://www.huffpost.com/entry/sandy-hurricane-damage-co_n_5842958 (2017/12/06).

[72] National Hurricane Center, “Costliest U.S. tropical cyclones tables updated.” Available at https://web.archive.org/web/20180127083930/https://www.nhc.noaa.gov/news/UpdatedCostliest.pdf (2018/01/26).

[73] Dispatch, “PJM manual 12: Balancing operations.” Available at https://www.pjm.com/-/media/documents/manuals/m12.ashx (2022/10/01).

[74] B. Ponstein, “An introduction to microgrids; combining multiple power sources for maximum efficiency and uptime.” Available at https://www.mtu-solutions.com/content/dam/mtu/download/technical-articles/21162_Microgrids_TA.pdf/_jcr_content/renditions/original./21162_Microgrids_TA.pdf.

DISTRIBUTION

Hardcopy—External

Number of Copies	Name(s)	Company Name and Company Mailing Address

Hardcopy—Internal

Number of Copies	Name	Org.	Mailstop
1	OFA/NFE Agreements	10112	0115

Email—Internal [redacted]

Name	Org.	Sandia Email Address
Technical Library	1911	sanddocs@sandia.gov

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.