SANDIA REPORT

SAND2013-5472
Unlimited Release
Printed July 2013

Microgrid Cyber Security Reference Architecture

Version 1.0

Cynthia K. Veitch, Jordan M. Henry, Bryan T. Richardson, Derek H. Hart

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

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

SAND2013-5472
Unlimited Release
Printed July 2013

Microgrid Cyber Security Reference Architecture

Version 1.0

Cynthia K. Veitch, Jordan M. Henry, Bryan T. Richardson, and Derek H. Hart

Critical Infrastructure Systems
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0671

Abstract

This document describes a microgrid cyber security reference architecture. First, we present a high-level concept of operations for a microgrid, including operational modes, necessary power actors, and the communication protocols typically employed. We then describe our motivation for designing a secure microgrid; in particular, we provide general network and industrial control system (ICS)-specific vulnerabilities, a threat model, information assurance compliance concerns, and design criteria for a microgrid control system network. Our design approach addresses these concerns by segmenting the microgrid control system network into enclaves, grouping enclaves into functional domains, and describing actor communication using data exchange attributes. We describe cyber actors that can help mitigate potential vulnerabilities, in addition to performance benefits and vulnerability mitigation that may be realized using this reference architecture. To illustrate our design approach, we present a notional a microgrid control system network implementation, including types of communication occurring on that network, example data exchange attributes for actors in the network, an example of how the network can be segmented to create enclaves and functional domains,

and how cyber actors can be used to enforce network segmentation and provide the necessary level of security. Finally, we describe areas of focus for the further development of the reference architecture.

Acknowledgments

The Cyber Security technical team would like to acknowledge the following for help in this project:

- Ryan Custer, Mayuri Shakamuri, and Susan Wade of Sandia National Laboratories (SNL) for their extensive support in collecting information regarding vulnerabilities and information assurance controls for industrial control systems
- Regis Cassidy of SNL for his contribution to a preliminary reference implementation.
- Adrian Chavez of SNL for his contribution to identifying data exchanges between cyber security actors.
- John Clem of SNL for his contribution to a preliminary threat model analysis.
- Brian Van Leeuwen of SNL for his invaluable knowledge of communication protocols in industrial control systems
- Jonathan Gray of Idaho National Laboratory (INL) for his review, feedback, and contribution to building data exchange worksheets included in this document
- Erik Limpaecher, Scott VanBroekhoven, Michael Zhivich, and Mayank Varia of Massachusetts Institute of Technology (MIT) Lincoln Laboratory for their review and feedback.
- Representatives from US Pacific Command (USPACOM) and the Joint Information Operations Warfare Center (JIOWC) for their invaluable input.

The following government and industry partners offered continued review and valuable feedback through multiple iterations of the Cyber Security Reference Architecture document:

- Melanie Johnson of the US Army Engineer Research and Development Center (USAERDC) Construction Engineering Research Laboratory (CERL)
- Douglas Ellman of the Joint Innovation and Experimentation Division of USPACOM
- Robert Bradford of Burns & McDonnell
- Darrell Massie and Aura Lee Keating of Intelligent Power and Energy Research Corporation (IPERC)
- PJ Olson of SPARTA, Inc.

This page intentionally left blank.

Executive Summary

This document summarizes the on-going cyber security work and resulting cyber security reference architecture for a secure microgrid control system network. The architecture presented here provides guidelines and security recommendations for the implementation of a secure microgrid control system at Department of Defense (DOD) installations. The microgrid is designed using the Energy Surety Microgrid™ (ESM) methodology developed by Sandia National Laboratories (SNL). Microgrids developed using the ESM methodology demonstrate—

- increased reliability for critical mission loads resulting from the interconnection of electrical generation assets using the existing distribution network
- reduced reliance on diesel-generated backup power through the use of renewable energy sources during outages
- increased efficiency of diesel backup generators through careful, coordinated operation across the microgrid system
- reduced operational risk through a strong focus on cyber security

The design of a microgrid control system needs to be more robust than that of a traditional industrial control system (ICS) for the following reasons:

- The microgrid is used in emergency situations and may be critical to continuity of operations of an installation.
- The microgrid must function during active attack by a capable adversary.

As such, the traditional design and implementation for an ICS may not be sufficient for implementing a robust and secure microgrid.

Best practices for securing ICSs leverage network segmentation; for example, see [1], [2], and [3]. In most cases, however, network segmentation is focused on separation of the control system network from other less-trusted networks, such as the enterprise network and the Internet. The concept of network segmentation within the control system network itself is addressed to a minimal degree in a recommended practices document [1] published by the Department of Homeland Security (DHS) Control System Security Program (CSSP), but the additional complexities of configuring and managing such a network often result in this level of defense-in-depth being dismissed. In geographically dispersed control systems and field devices, physical segmentation often inherently exists within ICS command and control networks due to the employment of third-party providers for communication services. This segmentation is not leveraged to enhance security, however, as neither physical nor logical

segmentation is currently used as a basis for providing additional defense-in-depth within modern ICS networks.

The SNL approach to designing a secure microgrid control system network leverages segmentation to reinforce defense-in-depth practices. The microgrid control system network is segmented into enclaves defined by system functions, physical locations, and security concerns. An *enclave* is a collection of computing environments that is connected by one or more internal networks and is under the control of a single authority and security policy [4]. This concept of enclaves (already leveraged by DOD information systems in operation today [4, 5]) reduces the complexity of configuring and managing a segmented control system network. Enclaves are grouped together into *functional domains* that allow actors to collaborate in operational system functions that crosscut enclaves. Functional domains support reliable and secure data exchange necessary to accomplish system function by determining the necessary level of access for participating enclaves and arbitrating inter-enclave communication between actors within enclaves based on *data exchange* definitions.

Data Exchange

Data exchange defines communication between actors within enclaves and functional domains. Within an enclave, data exchange attributes describe the latency, bandwidth, and quality of service (QoS) for intra-enclave communications; types of network traffic to expect; and the necessary level of enclave cyber security. Within a functional domain, data exchange worksheets help to identify which enclaves need to communicate; types of network traffic that will be communicated between enclaves; latency, bandwidth, and QoS for inter-enclave communications; and cyber security concerns for inter-enclave communications.

A template data exchange worksheet was developed to support consistent identification of the operational necessities for data exchange between actors and cyber security needs for information assurance. For each actor interaction (i.e., communication between actors), the data exchange worksheet identifies the exchange to occur (including the type, interval, method, priority, and tolerance to latency), the data to be exchanged (including the type, accuracy, volume, and reliability), and the levels of information assurance required for securing the data exchange (including confidentiality, integrity, and availability).

Information Assurance

The DOD certifies and accredits information systems through an enterprise process known as the DOD Information Assurance Certification and Accreditation Process (DIACAP) for identifying, implementing, and managing information assurance (IA) capabilities and services, expressed as IA controls [5]. DIACAP will eventually be updated with DOD's Risk Management Framework, which will include a clearer mapping between DOD IA controls and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls [6]. As a necessary consideration of a microgrid at a DOD installation, we provide an overview of the controls necessary for compliance with DOD IA directives for information systems; these controls help to provide an appropriate level of security for information

assets essential to the operation of the microgrid. Information system integrators should take advantage of available certification and accreditation (C&A) tools, such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)[1] and DHS's Cyber Security Evaluation Tool (CSET)[2], to verify compliance with applicable IA controls. The microgrid cyber security reference architecture should, if utilized, help meet a majority of the technical IA requirements automatically.

Performance Benefits and Vulnerability Mitigation

By leveraging network segmentation to reinforce defense-in-depth practices, the cyber security reference architecture is expected to offer the following performance benefits and vulnerability mitigation:

- Each enclave operates under a single authority and security policy and provides a trusted environment for actors that need to communicate. Actors who wish to join a particular enclave must meet or exceed the level of security for the enclave in order to become part of that enclave. This ensures that all actors of the enclave are secured at the same rigor and level as the actors with which they are communicating.

- Enclave inter-communication is restricted and managed by functional domains. The functional domains govern the policies that enable actors in one enclave to communicate with actors in another enclave based on necessary data exchange attributes.

- Enclave boundaries provide good locations to monitor intrusion detection, unauthorized access attempts, and other logged events.

- Cleaving the logical network based on functional necessities, physical locations, and/or security concerns ensures a higher level of trust on each network segment.

- Isolation of enclaves minimizes both malicious opportunities and accidental damage done by a trusted, valid party. Providing communication barriers between enclaves and implementing enclave-specific security policies limits access by malicious actors within enclaves. This isolation also has the side effect of compartmentalizing valid actor access to only the enclave- or functional domain-level needed.

- Network performance may be improved based on necessary latency, bandwidth, and QoS.

- Traffic monitoring can be implemented within enclaves to perform deep packet inspection and detect any anomalous message codes. Since each data exchange has very specific attributes, the message code on the microgrid control system messages should be known for each actor interaction. The reduced traffic per enclave (due to fewer actors on the network segment) enables more accurate parsing and inspection of the traffic being monitored.

[1] `http://iase.disa.mil/stigs/`

[2] `http://www.us-cert.gov/control_systems/satool.html`

The use of enclaves to segment the microgrid control system network is expected to mitigate many of the vulnerabilities identified for traditional ICSs. Because segments of the control system network will be isolated, certain security risks (e.g., masquerading, message replay attacks, unauthorized access, eavesdropping, and network perimeter vulnerabilities) can be at least partially mitigated. By localizing the influence of actors to a particular enclave, the consequences of both local failures and vulnerabilities are isolated within that enclave.

Cyber Security Reference Architecture

This document is the microgrid cyber security reference architecture. First, we present a high-level concept of operations for the microgrid, including operational modes, necessary power actors, and the communication protocols typically employed. We then describe our motivation for designing a secure microgrid; in particular, we provide general network and ICS-specific vulnerabilities, a threat model, information assurance compliance concerns, and design criteria for the microgrid control system network. Our design approach addresses these concerns by segmenting the microgrid control system network into enclaves, grouping enclaves into functional domains, and describing actor communication using data exchange attributes. We describe cyber actors that can help mitigate potential vulnerabilities, in addition to performance benefits and vulnerability mitigation that may be realized using this reference architecture. To illustrate our design approach, we present a notional microgrid control system network implementation, including types of communication occurring on that network, example data exchange attributes for actors in the network, an example of how the network can be segmented to create enclaves and functional domains, and how cyber actors can be used to enforce network segmentation and provide the necessary level of security. Finally, we describe areas of focus for the further development of the microgrid cyber security reference architecture.

In addition to the cyber security reference architecture, this document includes appendices that (A) describe a cyber security reference implementation to illustrate the architecture; and (B) provide completed worksheets for the data exchanges used as part of the illustrative system.

Contents

List of Figures

List of Tables

Acronyms and Abbreviations

AGMC	automated grid management and control
ATO	Authority to Operate
ATS	automatic transfer switch
BITW	bump-in-the-wire
BMS	building management system
C&A	certification and accreditation
CERL	Construction Engineering Research Laboratory
CSCM	cyber security configuration management
CSET	Cyber Security Evaluation Tool
CSSA	cyber security situational awareness
CSSP	Control System Security Program
CSWG	Cyber Security Working Group
DER	distributed energy resource
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DIACAP	DOD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DNP3	Distributed Network Protocol
DNS	Domain Name System
DOD	Department of Defense
DODD	DOD Directive
DODI	DOD Instruction
DOE	Department of Energy
DoS	denial of service
EMS	energy management system
ESM	Energy Surety Microgrid™
EVSE	electric vehicle supply equipment
FEP	front-end processor
HMI	human-machine interface
HTTP	Hypertext Transfer Protocol

IA	information assurance
ICS	industrial control system
IDART	Information Design Assurance Red Team
IDS	intrusion detection system
IED	intelligent electronic device
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
IP	Internet Protocol
IPC	intelligent power controller
IPERC	Intelligent Power and Energy Research Corporation
IPS	intrusion prevention system
IPsec	Internet Protocol Security
IPv4	IP version 4
IPv6	IP version 6
IT	information technology
JIOWC	Joint Information Operations Warfare Center
kVAr	kilovolt-amperes reactive
kW	kilowatt(s)
LPG	liquefied petroleum gas
MAC	mission assurance category
MIT	Massachusetts Institute of Technology
MITM	man-in-the-middle
NCSD	National Cyber Security Division
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NREL	National Renewable Energy Laboratory
NSA	National Security Agency
NTP	Network Time Protocol
ORNL	Oak Ridge National Laboratory
PCC	point of common coupling
PEV	plug-in electric vehicle
PLC	programmable logic controller
PMU	phasor measurement unit
PV	photovoltaic

QoS	quality of service
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SNL	Sandia National Laboratories
SGIP	Smart Grid Interoperability Panel
SNAC	Systems and Network Analysis Center
SP	Special Publication
STIG	Security Technical Implementation Guide
SSH	secure shell
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS/SSL	Transport Layer Security/Secure Sockets Layer
UDP	User Datagram Protocol
UPS	uninterruptible power supply
US	United States
USAERDC	US Army Engineer Research and Development Center
USPACOM	US Pacific Command
VCSE	Virtual Control System Environment
VLAN	virtual local area network
XML-RPC	Extensible Markup Language for Remote Procedure Call

This page intentionally left blank.

Chapter 1

Introduction

This document summarizes the on-going cyber security work and resulting cyber security reference architecture for a secure microgrid control system network. The architecture presented here provides guidelines and security recommendations for the implementation of a secure microgrid control system at Department of Defense (DOD) installations. The microgrid is designed using the Energy Surety Microgrid™ (ESM) methodology developed by Sandia National Laboratories (SNL). The Department of Energy (DOE) design team includes experts from SNL, National Renewable Energy Laboratory (NREL), Oak Ridge National Laboratory (ORNL), and Idaho National Laboratory (INL). The ESM design allows the microgrid to operate in either grid-tied or islanded mode. Microgrids developed using the ESM methodology demonstrate—

- increased reliability for critical mission loads resulting from the interconnection of electrical generation assets using the existing distribution network
- reduced reliance on diesel-generated backup power through the use of renewable energy sources during outages
- increased efficiency of diesel backup generators through careful, coordinated operation across the microgrid system
- reduced operational risk through a strong focus on cyber security

1.1 Background

A microgrid, like any other microgrid or general power system, benefits from a control or automation system that helps facilitate, automate, and optimize operation of the power system. This control or automation system is commonly referred to as an *industrial control system* (ICS); in this document, we use the term *microgrid control system* to describe the information system used to facilitate operation of a microgrid. Given that the goal of a microgrid is to increase the reliability for critical DOD mission loads, it is crucial that the control system operating a microgrid be secure against adversarial attack. A large amount of work has gone into developing guidelines and best practices for securing ICSs, including publications by the DOD (e.g., [7]), the DOE (e.g., [8]), the Department of Homeland Security (DHS) (e.g., [1, 9, 10]), and the National Institute of Standards and Technology (NIST) (e.g., [2, 3], which were contributed to by DOD agencies and DOE laboratories). Such guidelines and best practices are referenced in this document, leveraged during the development of our design approach, and expanded on as part of the reference architecture.

1.2 Scope

The intent of this document is to support the intrinsically secure design of a microgrid control system with a focus on securing the data exchanges necessary for microgrid operations. Integrators are expected to leverage this document to—

- identify necessary data exchanges and their attributes
- determine how the microgrid control system network should be segmented based on the necessary data exchanges and any applicable information assurance (IA) controls
- identify the appropriate technologies and procedures best suited to implement the necessary network segmentation, mitigate general network and ICS-specific vulnerabilities, and comply with the DOD Information Assurance Certification and Accreditation Process (DIACAP) [5], if applicable, or any other regulatory requirements.

Future versions of this document will include a stronger focus on the design principles of monitoring and reconfiguration, in addition to an assessment of IA controls and how they can be met using the reference architecture and industry best practices for securing control systems.

1.3 Report Structure

This document is organized as follows:

- Chapter 1 provides background, scope, and purpose.
- Chapter 2 presents a high-level concept of operations for the microgrid, including operational modes, necessary power actors, and the communication protocols typically employed.
- Chapter 3 describes our motivation, including general network and ICS-specific vulnerabilities, the microgrid threat model, information assurance compliance concerns, and design criteria for the microgrid control system network.
- Chapter 4 describes our approach for designing a secure microgrid control system. The design approach includes segmenting the microgrid control system network into enclaves, grouping enclaves into functional domains, and describing actor communication using data exchange attributes. We describe cyber actors that can help mitigate potential vulnerabilities, in addition to performance benefits and vulnerability mitigation that may be realized using this reference architecture.
- Chapter 5 presents a notional microgrid control system network implementation, including types of communication occurring on that network, example data exchange attributes for actors in the network, an example of how the network can be segmented to create enclaves and functional domains, and how cyber actors can be used to enforce network segmentation and provide the necessary level of security.

- Chapter 6 introduces areas of focus for further development of the microgrid cyber security reference architecture.
- Appendix A describes a cyber security reference implementation.
- Appendix B provide completed worksheets for some data exchanges.

This page intentionally left blank.

Chapter 2

Concept of Operations

A microgrid is designed using the Energy Surety Microgrid^{TM} (ESM) methodology developed by Sandia National Laboratories (SNL). An ESM design implies a microgrid that can operate either grid-tied or in islanded mode and is comprised of the following types of loads:

- Tier 1 loads are critical to the mission of an installation and, usually, have dedicated backup generators.
- Tier 2 loads are conveniences during microgrid operations: they can be switched on or off the microgrid at the discretion of power system operators. Some Tier 2 loads have dedicated backup generators.
- Tier 3 loads are not powered during microgrid operations.

Microgrids developed with the ESM methodology demonstrate increased reliability for critical mission loads due to the interconnection of electrical generation assets on the existing distribution network; reduced reliance on diesel-generated backup power through the use of renewable energy resources during outages; increased efficiency of diesel backup generators through careful coordinated operation across the microgrid system; and reduced operational risk through a strong focus on cyber security.

2.1 Operational Modes

For the purpose of this reference architecture, a microgrid and its associated control system network will have three modes of operation. These modes are—

1. The microgrid is not active, and the microgrid energy management system (EMS) works with other microgrid control system actors for proper monitoring of the installation's power distribution system and initialization of the microgrid.
2. The microgrid is not active, but it is islanded from the installation's incoming utility feed. Backup diesel generators are active and powering their individual loads, but all renewable generation is offline.
3. The microgrid is active and islanded from the installation's incoming utility feed, sharing backup diesel and renewable generation resources. The microgrid control system is in a heightened cyber security state.

The first mode reflects the normal day-to-day operations of the microgrid. Although the microgrid is not active, parts of the microgrid control system are operational. For example, points of common coupling (PCCs) continually monitor the state of the installation's incoming utility power for outages and sustained periods of poor power quality.

The second mode reflects an emergency state moments after islanding the microgrid. All Tier 1 and Tier 2 loads with backup power generation are powered individually using their own resources. Once again, although the microgrid is not active at this point, parts of the microgrid control system are monitoring diesel generation and changing breaker connections in preparation for activation of the microgrid.

The third mode reflects an emergency state where the microgrid must be activated to ensure continuity of operations for the installation's critical and priority loads. Because the nature of this emergency might be unknown, it must be assumed that a capable adversary is actively attacking the installation's power distribution system. If the distribution system is under attack, the cyber security posture used for normal day-to-day operations might not be sufficient. For example, it might not be acceptable to allow communications from non-critical actors of the microgrid control system, especially if that actor is expected to be without power when the microgrid is active.

To describe the general operation of a microgrid, the following figures illustrate a simple implementation and show how the various distributed energy resources (DERs) (e.g., diesel generators) and loads transition from being grid-tied to an islanded microgrid. Figure 2.1 illustrates a microgrid feeder from a substation with a PCC (e.g., main breaker) dividing the upstream utility portion of the feeder from the downstream microgrid portion of the feeder. The microgrid consists of a collection of Tier 1 and Tier 2 loads (in this case, buildings), designated by the solid boxes, and Tier 3 loads, designated by the dashed boxes. Although most DERs are associated with a particular load (typically, an entire building), the renewable energy source is not attached to a specific load; instead, it is connected to the grid as an independent generation asset. The first mode of the microgrid's operation, characterized by power supplied by the utility and an inactive microgrid, is depicted in Figure 2.1.

Next, Figure 2.2 depicts the loss of utility power and the subsequent temporary interruption of power in all grid-tied loads that do not have uninterruptible power supply (UPS) systems. (In this example microgrid, only building B has a UPS system and experiences uninterrupted power.) All inverter-based renewable energy resources are simultaneously disconnected from the microgrid [11]. The microgrid control system signals Tier 3 building feeds to open, preventing them from being part of the microgrid. During this period, the Tier 1 and Tier 2 loads with diesel generation are powered individually by their backup diesel generator systems. Figure 2.3 illustrates this second mode of operation for the microgrid.

If loss of utility power is greater than a predetermined time period, generators are synchronized sequentially to the microgrid portion of the feeder until all Tier 1 and Tier 2 loads are supplied. At this point, the microgrid enters the third mode of operation, as illustrated in Figure 2.4. As appropriate, the generation provided by the diesel generators is automatically adjusted for more efficient use. In Figure 2.5, the entire microgrid is powered

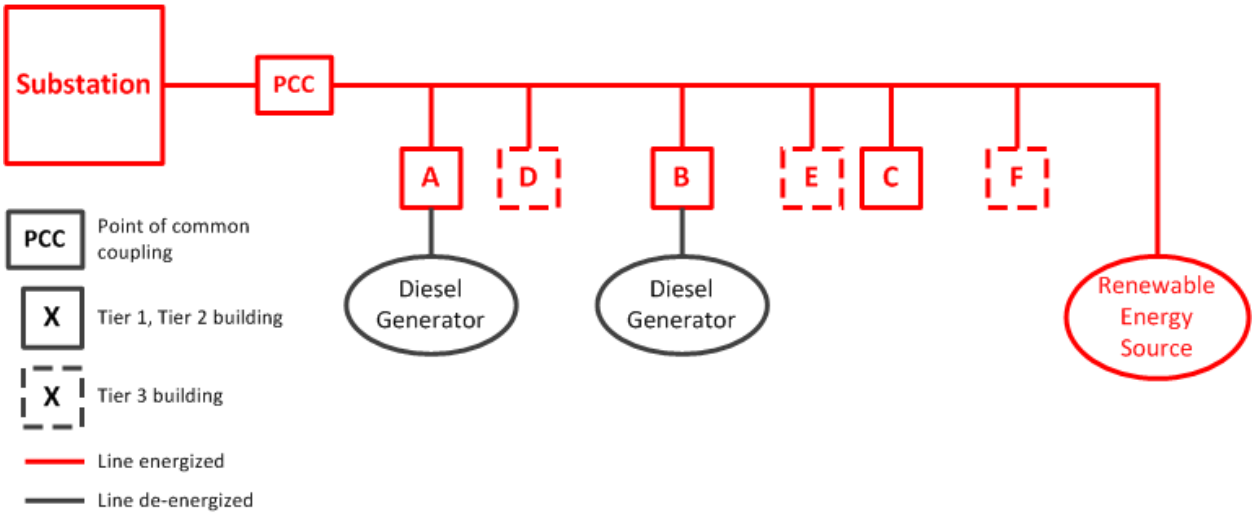

Figure 2.1. Normal day-to-day operations of a microgrid. All loads are grid-tied to a feeder supplied by the utility.

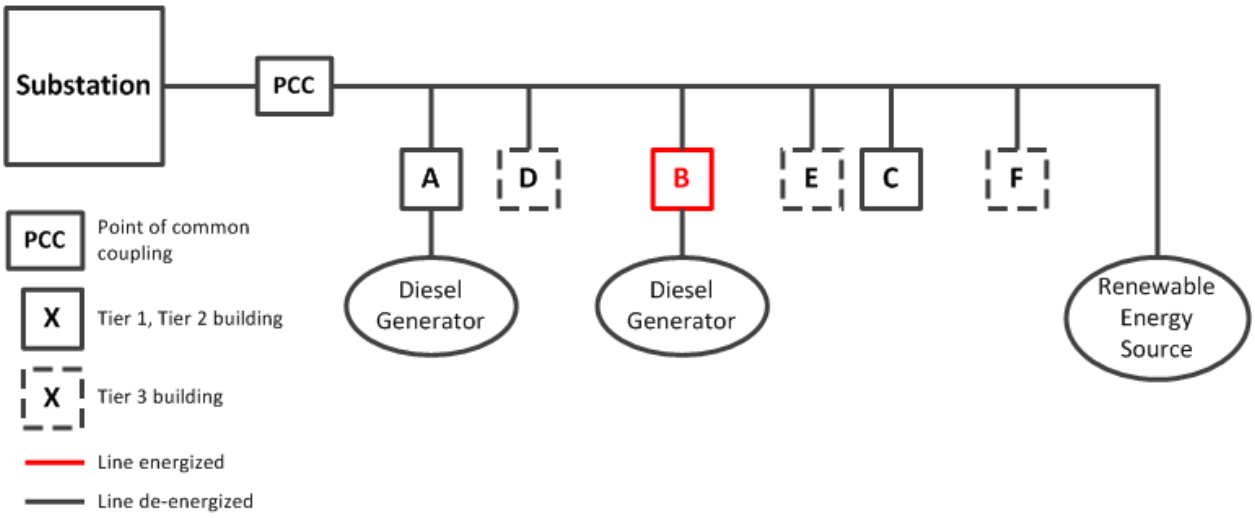

Figure 2.2. Microgrid conditions moments after a utility outage. Only loads with a UPS system (e.g., building B) experience no power interruptions.

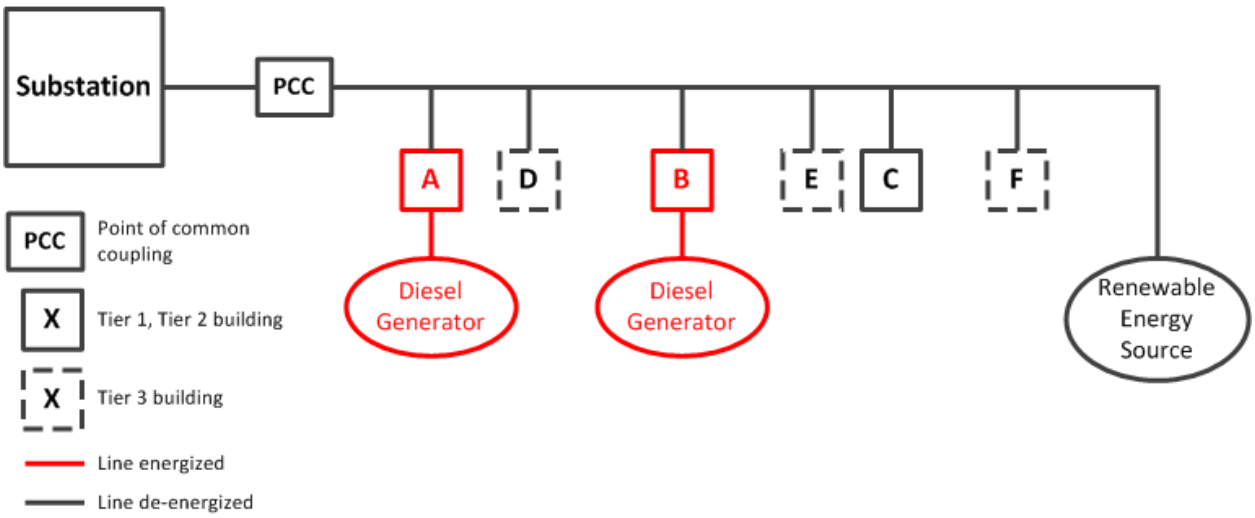

Figure 2.3. Normal emergency operations after a utility outage. Tier 1 and Tier 2 loads with backup diesel generator systems are powered individually.

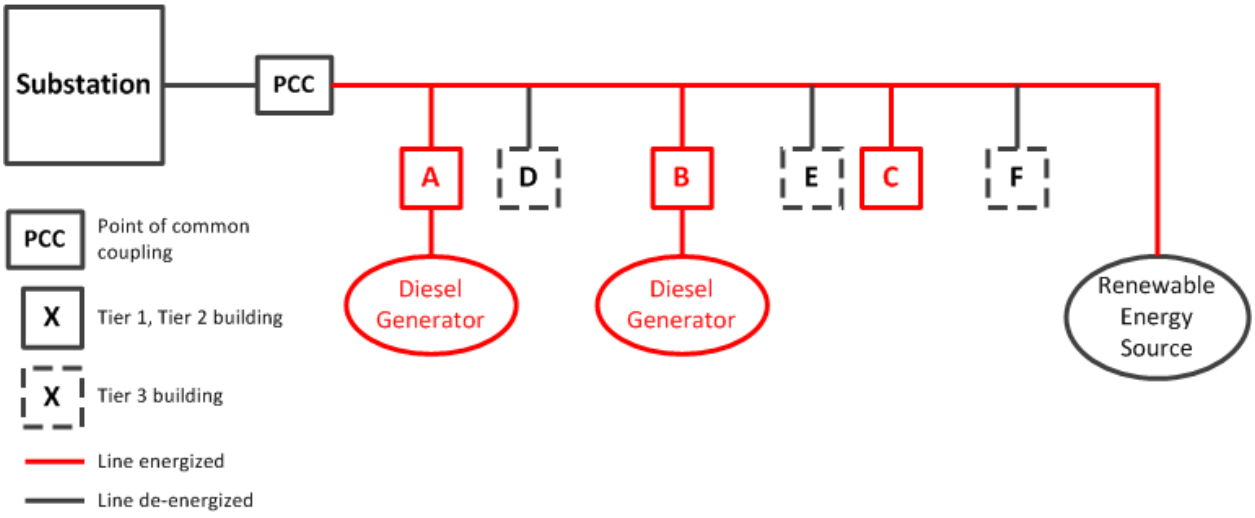

Figure 2.4. Microgrid conditions after generators are synchronized. After Tier 3 loads are disconnected, backup generators energize the microgrid to power all Tier 1 and Tier 2 loads.

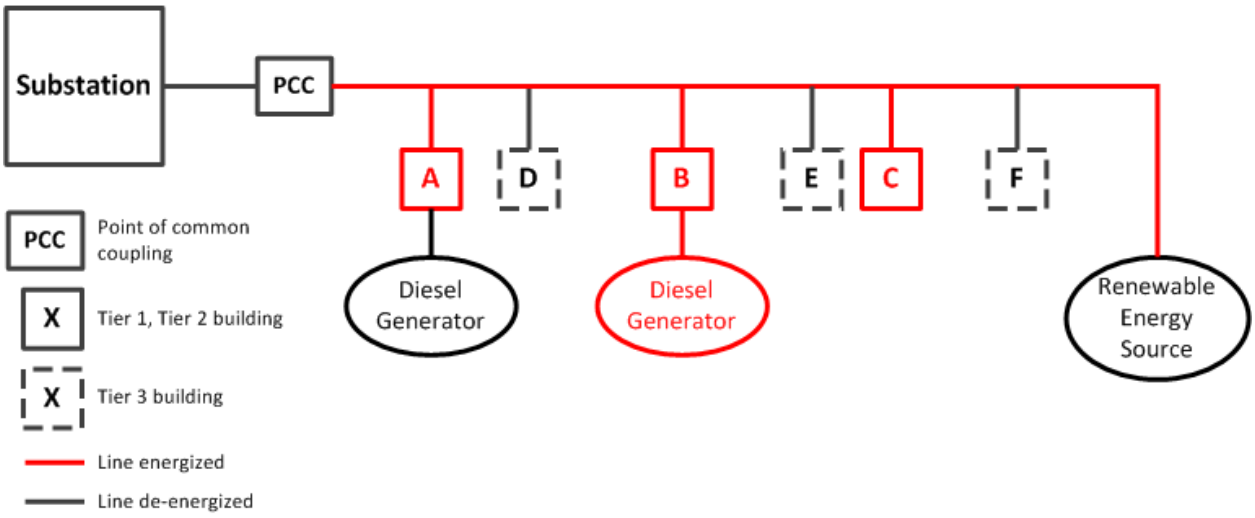

Figure 2.5. Microgrid conditions with efficient generation. After the microgrid is energized, unnecessary DERs can be cycled down.

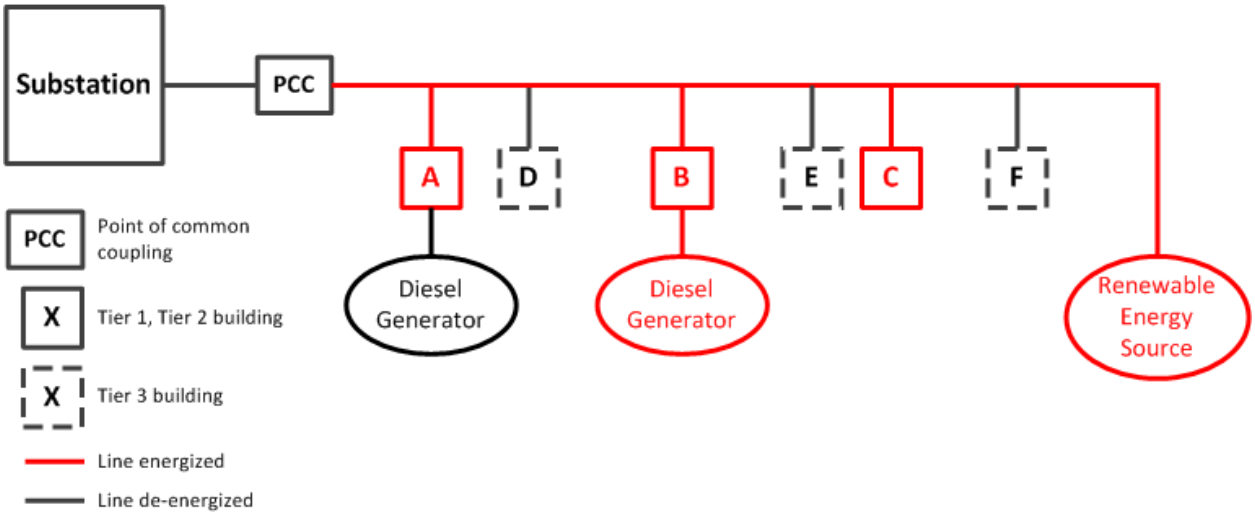

Figure 2.6. Microgrid conditions with connected renewable energy sources. After the microgrid is energized, inverter-based renewable resources connect to microgrid, signaling full activation of the microgrid.

by a single generator connected to building B. Then, if the microgrid remains energized for another specified period of time, inverter-based renewable energy sources come back online and begin supplying power to the microgrid, as depicted in Figure 2.6.

If utility power is restored for a sufficient period of time, the diesel generators either revert back to supplying only their Tier 1 loads (i.e., the second microgrid mode) or synchronize with the utility at the PCC. In the first case, the microgrid will lose power temporarily requiring any renewable energy sources to disconnect. The PCC then closes, restoring normal power to all loads and, later, allows renewable energy sources to reconnect to the microgrid.

2.2 Power Actors

The safety and stability of the microgrid requires the proper coordination of numerous power actors in the microgrid. In Table 2.1, these power actors are listed with a description of their purpose and whether or not the actor has a control system network connection. It is important to note that not every microgrid will include all the power actors described below; this list is meant to be generic in order to address most microgrid designs.

Table 2.1: Power actors in the microgrid control system network.

Actor	Description	Network Connection
Monitoring and Control		
Microgrid energy management system (EMS)	Central or distributed control system to monitor, control, and optimize microgrid operations	Yes: usually has a network connection to all other network-connected controllers
Historian	Database application that logs and records microgrid operational data	Yes: sends and receives data from EMS
Human-machine interface (HMI)	Console where a human can interact with EMS, including manual operation and control of microgrid	Yes: accesses HMI server to display operational data
HMI server	Information system that parses and formats EMS data to be viewed on HMI	Yes: receives data from EMS and sends data to HMI

Continued on next page.

Table 2.1 – continued from previous page.

Actor	Description	Network Connection
Protection		
Intelligent electronic device (IED)	General term that encompasses relays, microgrid controllers, or any microprocessor-based power system controller for power system equipment	Yes: sends power data to EMS for control functions
Protection relay	Electromechanical device that monitors flow in an electrical circuit and trips circuit breakers when a fault is detected	Depends: some do not possess network connection capabilities
Breaker	Automated electrical switch that protects circuits and devices from damage caused by a fault	No
Fuse	Sacrificial device that protects equipment and lines from fault current by allowing conductive material to melt and disrupt current	No
Generation		
Generator	Non-renewable electrical generation device, including diesel generators, gas generators, natural gas generators, and liquefied petroleum gas (LPG) generators	No
Generator controller	Device that controls generator power output, voltage, and frequency based on setpoints or commanded EMS values	Yes: EMS can monitor controller data and dynamically change controller setpoints
Automatic transfer switch (ATS)	Electrical switch installed where a backup generator is located; automatically switches load from utility source to backup generating source when power loss detected	Depends: some have network connectivity functionality, but it may not be utilized
Renewable energy generator	Generator that produces energy from a natural source, such as photovoltaic (PV) arrays, wind turbines, or geothermal resources	No
Renewable energy controller	Device that controls renewable power output, voltage, and frequency based on available natural resources or on commanded EMS values	Yes: EMS can monitor controller data and dynamically change controller setpoints

Continued on next page.

Table 2.1 – continued from previous page.

Actor	Description	Network Connection
Load		
Building management system (BMS)	Control system installed in a building that controls and monitors the building's electrical and mechanical equipment, such as lighting and environmental systems	Yes: EMS can monitor building energy consumption and change operational parameters, such as temperature setpoints
Load controller	Device that monitors and controls the amount of energy loads consumed by shedding, adding, or shifting load based on predetermined setpoints or by EMS commands	Yes: sends load data to EMS and receives EMS commands
Smart meter	Electrical meter that records energy consumption and power quality for monitoring and data collection purposes	Yes: sends energy information to EMS and historian
Distribution		
Remote terminal unit (RTU)	Equipment that monitors digital and analog field devices	Yes: transmits data to EMS
Phasor measurement unit (PMU)	Device that measures electrical waveforms in the microgrid using synchrophasors to assess the state of the electrical system and manage power quality	Yes: sends phasor data to EMS to adjust generation and load control setpoints
Point of common coupling (PCC) synchronizing relay	Relay that ensures the microgrid and utility are isolated when necessary and properly synchronized before reconnection	Yes: sends connection information and flow data to EMS
Distribution transformer	Transformer that converts electrical energy from one voltage to another	Depends: some have tap changers that allow finer voltage control and may allow tap settings to be changed remotely
Grounding transformer	Transformer that establishes an earth reference point for an ungrounded microgrid	No
Disconnect switch	Manually operated device to disconnect power system components from the power system after the power circuit has been interrupted by some other means	Depends: some can be manually operated from a remote location

Continued on next page.

Table 2.1 – continued from previous page.

Actor	Description	Network Connection
Storage		
Energy storage system	Equipment, such as batteries, flywheels, and pumped water, that stores some form of energy to convert into electrical energy at a later time	No
Energy storage controller	Device that controls low level charging and discharging rates and reports voltage, current, and state of charge information to EMS	Yes: EMS can control charging and discharging schemes to optimize energy usage or improve power quality
Plug-in electric vehicle (PEV)	Motor vehicle that stores and uses electricity in rechargeable battery packs to propel or assist in propelling the vehicle	Depends: EMS may have network connection to vehicle, but some only interface with electric vehicle supply equipment
Electric vehicle supply equipment (EVSE)	Equipment that supplies electric energy for the recharging of PEVs	Yes: sends connection status and charging/discharging information to EMS

2.3 Communications

The implementation of a microgrid requires the integration of communications to enable the control architecture necessary for safety, security, reliability, sustainability, and cost-effectiveness. Control system networks implemented for microgrids will likely leverage the Internet protocol suite of communications protocols, including communications at the link, internet, transport, and application layers. The Internet protocol suite is commonly known as Transmission Control Protocol/Internet Protocol (TCP/IP); however, microgrid control system networks employ several different protocols to enable communication between the many types of power and cyber actors. Table 2.2 describes the purpose of communication at each layer in the protocol stack and presents the various protocols that may be found in a microgrid control system network. Additionally, security protocols, such as TLS/SSL, may be used at any layer to protect data sent between applications and hosts.

2.3.1 Link Layer

Link layer protocols support local network communication, allowing hosts to communicate without intervening routers. Control systems implemented for microgrids will likely leverage Ethernet networks primarily, but may include some serial communications. For example, communication between an HMI and its server will likely occur over Ethernet, but many power actors, such as generator controllers, may only be able to send data and receive

Table 2.2. Communication protocol stack.

Layer	Purpose	Protocols
Application	Process-to-process communication: allows applications on the same or different hosts to share data	DHCP, DNS, HTTP, NTP, SSH, XML-RPC; Control system-specific: DNP3, Modbus, LonTalk; proprietary protocols developed by vendors of micro-EMSs
Transport	Host-to-host communication: allows for different hosts to communicate on either the same network or on networks separated by routers	TCP, UDP
Internet	Internetwork communication: allows for host-to-host communication across network boundaries through intervening routers	IP (IPv4, IPv6), IPsec
Link	Local network communication: allows for host-to-host communication without intervening routers	Ethernet, serial

commands via a serial connection. The protocols employed at the link layer will be dependent on the hardware implementation of the microgrid.

2.3.2 Internet Layer

Internet layer communication protocols support internetworking; they allow for hosts to communicate across network boundaries through intervening routers. The Internet Protocol (IP) is the principal component of the internet layer, and as such, will be employed in a microgrid controls system. As an internet layer communication protocol, IP defines the format of data packets and a system for addressing hosts such that those packets can be sent from one host to another.

IP version 4 (IPv4) is the dominant protocol of the Internet, but its successor, IP version 6 (IPv6) is seeing increased use. IPv6 provides many features that can be useful for the creation of enclaves in a microgrid control system network. The prominent difference between the two IP versions is their respective host addressing systems: IPv4 uses 32-bit addresses while IPv6 uses 128-bit addresses. The larger network address space makes the allocation of addresses and network segmentation easier, but will likely have minimal impact in smaller installations. Additionally, multicasting, the transmission of a packet to multiple destinations in a single send operation, is part of the base specification in IPv6 and, in effect, replaces the traditional broadcast feature of IPv4. Multicasting can be employed to allow power actors in the microgrid control system network to efficiently communicate necessary data to all

concerned hosts within an enclave for the management of the microgrid. Finally, IPv6 hosts can use either stateless address autoconfiguration, stateful configuration via Dynamic Host Configuration Protocol (DHCP), or static configuration.

Employment of IPv6 in a microgrid control system network will require certain mitigations. If not all equipment in the network is IPv6-compatible, transition mechanisms will be required to enable IPv6-only hosts to reach IPv4 services and to allow isolated IPv6 hosts and network to reach each other over IPv4-only infrastructure. Transition mechanisms include dual-stack implementation (i.e., side-by-side implementation of both protocols) and tunneling (i.e., encapsulation of one protocol within another). Alternatively, protocol translators can be installed on the network. Additional information regarding the impacts of IPv6 on control systems can be found in [8].

2.3.3 Transport Layer

Transport layer protocols support host-to-host communication that is hardware independent. The two most common transport layer protocols are Transmission Control Protocol (TCP), which is connection-oriented, and User Datagram Protocol (UDP), which is considered connectionless. The sole purpose of these protocols is to create a basic data channel that can be used by an application for data exchange related to a specific task. Employment of either TCP or UDP within a microgrid control system network will be based primarily on the importance of speed versus reliability and the necessity for error detection.

2.3.4 Application Layer

Application layer protocols support process-to-process communication and rely on transport and internet layer protocols to establish and maintain the host-to-host connections between hosts running the processes. The microgrid control system network will include both supervisory control and data acquisition (SCADA) application protocols and other general-use application protocols. Many common application protocols, such as DHCP, Domain Name System (DNS), and Network Time Protocol (NTP), are used for network management and are found in typical information technology (IT) networks in addition to control system networks. The microgrid control system network will also include protocols specific to the included SCADA applications, such as Distributed Network Protocol (DNP3), Modbus, and Lontalk for control system operations; Extensible Markup Language for Remote Procedure Call (XML-RPC) and Hypertext Transfer Protocol (HTTP) for control system management; and proprietary protocols developed by vendors of micro-EMSs. For example, consider a control system front-end processor (FEP) application running on a server communicating with an IED using Modbus as the application layer protocol over TCP/IP as the transport and network layer protocols. The FEP is using Modbus to gather control system data from the IED over the IP network. It relies on the host server its running on to actually create the TCP connection to the IED in support of this activity. The application layer protocols are employed independent of protocols implemented at the lower layers.

2.3.5 Security Protocols

Historically, in both the information technology and industrial control system (ICS) fields, application layer protocols leveraging IP communications have relied on other application layer protocols or internet layer protocols to provide network security (such as authentication and encryption) rather than designing security into the protocol itself. Using Modbus again as an example, there is no authentication required for any request, whether it be a monitor or control request. If one has access to an IP network that a Modbus device resides on, packets can be sent to the device, and as long as they are well-formed Modbus packets, the device will react to the packets. The DNP3 protocol, which is commonly used in United States (US) electric power systems, has an option that some might consider a form of authentication wherein a DNP3 device can be programmed to only respond to requests coming from whitelisted IP addresses. However, this should not be considered a strong form of authentication since IP addresses are easily spoofed. A microgrid control system network will likely employ a separate security protocol, such as TLS/SSL, IPsec, SSH, or a custom secure protocol (Table 2.3).

Transport Layer Security/Secure Sockets Layer (TLS/SSL) is an optional cryptographic protocol implemented on top of the TCP transport layer protocol; it encapsulates and protects data sent using other application layer protocols. If implemented in a microgrid control system network, two applications establishing a connection have the option of starting a TLS/SSL connection prior to exchanging any data. The TLS/SSL handshake is comprised of exchanging security certificates, optionally verifying the certificates, and using the certificates to generate pre-shared keys to protect the data being sent between the applications. Because TLS/SSL must be started after a connection exists at the transport layer, it must be supported by and integrated into each application.

Internet Protocol Security (IPsec) is an optional specification of the base IPv6 protocol suite, and thus, provides security at the internet layer of the protocol stack. IPsec is a protocol suite for securing IP communications by authenticating and encrypting each packet of a communication session. One advantage of using IPsec instead of TLS/SSL is that applications do not have to support IPsec, making it a good candidate for use in legacy systems. Another advantage is that IPsec supports UDP and multicast traffic as well as TCP, while TLS/SSL only supports TCP traffic. However, a disadvantage in using IPsec is since the security is applied at the host kernel level, any application running on the host can use the IPsec tunnel to send and receive traffic, including malicious applications. Other disadvantages could include additional traffic latency, which is true for TLS/SSL or any other security protocol, and the effects of which are system- and application-dependent.

Yet another option for securing communications between control system applications is the secure shell (SSH) protocol. SSH is a cryptographic application layer protocol used for secure data exchange, remote shell services and command execution, and other secure network services. Although SSH is an application layer protocol, existing applications can take advantage of its secure communication capabilities without modification through the use of SSH's extensible port forwarding and secure tunneling features. The compilation, management, latency, and capability aspects of SSH and IPsec need to be compared when deciding

which is best suited for use in a microgrid control system network. For example, while SSH tunneling can support UDP traffic, it requires additional configuration and additional services to be running. The same is true for multicast traffic.

Table 2.3 compares the security protocol support available for different types of traffic. Other protocols for securing communications between hosts and applications exist, as does the option for building authentication and encryption capabilities directly into application protocols. Which approach to take and which protocols to use ultimately depends on the requirements of the microgrid control system network in question, the capabilities of the applications and devices in use, and the level of security necessary for the system under control.

Table 2.3. A comparison of security protocol support for different types of network traffic.

	TCP Unicast	**UDP Unicast**	**Multicast**
TLS/SSL	supported	not supported	not supported
IPsec	supported	supported	supported
SSH	supported	configurable	configurable
Custom Secure Protocol	supported	supported	supported

This page intentionally left blank.

Chapter 3

Motivation

The design of a microgrid control system needs to be more robust than that of a traditional industrial control system (ICS) for the following reasons:

- The microgrid is used in emergency situations and may be critical to continuity of operations of an installation.
- The microgrid must function during active attack by a capable adversary.

As such, the traditional design and implementation for an ICS may not be sufficient for a robust and secure microgrid.

Traditional ICS networks have a flat design where every actor is visible to every other actor; see Figure 5.1 for an example flat network. Although the traditional approach separates the control system network from the enterprise network and the Internet, there is little or no segmentation on the control system network itself [1, 2, 3]. In a flat network with little or no segmentation for defense-in-depth, any adversary that can access the network will have access to all actors within the network.

In the event that the local utility is not able to deliver power, the continued mission-critical operations of the installation will rely on the microgrid. Therefore, it is desirable to employ defense-in-depth to enhance the microgrid control system's operational security. The National Security Agency (NSA) describes *defense-in-depth* as a balanced focus on the primary elements of people, technology, and operations [12]. However, in this document, we focus solely on the technology aspect of defense-in-depth. In particular, our defense-in-depth strategy is based on the principles of—

- Defense in multiple places (e.g., networks and infrastructure, enclave boundaries, and computing environments)
- Layered defenses
- Defense strength appropriate to asset value and applicable threat
- Robust key management
- Intrusion detection, analysis, and response

Defense-in-depth implemented via network segmentation, authentication, and encryption will help to mitigate most, if not all, of the vulnerabilities identified in the following section.

3.1 Vulnerabilities

Most control communications in the microgrid will occur over an Internet Protocol (IP) network, and therefore, the control system network will have the same vulnerabilities that exist in traditional IP networks. These vulnerabilities are presented in Table 3.1. The microgrid control system may also have vulnerabilities that are more specific to ICSs. These vulnerabilities are presented in Table 3.2. In general, one or more of these vulnerabilities might allow an attacker to compromise the confidentiality, integrity, or availability of the microgrid.

Table 3.1: Common vulnerabilities found in IP networks.

Vulnerability Category	**Description**
Denial of service (DoS)	The normal use or management of networks or network devices is prevented or prohibited. For example, service can be denied using multiple client machines to overrun a server with requests so that the server is unable to respond to any of the requests in time.
Eavesdropping	Network communications are passively monitored for data, including authentication credentials. For example, an adversary uses monitoring software and local IP network access to record the exchange of data between a client and server, including the client's username and password that are sent in plain text.
Man-in-the-middle (MITM)	Network communications between two legitimate parties are actively intercepted. An adversary can thereby obtain authentication credentials and data and then masquerade as a legitimate party. For example, an adversary uses software to make a client information system think the adversary's information system is the legitimate server and vice-versa. The adversary is then able to monitor, record, and modify all data exchanged between the client and server.
Masquerading	An authorized user is impersonated, allowing an adversary to gain certain unauthorized privileges. For example, an adversary is able to steal the username and password for a legitimate user. The adversary uses these credentials to gain access to the information system.
Message modification	A legitimate message is altered by deleting, adding to, changing, or reordering it. For example, an adversary uses software to change the status values reported in network messages.
Message replay	Network communications are passively monitored and retransmitted at a later time. For example, an adversary records a message that disables monitoring equipment and sends a copy of the same message whenever he wishes to disable monitoring.

Continued on next page.

Table 3.1 – continued from previous page.

Vulnerability Category	Description
Traffic analysis	Network communications are passively monitored in order to identify communication patterns and participants. For example, an adversary records traffic for several days and uses software to identify the times of day that an operator is not monitoring the network.
Unauthorized access	Logical or physical access to a network, system, application, data, or other resource is achieved without explicit permission. For example, an adversary uses a misconfigured server as an access point (that doesn't require legitimate credentials) to the rest of the information system.

Table 3.2: Vulnerabilities found in ICS networks.[3]

Vulnerability Category	Description
Attacks on field devices	Security features are uncommon in field devices (due to limited memory and processing resources), so those devices are more susceptible to attack by an adversary. For example, portions of some field devices' memory may be writable by any device with network access. An adversary with network access could write bad values to a device's memory and cause it to crash or malfunction.
Backdoor or malicious software installed on command and control network	An operator installs malicious software, either unknowingly or with intent, on the ICS's command and control network. This software may provide an adversary with concealed access to actors in the control system network. For example, an operator might install software on an information system on the ICS network that allows him to gain remote access from home. This software might have a hardcoded username and password that can be used by an adversary to gain access to the ICS from the Internet.
Database attacks	ICSs may rely on the continuity of databases for proper function or logging of the system. Attacks against the databases that reflect the state or history of the system may impact the system security or prevent the collection of artifacts. For example, an adversary with access to a database might update device values that are normally only changed via a human-machine interface (HMI). The new values may be written to the device, but perhaps not reflected in the HMI.

Continued on next page.

[3]The vulnerabilities in this table were collected from ICS guidelines and industry best practices (e.g.,[1, 3]).

Table 3.2 – continued from previous page.

Vulnerability Category	Description
Devices with few or no security features	ICS devices are not typically designed to have security features. These devices might not have the ability to authenticate the sender of messages, encrypt network traffic, or other simple security mechanisms. For example, an adversary with a presence on the ICS network might be able to send control messages that disable ICS devices. The messages would be executed because the device has no way of checking the authenticity or validity of the messages.
Improper configuration of actors	Actors in an ICS network are not configured to bolster security. These actors might have default configurations and passwords or may be misconfigured; both conditions have a negative impact on the system's security. For example, actors that are capable of performing authentication, but do not have it enabled, and actors that use default or hard-coded credentials may negatively impact security.
Improper cyber security procedures or training for internal and external personnel	Personnel with access to the ICS are not trained in security practices and policy. The result can be the unintentional or intentional degradation of ICS security. For example, personnel may disable the firewall on an ICS information system after installing new software requiring the use of blocked ports. Although this action may allow the new software to function properly, it also negatively impacts the security profile of the information system.
Improper or no network perimeter definition	The perimeter of the ICS is not strictly defined or does not exist. Systems that are used for ICS command and control are not completely separated from the enterprise network that provides access to email, the Internet, or other services. For example, an operator on an ICS network might open a fraudulent email with a malicious file attachment. The malicious code could exploit a vulnerability on an ICS information system, giving an adversary access to the ICS from the Internet.
Improper or nonexistent patching of software and firmware	Typically, the primary focus of ICS design is system availability. Anything that might impact system availability (e.g., patching) is viewed as a risk, even if it offers security as a trade-off. For example, a critical information system on the ICS network may not have been updated since it was installed, because the ICS software vendor will void any warranty provided to the asset owner if patches are installed without the vendor's approval.
Insecure coding techniques	The software and firmware used throughout ICSs have historically suffered from insecure coding techniques. Improper authentication, access control, and error checking can negatively impact system security. For example, an adversary may easily bypass authentication that uses device serial numbers or short (16-bit) authentication keys.

Continued on next page.

Table 3.2 – continued from previous page.

Vulnerability Category	Description
Lack of ICS-specific mitigation technologies and security tools	There are not many mitigation technologies for vulnerabilities in ICSs. Additionally, ICSs do not have many security monitoring tools, such as intrusion detection systems (IDSs) for IP networks. For example, there may not be a monitoring tool available for detecting if new configuration values are written to a field device's memory from the network.
Lack of redundancy for critical actors	It is not always practical or possible to have redundant actors for all critical ICS actors. This might result in a single point of failure for the ICS. For example, it may not be practical from a financial or maintenance perspective to have redundant relays for every protection scheme required in a power system. As such, the failure of a relay could lead to equipment being damaged.
Unauthorized personnel have access to ICS actors	The design of the ICS or the policy of the operator may give unauthorized personnel access to at least part of the ICS. For example, policy may allow vendor staff unescorted access into a power generation facility for maintenance or repair. If their access is not monitored or restricted, the visitors may have unfettered access to all actors on the ICS network.
Vulnerabilities in common protocols	Many of the protocols used for ICS communications are long-established. These protocols tend to be vulnerable to well-known attacks, particularly if unpatched or out-of-date. For example, an adversary with physical access to the bus for a Profibus virtual token ring might be able to perform MITM or DoS attacks against the token ring. Profibus, like many ICS communication protocols, has no built in mechanism to mitigate this vulnerability.

The vulnerabilities presented above can be coupled with possible incident scenarios, like those described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82, *Guide to Industrial Control Systems (ICS) Security* [3], in an effort to better understand how each one has potential to impact a microgrid control system. We pair a small number of notional incident scenarios with the above vulnerabilities in Table 3.3. While the incident scenarios described in Table 3.3 are applicable to ICSs in general, the cyber security threat modeling effort, described in Section 3.2, attempted to identify scenarios specific to Department of Defense (DOD) microgrids.

Table 3.3: Notional incident scenarios for ICS networks.

Vulnerability Category	**Incident Scenario**
DoS, improper or no network perimeter definition	ICS operation is disrupted by delaying or blocking the flow of information through corporate or control networks, thereby denying availability of the networks to operators or causing information transfer bottlenecks or denial of service by information technology (IT)-resident services (such as domain name resolution).
Attacks on field devices, devices with few or no security features, improper or no network perimeter definition, masquerading	Unauthorized changes made to programmed instructions in programmable logic controllers (PLCs), remote terminal units (RTUs), or supervisory control and data acquisition (SCADA) controllers, alarm thresholds changed, or unauthorized commands issued to control equipment could potentially result in damage to equipment, premature shutdown of processes, causing an environmental incident or even disabling control equipment.
Database attacks, improper or no network perimeter definition, MITM, message modification, message replay	False information is sent to ICS operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators.
Improper configuration of actors, insecure coding techniques, lack of ICS-specific mitigation technologies and security tools, masquerading	ICS software or configuration settings are modified, producing unpredictable results.
Backdoor or malicious software installed on ICS command and control network, DoS, improper or no network perimeter definition, MITM, masquerading, message modification	Operation of safety systems is delayed or denied through interference with command and control communications.
Backdoor or malicious software installed on ICS command and control network, devices with few or no security features, improper cyber security procedures or training, improper or no network perimeter definition, improper or nonexistent patching, insecure coding techniques, lack of ICS-specific mitigation technologies and security tools, unauthorized access, vulnerabilities in common protocols	Malicious software (e.g., virus, worm, Trojan horse) is introduced into the ICS network.

3.2 Threat Model

The current performance of threat modeling is seen as an industry best practice, where trusted vendors develop and apply threat and risk models in support of their product designs [13]. However, it is difficult to identify a well-accepted standard for the process of modeling threats; different entities performing systems security engineering roles use different conceptual descriptions of threat modeling. What is more, it is not uncommon for system stakeholders and security analysts to sometimes equate "threats" with "adversaries." This is not necessarily wrong, but as with all terms used in systems security discussions, it is necessary to know how people define a term when they use it. The term *threat* can be defined in many different ways. Here, we use it to describe threat *actors* or those we would also refer to as goal-directed *adversaries*.

The Department of Homeland Security (DHS), in its publication, *Architecture and Design Considerations for Secure Software* [14], takes an approach similar to one used by Microsoft, where the system application is decomposed to determine how it works; its assets, functionality, and connectivity are inventoried; and then system vulnerabilities and threats are explored from the point of view of would-be adversaries. In a document prepared for NIST, *The ICT SCRM Community Framework Development Project: Final Report* [13], the Supply Chain Management Center at the University of Maryland describes threat modeling in the following way:

> *Threat modeling is a technique that identifies a set of potential attacks on a particular product or system and describes how those attacks might be perpetrated and the best methods of preventing potential attacks. Threat models are used as input to the creation of test plans and cases.*

Accordingly, there are many different approaches security analysts and developers can take to effectively model threats. Two of these include—

- Emphasizing the system architecture, where potential attacks and security issues are identified for each part of the architecture (including its sub-systems and components) using an adversary-based perspective, and

- Focusing on threat actors' capabilities and objectives for the target system, along with the related consequences of concern that stakeholders wish to avoid.

Our approach integrates an architecturally driven model with a generic adversary profile, bolstered by discussion of real world control system cyber security issues and incidents. Our intent is to produce a more complete threat model. The threat model is intended to support understanding of threats to DOD microgrids based on the cyber security reference architecture design. Our threat model is not site- or installation-specific.

The threat model addresses only threats that are typically associated with failures induced by malicious threat actors. The model includes threat discussion related to vulnerabilities in information and communication technologies, including software and hardware on

the control system network, threat conditions that enable malevolent actors to compromise systems, and characteristics of the class of threat actors of concern. The threat model does not currently include threats relating to purely physical attacks that would damage or destroy cyber or electrical system components comprising the microgrid or its interconnection to other systems. The threat model does not represent a comprehensive security threat assessment; each installation that acquires a microgrid system will select a system integrator to procure hardware, software, and electrical system components to build a site-specific system to serve the base. Because different sites have different missions, operational characteristics, equipment, and network architectures, the threat scenarios (along with associated impacts and consequences) applicable to each will be different.

The threat model for this cyber security reference architecture incorporates the following resources:

- Threats related to data-in-transit on IP networks, abstracted from wireless-specific threats as documented in NIST SP 800-97, *Establishing Wireless Robust Security Networks* [15] (as presented in Table 3.1)
- Common vulnerabilities in ICS networks (as presented in Table 3.2)
- General incident scenarios drawn from NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security* [3] (as presented in Table 3.3)
- Additional threats specific to DOD microgrids as identified by the design team
- A generic threat matrix, given in Figure 3.1, which is used by Sandia National Laboratories (SNL)'s Information Design Assurance Red Team (IDART) and documented in SAND2007-5791, *Categorizing Threat: Building and Using a Generic Threat Matrix* [16]

We assert that stakeholders of DOD microgrid systems should be prepared to confront a range of adversaries with skills from low to high. It is commonly accepted by leadership that threats originating from foreign nation states with capabilities at Threat Level 1 (according to the generic threat matrix in Figure 3.1) have been targeting United States (US) systems for decades. A Threat Level 1 adversary will have no problem mounting a supply-chain attack and embedding malicious components in an RTU or energy management system (EMS), which bypasses any protection offered by authentication and encryption of network traffic or network segmentation. If the system is designed, implemented, operated, and maintained with security designed to thwart or impede Threat Level 1 adversary, then it is reasonable to believe that attackers of lesser level will be more seriously challenged to interrupt or deny mission by tampering with or taking down the microgrid. Declaring that the system should be designed to operate successfully in a hostile environment to meet Threat Level 1 adversaries means that extremely robust security must be properly incorporated throughout the system life cycle.

Threats across the spectrum continue to develop and hone skills and knowledge needed to target critical infrastructure control networks. Because the strength of defense should

THREAT LEVEL		THREAT PROFILE						
		Commitment			Resources			
						Knowledge		
		Intensity	Stealth	Time	Technical personnel	Cyber	Kinetic	Access
High	1	H	H	Years to decades	Hundreds	H	H	H
	2	H	H	Years to decades	Tens of tens	M	H	M
	3	H	H	Months to years	Tens of tens	H	M	M
Mid	4	M	H	Weeks to months	Tens	H	M	M
	5	H	M	Weeks to months	Tens	M	M	M
	6	M	M	Weeks to months	Ones	M	M	L
Low	7	M	M	Months to years	Tens	L	L	L
	8	L	L	Days to weeks	Ones	L	L	L

Figure 3.1. Generic threat matrix. Reproduced from [16].

be proportional to the value of the asset to be protected and the applicable threat, each microgrid owner will need to conduct a threat model analysis specific to that microgrid installation. For a comprehensive understanding of the generic threat matrix and its use, the reader is encouraged to review the report, *Categorizing Threat: Building and Using a Generic Threat Matrix* [16].

3.3 Information Assurance Compliance

The implementation of a microgrid requires the integration of communications to enable the control architecture necessary for safety, security, reliability, sustainability, and cost effectiveness. The added communications in this context introduce additional cyber security vulnerabilities (as described in Section 3.1) and require adherence to DOD information assurance (IA) guidelines. According to DOD Directive 8500.01E, *Information Assurance(IA)*,

> *All DOD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DOD information system; and cost effectiveness.* [17]

The DOD certifies and accredits information systems through an enterprise process known as the DOD Information Assurance Certification and Accreditation Process (DIACAP) for identifying, implementing, and managing IA capabilities and services, expressed as IA controls [5]. DIACAP will eventually be updated with DOD's Risk Management Framework, which will include a clearer mapping between DOD IA controls and NIST SP 800-53 controls [6]. These controls help to provide an appropriate level of security for information assets essential to the operation of the microgrid. Information system integrators should take advantage of available certification and accreditation (C&A) tools, such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)[4] and DHS's Cyber Security Evaluation Tool (CSET)[5], to verify compliance with applicable IA controls. The microgrid cyber security reference architecture should, if utilized, help meet a majority of the technical IA requirements automatically.

There are four basic steps in assigning IA controls to an information system: (1) determine the type of information system; (2) determine the mission assurance category (MAC) and confidentiality level for the information system; (3) identify the baseline IA controls; and (4) augment the baseline IA controls.

3.3.1 Information System Type

The microgrid is considered a *special purpose system*, which is defined as a system or platform that employs computer resources (i.e., hardware, firmware, and optionally software) that are physically embedded in, dedicated to, or necessary in real time for the performance of the system's mission [4]. These computer resources are referred to as *platform information technology (IT)*. Platform IT is dedicated to the information processing assigned to it by its hosting special purpose system. Examples of special purpose systems include weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems, such as water and electric [4]. Because the microgrid falls under the definition of a special purpose system, the availability, integrity, confidentiality, authentication, and non-repudiation requirements of the data the platform IT processes in direct support of the microgrid's intended purpose must be inherently addressed in the system design and operation.

3.3.2 Mission Assurance Category

As applied to DOD information systems, the *mission assurance category (MAC)* reflects the importance of information relative to the achievement of DOD goals and objectives, particularly the warfighters' combat mission. MACs are primarily used to determine the requirements for availability and integrity. As described in Table 3.4, the DOD has three defined MACs. The MAC of a microgrid control system will be dependent on the specific installation.

[4] `http://iase.disa.mil/stigs/`

[5] `http://www.us-cert.gov/control_systems/satool.html`

Table 3.4. Mission assurance categories (MACs).

MAC	Definition	Integrity	Availability
I	Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. Consequences of loss of integrity or availability are unacceptable and could include the immediate and sustained loss of mission effectiveness.	High	High
II	Systems handling information that is important to the support of deployed and contingency forces. Consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time.	High	Medium
III	Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. Consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness.	Basic	Basic

3.3.3 Confidentiality Level

The *confidentiality level* applied to DOD information systems is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, internet, wireless). The DOD has defined three confidentiality levels: classified, sensitive, and public. A microgrid control system is typically considered to be sensitive; however, the system's confidentiality level is dependent on the specific installation.

3.3.4 Information Assurance Controls

An *information assurance (IA) control* is an objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities [4]. Specific management, personnel, operational, and technical controls are applied to each DOD information system to achieve an appropriate level of integrity, availability, and confidentiality. Included are IA controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations (e.g., penetration testing). IA controls provide a common management language for establishing IA needs; interacting with system security engineers to ensure a purposeful design to meet those needs consistent with DOD and DOD Component-level guidance; testing

and validating the implemented IA solutions; managing changes to the validated baseline; negotiating interconnections; and reporting IA readiness.

In order to receive an Authority to Operate (ATO), all DOD information systems must fulfill the minimum set of IA controls delineated in DOD Instruction (DODI) 8500.2, *Information Assurance (IA) Implementation* [4], based on the system's MAC and confidentiality level. The baseline IA controls must be explicitly addressed as part of an information system security engineering process. They can be augmented with additional IA controls to address special security needs or unique requirements of the information system to which they apply.

3.4 Design Criteria

As mentioned previously, the design of the microgrid must be secure and robust. Based on the microgrid concept of operations and the vulnerabilities described above, the following criteria guide our design approach. A secure microgrid control system network must be—

- **Simplistic**: While network security is important, system operation still maintains a higher priority in control systems. Keeping the network infrastructure as simple as possible supports necessary change, monitoring, and administration by personnel who may be operators first and network engineers second. By segmenting the network based on system functionality, the network design becomes structured, manageable, and function-aligned. Such segmentation supports the planned operation of a microgrid by supporting the operational functions required to transition between the three modes of operation at the network level in a way that directly aligns with the operational functions themselves.

- **Segmented**: Segmenting network traffic and interactions that are similar in nature enables improved network capacity, stronger security enforcement, detailed logging, and more accurate monitoring capabilities. This supports improved security by facilitating mitigation strategies directly aimed at reducing the vulnerabilities identified for control system networks. Such strategies include firewalling, authentication, encryption, intrusion detection, situational awareness, and forensics.

- **Monitored**: The system is designed and instrumented for monitoring with minimal or no impact on operations. By focusing monitoring capabilities on specific network segments, false positives can be decreased as the list of data expected in each network segment becomes smaller.

- **Independent**: Segmenting actors that support particular system functions not only helps to better define and improve network security, but also enables the independent operation of functions in the event that actors in a different enclave are compromised. By design, independent operation provides an increased level of resiliency to the microgrid operations that can be increased even further through the use of distributed management capabilities.

- **Reconfigurable**: During normal, day-to-day operations, the microgrid will not be in operation. Only during emergency situations will it be activated, and during this time, the microgrid's cyber security should be elevated to ensure operations are not interrupted. Reconfiguration of certain aspects of the network and cyber infrastructure will support detection of anomalous events that occur during microgrid operation, whether they are inadvertent or adversarial, providing yet another means of reducing the vulnerabilities present during emergency operations.

While the above criteria guide our design approach described in Chapter 4, they should also be considered when leveraging the reference architecture to develop a site-specific microgrid control system network given that many design considerations must be based on site-specific requirements and capabilities. For example, consider segmentation: there are many options for deciding how to segment a microgrid control system into enclaves, each having positive and negative attributes that will vary from site-to-site. Additionally, depending on the entity responsible for deploying and managing the microgrid control system network, the level of expertise available may dictate the extent to which the network is segmented and communications are limited for simplicity.

This page intentionally left blank.

Chapter 4

Design Approach

Best practices for securing industrial control systems (ICSs) leverage network segmentation; for example, see [1], [2], and [3]. In most cases, however, network segmentation is focused on separation of the control system network from other less-trusted networks, such as the enterprise network and the Internet. The concept of network segmentation within the control system network itself is addressed to a minimal degree in a recommended practices document [1] published by the Department of Homeland Security (DHS) Control System Security Program (CSSP), but the additional complexities of configuring and managing such a network in the data and control zones[6] often result in this level of defense-in-depth being dismissed. In geographically dispersed control systems and field devices, physical segmentation often inherently exists within ICS command and control networks due to the employment of third-party providers for communication services. This segmentation is not leveraged to enhance security, however, as neither physical nor logical segmentation is currently used as a basis for providing additional defense-in-depth within modern ICS networks.

The Sandia National Laboratories (SNL) approach to designing a secure microgrid control system network leverages segmentation to reinforce defense-in-depth practices. The microgrid control system network is segmented into enclaves defined by system functions, physical locations, and security concerns. Enclaves are then grouped together into functional domains that allow actors to collaborate in operational system functions that crosscut enclaves. Data exchange worksheets describe communication between actors within enclaves and functional domains.

4.1 Enclaves

An *enclave* is a collection of computing environments that is connected by one or more internal networks and is under the control of a single authority and security policy [4]. This concept of enclaves (already leveraged by Department of Defense (DOD) information systems in operation today [4, 5]) reduces the complexity of configuring and managing a segmented control system network. Enclaves support specific access and monitoring policies and enable more effective use of technological and administrative capabilities to enforce such policies. An enclave-based approach to segmentation is applicable to control system networks as well, supporting access control and monitoring of specific control functions at a finer granularity.

[6]The data and control zones are defined by the Purdue Model for Control Hierarchy (described in [1]). The manufacturing/data zone is the area of connectivity where a vast majority of monitoring and control takes place. The control/cell zone is the area of connectivity to devices like programmable logic controllers (PLCs), human-machine interfaces (HMIs), and basic input/output devices, such as actuators and sensors.

Within the microgrid control system network, enclaves are defined based on a suite of actors that participate in a particular system function, share geographical location, have similar security concerns (e.g., information assurance (IA) controls), or share any combination of these features. An enclave based on a particular system function could include actors at multiple physical locations; for example, intelligent electronic devices (IEDs) that are geographically dispersed may need to communicate their states with each other or an engineering console. In addition, actors at a particular physical location may be segregated into separate enclaves based on whether they contribute to operations-related functions or cyber security-related functions.

This network segmentation process is demonstrated in Figure 4.1 where enclaves (segmented by system function and physical location) participate in functional domains defined only by system function, rather than by physical location. For example, consider that all of the actors at Site II are grouped into a single enclave (Enclave 3) based on physical location, whereas the actors at Site I are segregated into two enclaves (Enclave 1 and Enclave 2), which may be based on physical location, system function, security concerns, or a combination of features.

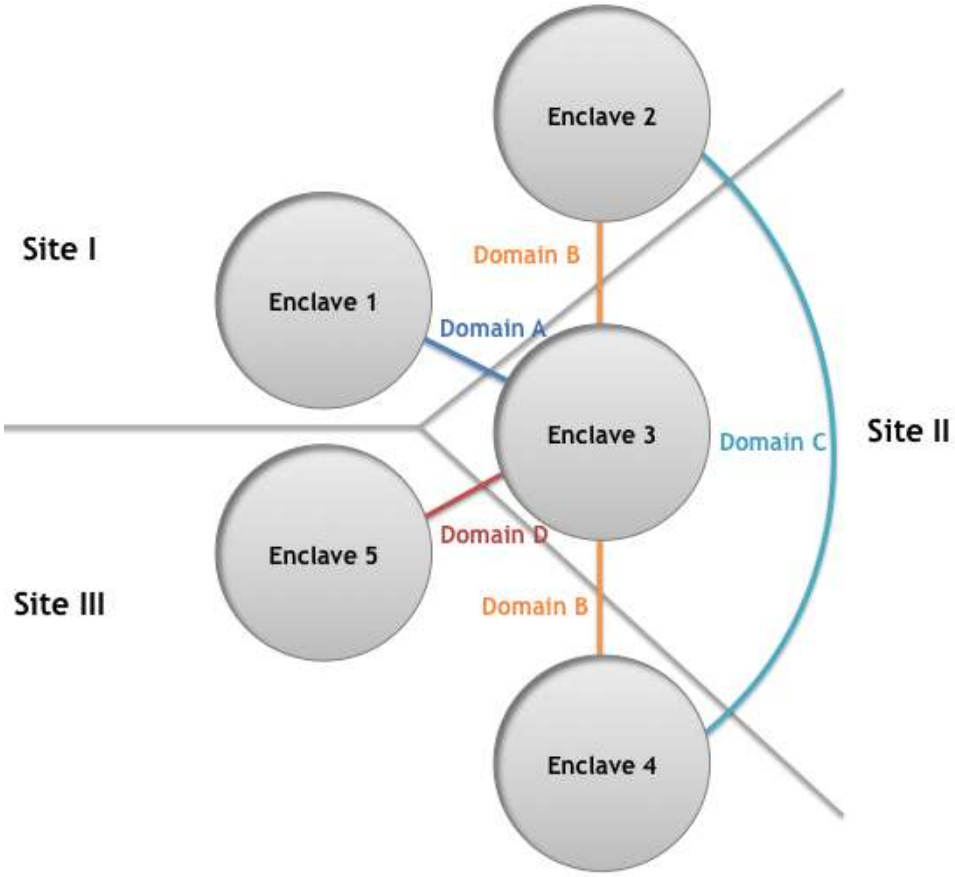

Figure 4.1. Example segmentation of network into enclaves and functional domains.

4.2 Functional Domains

Although some enclaves are defined based on actors that participate in a particular system function, some actors necessarily crosscut enclaves that are defined by physical location or security concerns. For example, the energy management system (EMS) interacts with actors at the points of common coupling (PCCs), which could belong to enclaves defined by physical locations. Additionally, some actors participate in multiple system functions. With the granular segmentation of the actors into enclaves, communication (or data exchange) between actors in separate enclaves may be necessary to accomplish system-level functional operations. A collection of interacting enclaves is considered a *functional domain*.

This approach of using a domain to control interactions between enclaves is similar to an approach championed by James Rome at Oak Ridge National Laboratory (ORNL) [18]. The ORNL approach uses enclaves to protect and segregate computing environments based on the type of information and computing requirements of the resources located in the enclave. The need to communicate among enclaves drives the need to create a higher-level arbitration mechanism. To satisfy this need, collaborative domains are used to set access policies and allow communication across enclave boundaries. The ORNL approach uses collaborative domains to handle enclave communication across geographically separated locations with differing security policies. Our functional domain approach builds on the collaborative domain mechanism, and each functional domain contains a group of enclaves that accomplish a system function.

Functional domains highlight areas of common communication that define system operations. For instance, in Figure 4.1, Enclave 3, which is defined by physical location, participates in three functional domains: A, B, and D. Therefore, it seems obvious that the actors in Enclave 3 are necessary for a variety of system functions; for example, the enclave may include the EMS required for both operational and maintenance system functions. On the other hand, Domain C demonstrates an atypical functional domain for this microgrid control system network: one that does not require the participation of any actors (such as the EMS) in Enclave 3. This functional domain could be devoted to the communication pipeline between redundant devices at geographically dispersed locations and would only be required for communications that necessarily do not involve devices in Enclave 3, possibly due to security concerns.

4.2.1 High-Level System Functions

For the purposes of this reference architecture, microgrid control system networks consist of the following four high-level system functions:

- **Automated grid management and control (AGMC) operations**: interactions between the EMS, aggregators, inverters, relays, and nearly every other power actor in the microgrid control system network (e.g., remote terminal units (RTUs) and IEDs)
- **AGMC maintenance**: interactions between the engineering consoles and all power actors in the microgrid control system network

- **Cyber security situational awareness (CSSA)**: interactions between the correlation engine, AGMC actors, and nearly every cyber actor in the microgrid control system network (e.g., firewalls, routers, and switches)

- **Cyber security configuration management (CSCM)**: interactions between management systems (e.g., the intrusion detection system (IDS) or the authentication server) and the cyber actors in the microgrid control system network

These higher level system functions can be subdivided into smaller functions to facilitate network segmentation. If necessary, more granularity can be achieved through even further division of the functions; however, for most implementations, the AGMC operations and AGMC maintenance functions can be sufficiently subdivided into the following:

- **Monitoring and control**: supervising, coordinating, and optimizing microgrid operations

- **Generation**: production and regulation of electricity by converting one form of energy (e.g., chemical, solar, mechanical, thermal, etc.) into electrical energy

- **System protection**: protection of the electrical system from electrical faults by isolating faults from the rest of the system

- **Electrical distribution**: provision of power lines, transformers, capacitor banks, etc. that allow power to be transported from generation to load

- **Energy consumption (load)**: consumption of electrical energy provided by the microgrid

- **Energy storage**: storage of electrical energy for use at later times

Similarly, the CSSA and CSCM functions can be subdivided into the following:

- **Networking**: route and transmit information to facilitate information sharing and delivery of control signals

- **Authentication and encryption**: verify the identity of microgrid devices approved for operation in the microgrid and encode data so that unauthorized parties are unable to read or alter it

- **Security devices** (e.g., IDS, firewall, bump-in-the-wire (BITW), etc.): provision security services that provide a higher level of security, such as deep packet inspection, encryption, port blocking, etc.

Each high-level system function is decomposed into smaller functional interactions. For each functional interaction, the actors contributing to the system function and the attributes that describe data exchange between those actors are identified as described in Section 4.3.

4.2.2 Access Restrictions

Functional domains support reliable and secure data exchange necessary to accomplish system function by establishing the necessary level of access for participating enclaves and arbitrating inter-enclave communication (as defined by applicable data exchange worksheets). As participants in functional domains, enclaves are responsible for—

- meeting the domain access restrictions
- communicating (i.e., exchanging data) with other enclaves in the domain
- participating to the degree necessary to accomplish the system function

Enclave and functional domain access controls restrict communication between actors and enclaves. Enclaves can participate in more than one functional domain but must adhere to access levels prescribed by each particular domain. For example, a functional domain can restrict access and control among its enclaves, allowing participating enclaves to communicate only with other enclaves within the functional domain. Additionally, an enclave can have stricter access controls than required by the functional domain, but only if the operational necessities of the domain can still be met.

4.3 Data Exchange

Data exchange defines communication between actors within enclaves and functional domains. Within an enclave, data exchange attributes describe—

- latency, bandwidth, and quality of service (QoS) for intra-enclave communications
- types of network traffic to expect
- necessary level of enclave cyber security

Within a functional domain, data exchange worksheets help to identify—

- which enclaves need to communicate
- types of network traffic that will be communicated between enclaves
- latency, bandwidth, and QoS for inter-enclave communications
- cyber security concerns for inter-enclave communications

A template data exchange worksheet (Table 4.1) has been developed leveraging previous work completed as part of NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security* [2], and Institute of Electrical and Electronics Engineers (IEEE) Standard 2030, *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications,*

and Loads [19]. As presented in Table 4.1, the data exchange worksheet assists in identifying the operational necessities for data exchange between actors and cyber security needs for information assurance. In the template, *system function* is replaced with the high-level system function (described in Section 4.2.1) being analyzed. The source and destination endpoints are the *control system actors* participating in the data exchange. Additional columns are added for multiple exchange types applying to each source-destination pair. For each pair and exchange type, the attributes describing data exchange and necessary cyber security are identified and recorded. Each field of the worksheet has specific values that can be used to describe the data exchange attributes. Table 4.2 presents each attribute, its definition, and example values used to complete that field. See Section 5.2 for data exchange worksheets used in an example reference implementation.

Table 4.1. Template for data exchange worksheet.

Data Exchange Attributes for *System Function*	
Source	*Control system actor*
Destination	*Control system actor*
Exchange	
Type	
Interval	
Method	
Priority	
Latency Tolerance	
Data	
Type	
Accuracy	
Volume	
Reliability	
Information Assurance	
Confidentiality	
Integrity	
Availability	

Table 4.2. Data exchange attributes and example values.

Attribute	Description	Example Values
Exchange		
Type	type of data exchange to occur	monitor, control, report, write
Interval	how often data exchange occurs	unit of time (e.g., milliseconds or seconds)
Method	how data will be exchanged	unicast, multicast, broadcast
Priority	relative importance of exchanging the data	high, medium, low
Latency Tolerance	tolerance to delayed access to control processes and delayed exchange of data	high (i.e., normal operation is maintained even when receiving significantly delayed data), medium, low
Data		
Type	type of data to be exchanged	voltage, setpoint, status
Accuracy	necessary precision and/or timeliness of data	number of significant digits, unit of time (e.g., milliseconds)
Volume	amount of data to transferred per exchange	unit of data size (e.g., bytes or kilobytes)
Reliability	necessity of access to control processes and data	critical, important, informative
Information Assurance		
Confidentiality	importance of preserving authorized restrictions to control processes and information access (based on risk to system operations and/or system security)	high, medium, low
Integrity	importance of preventing unauthorized changes to control processes or data, to include the authenticity of data (based on reliability with respect to operations)	high, medium, low
Availability	importance of timely and reliable access to control processes and data (based on priority and latency tolerance with respect to operations)	high, medium, low

4.4 Cyber Actors

The proper function of the microgrid depends on the security features offered by certain cyber actors in the microgrid control system network. In Table 4.3, these cyber actors are listed along with the security features each should offer. These features are necessary to help mitigate security vulnerabilities within the network. The mitigated vulnerabilities shown here are drawn from common vulnerabilities found in Internet Protocol (IP) networks (Table 3.1) and also from ICS-specific vulnerabilities (Table 3.2).

Table 4.3: Cyber actors in the microgrid control system network.

Actor	Necessary Security Features	Vulnerabilities Mitigated
Networking		
Switch	Traffic logging, configuration logging, layer-2 and maintenance access control, filtering	Database attacks, devices with few or no security features, eavesdropping, improper or no network perimeter definition, MITM, masquerading, traffic analysis, unauthorized access
Router	Port blocking, traffic logging, configuration logging, access control, filtering	DoS, improper or no network perimeter definition, traffic analysis, unauthorized access
Authentication and Encryption		
Bump-in-the-wire (BITW) security device	Authentication and encryption of IP packets, mutual authentication, cryptographic key negotiation, message integrity, enhanced logging	Attacks on field devices, backdoor or malicious software installed, database attacks, denial of service, devices with few or no security features, eavesdropping, MITM, message modification, message replay, traffic analysis, unauthorized access
Authentication server	Authentication, logging, access control	Attacks on field devices, database attacks, devices with few or no security features, eavesdropping, MITM, masquerading, message modification, unauthorized access
Key management server	Key generation, exchange, storage, use, replacement, logging, access control	Database attacks, devices with few or no security features, MITM, masquerading, message replay, traffic analysis, unauthorized access

Continued on next page.

Table 4.3 – continued from previous page.

Actor	Necessary Security Features	Vulnerabilities Mitigated
Security Devices		
Firewall	Port blocking, traffic logging, configuration logging, access control, filtering	Attacks on field devices, DoS, improper or no network perimeter definition, message replay, traffic analysis, unauthorized access
Intrusion detection system (IDS)	Detection of malicious activities or policy violations, reporting, deep packet inspection, logging	Attacks on field devices, backdoor or malicious software installed, database attacks, devices with few or no security features, eavesdropping, message modification, message replay, unauthorized access
Intrusion prevention system (IPS)	Detection and prevention of malicious activities or policy violations, reporting, deep packet inspection, logging	Attacks on field devices, backdoor or malicious software installed, database attacks, devices with few or no security features, eavesdropping, message modification, message replay, unauthorized access

Interactions between cyber actors and power actors will likely occur in a microgrid control system network. The bulk of these interactions will manifest themselves during authentication and routing of control system traffic. For example, depending on the authentication scheme implemented, a power actor, such as a RTU or an EMS, may need to communicate with a central authentication server to validate itself as a trusted device within the control system network. Additionally, a protection relay may need to communicate with a BITW security device that provides Internet Protocol Security (IPsec) services. As such, these interactions must also be regulated using functional domains and enclaves to promote a more secure operating environment.

4.5 Performance Benefits and Vulnerability Mitigation

SNL's approach to designing a secure microgrid control system network leverages segmentation to reinforce defense-in-depth practices, offering the following performance benefits and vulnerability mitigation:

- Each enclave operates under a single authority and security policy and provides a trusted environment for actors that need to communicate. Actors who wish to join a particular enclave must meet or exceed the level of security for the enclave in order to become part of the enclave. This ensures that all actors of the enclave are secured at the same rigor and level as the actors with which they are communicating.

- Enclave inter-communication is restricted and managed by functional domains. The functional domains govern the policies that enable actors in one enclave to communicate with actors in another enclave based on data exchange attributes.

- Enclave boundaries provide good locations to monitor intrusion detection, unauthorized access attempts, and other logged events.

- Cleaving the logical network based on functional necessities, physical locations, and/or security concerns ensures a higher level of trust on each network segment.

- Isolation of enclaves minimizes both malicious opportunities and accidental damage affected by a trusted, valid party. Providing communication barriers between enclaves and implementing enclave-specific security policies limits access by malicious actors within enclaves. This isolation also has the side effect of compartmentalizing valid actor access to only the enclave- or functional domain-level needed.

- Network performance may be improved based on necessary latency, bandwidth, and QoS.

- Traffic monitoring can be implemented within enclaves to perform deep packet inspection and detect any anomalous message codes. Since each data exchange has very specific attributes, the message code on the microgrid control system messages should be known for each actor interaction. The reduced traffic per enclave (due to fewer actors on the network segment) enables more accurate parsing and inspection of the traffic being monitored.

The use of enclaves to segment the microgrid control system network mitigates many of the vulnerabilities presented in Section 3.1. Because segments of the control system network are now isolated, certain security risks, such as masquerading, message replay attacks, unauthorized access, eavesdropping, and network perimeter vulnerabilities, are at least partially mitigated. For example, if an adversary gains a foothold in one enclave on the microgrid control system network, it may be possible for the adversary to eavesdrop on communications within that enclave but traffic within other enclaves remains secure. As such, eavesdropping is partially mitigated for a segmented control system network. In contrast, an adversary with access to a single point in a flat control system network may be able to eavesdrop on traffic for the entire network. By localizing the influence of actors to a particular enclave, the consequences of both local failures and vulnerabilities are isolated within that enclave.

Chapter 5

Example Reference Architecture Implementation

One approach to segmenting the microgrid control system network is to first identify the system functions that occur as part of the microgrid operations. These functions should be selected at a granularity that captures a full system function that does not directly overlap another function. For example, a system function might be one listed in Section 4.2.1 or could be more granular, such as sensing loss of utility power, isolating from the utility, disconnecting renewables, or energizing the microgrid. Once the functions are defined, a suite of actors contributing to each function can be identified. Actors that participate in a common set of system functions can then be grouped together into appropriate enclaves. If it makes sense, further enclave segmentation may be performed along physical boundaries or by data exchange requirements. Lastly, in order to complete a full system function, two or more enclaves may need to communicate; these enclaves are grouped into functional domains and data exchange attributes are used to define communication across enclave boundaries.

To illustrate the segmentation process, we briefly use the *Connect/Disconnect Microgrid* system function as a basis for applying the segmentation steps. Islanding of the microgrid when the installation's distribution system loses power is one of the key functions of the system's operation. This function enables an installation to isolate itself from the power utility and permits activation of the microgrid. This example is predicated on the microgrid control system having already sensed a loss of power and only focuses on the steps that occur after the decision to disconnect from the distribution system has been made. The identified system function is *Connect/Disconnect Microgrid* and the power actors typically involved in this system function include—

- intelligent electronic devices (IEDs) at the points of common coupling (PCCs) used to monitor voltage and current sensors and control breakers and disconnect switches, and
- the energy management system (EMS) that optimizes and controls the microgrid.

The IEDs located at the PCCs are critical to the *connect/disconnect* function, but the EMS, in its oversight and optimization role, will participate in many system functions. Therefore, it's reasonable to segment the IEDs at the PCC into one enclave and the EMS into another. Because the two enclaves need to communicate, they will be participants in a functional domain that allows the enclaves to communicate in order to complete the *Connect/Disconnect Microgrid* system function.

In the following sections, we present an example microgrid control system network implementation, including types of communication occurring on that network, example data exchange attributes for actors in the network, an example of how the network can be segmented to create enclaves and functional domains, and how cyber actors can be used to enforce network segmentation and provide the necessary level of security.

5.1 Microgrid Control System Network

Figure 5.1 depicts a basic microgrid control system network complete with a generator, breakers, transformers, an automatic transfer switch (ATS), IEDs, an EMS, a renewable energy source, and a human-machine interface (HMI) client and server. The network configuration is a typical flat network where all actors communicate using Distributed Network Protocol (DNP3) over the same segment of a Transmission Control Protocol/Internet Protocol (TCP/IP) control network. The goal of applying the microgrid cyber security reference architecture to this example network is to arrive at a more secure network configuration.

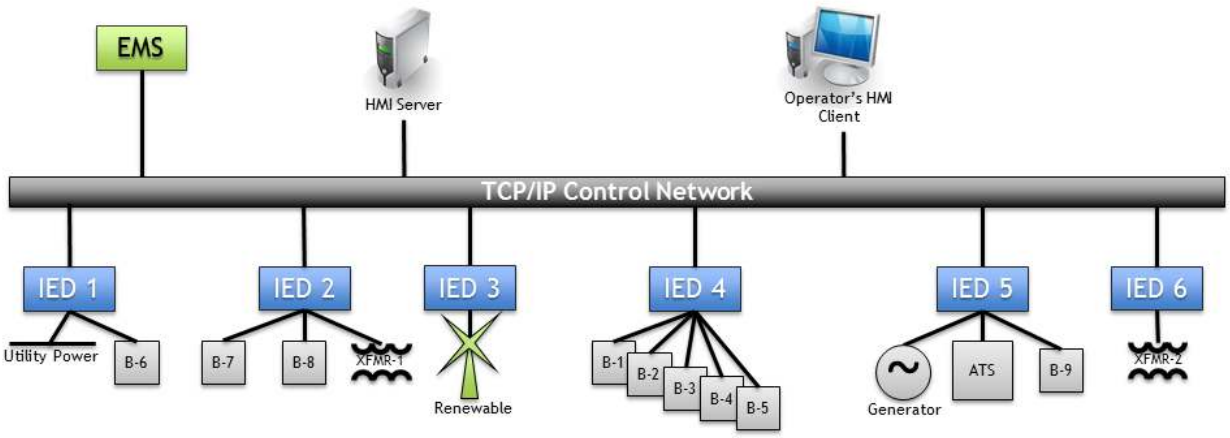

Figure 5.1. Example microgrid control system network in flat configuration.

5.2 High-Level Data Exchanges

Figure 5.2 presents a high-level overview of the data exchanges in which an IED on this particular microgrid control system network is involved. The IED collects data from a connected power component and processes the raw data in two different ways. One, the data is encapsulated in a TCP message that is then sent to the EMS. Two, the data is processed by a local program that may trigger a reaction by the IED to send a control signal to a connected power actor. The IED also receives control messages from the EMS

over the Transmission Control Protocol/Internet Protocol (TCP/IP) network. These control messages may be in the form of an information request to which the IED replies with an appropriate response or it may be a control action the EMS wants the IED to execute on a power system device.

Figure 5.3 presents a high-level overview of the data exchanges in which an EMS on the microgrid control system network is involved. The EMS receives power data from IEDs over the TCP/IP network, and it forwards that data to an HMI server. The power data is also processed by a local program that is used to automate control over the power network and may result in control signals being sent to appropriate IEDs. The EMS may also receive manual control messages from an operator of an HMI system. These control messages are sent from the HMI server via the EMS to the appropriate IEDs.

For some implementations, this high level analysis of the data exchanged between power actors might be sufficient to adequately segment the network; however, most implementations will require closer examination. Data exchange worksheets, described in Section 4.3, are completed for each type of data exchange between any actors in the microgrid control system network. For example, consider Table 5.1 and Table 5.2 that describe the data exchanges between the EMS and a generator controller and the HMI system, respectively. To help determine if the generator controller on the diesel generator connected to IED-5 (Figure 5.1) should be in a different enclave than the HMI system, we can compare the data exchange attributes described in the worksheets. Stark differences in data exchange requirements in conjunction with differences in system function might warrant a separation. In this case, we find that the EMS communications to the generator controller are lower in volume and at times require lower integrity than the EMS communications to the HMI. This realization and acknowledging the differences in system functions between the two (i.e., the HMI and generator controller predominantly participate in different system functions), makes a strong case to separate the generator controller and HMI into separate enclaves.

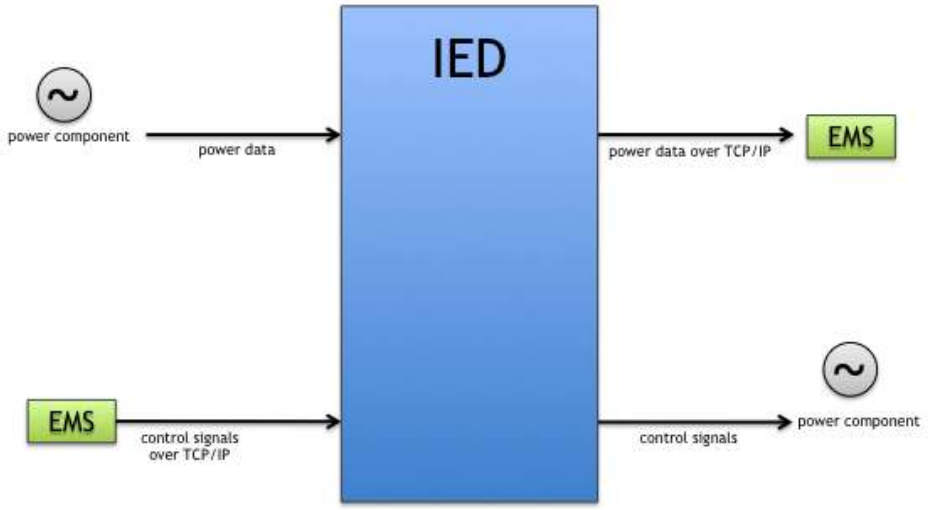

Figure 5.2. High-level data exchanges of an IED.

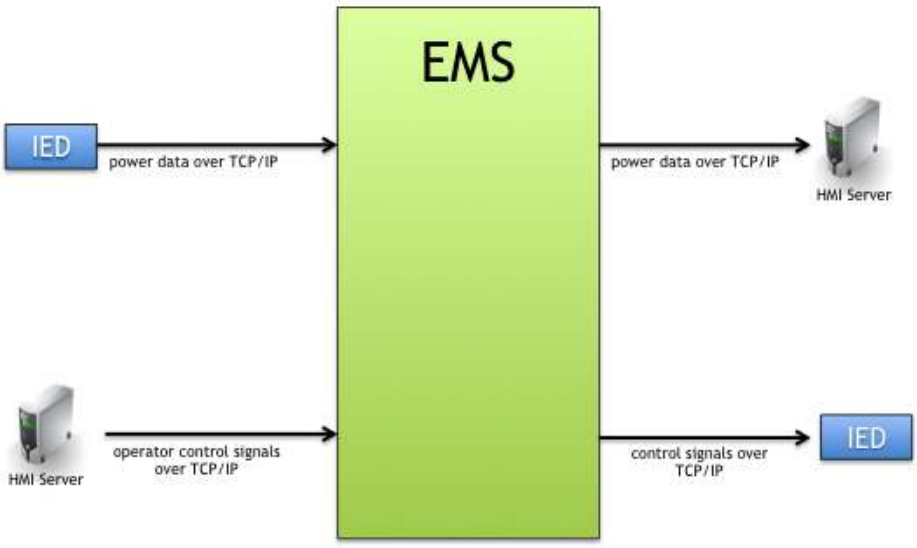

Figure 5.3. High-level data exchanges of an EMS.

Table 5.1. Example attributes for data exchanges related to AGMC operations that originate from an EMS and terminate at a generator controller.

Data Exchange Attributes for *Automated Grid Management and Control (AGMC) Operations*		
Source	*EMS*	*EMS*
Destination	*Generator controller*	*Generator controller*
Exchange		
Type	monitor	control
Interval	seconds	seconds, minutes
Method	unicast	unicast
Priority	medium	medium
Latency Tolerance	medium	medium
Data		
Type	run/stop status, breaker status, kilowatt(s) (kW) output, kilovolt-amperes reactive (kVAr) output, frequency, power factor, diesel fuel level	start, stop, breaker control, excitation control, governor droop settings
Accuracy	1 decimal, second	second
Volume	bytes	bytes
Reliability	important	critical
Information Assurance		
Confidentiality	medium	medium
Integrity	medium	high
Availability	high	high

Table 5.2. Example attributes for data exchanges related to AGMC operations that originate from an EMS and terminate at an HMI.

Data Exchange Attributes for *Automated Grid Management and Control (AGMC) Operations*	
Source	*EMS*
Destination	*HMI*
Exchange	
Type	report
Interval	seconds
Method	unicast
Priority	medium
Latency Tolerance	medium
Data	
Type	all read-only data listed for exchanges where supervisory control and data acquisition (SCADA)/EMS is the source of the data exchange
Accuracy	1 decimal, seconds
Volume	kilobytes
Reliability	critical
Information Assurance	
Confidentiality	medium
Integrity	high
Availability	high

5.3 Network Segmentation

As shown in Figure 5.4, five different enclaves were created for this example of a generic electric power system and microgrid control system network. The **Operator** enclave that segments the operator's HMI client from the rest of the network was created because of potentially unique security concerns. Actors within this enclave may be at higher risk, because a human operator has the potential to be an insider or carry in malicious software via removable media. The **Server** enclave was created to contain server-based systems that automate parts of the microgrid control system network and require minimal human interaction. The importance of the EMS to the overall functionality of the microgrid and the broad influence it has over the devices, in addition to the sheer volume of data being exchanged, warrants the creation of its own enclave. The remaining enclaves were defined through consideration of the system functions that support the microgrid operational modes (described in Section 2.1) and the data exchange attributes relevant to each IED and their respective power components. The enclaves include—

- **Distribution**: detection of utility power status, system protection, and isolation and re-syncing of the microgrid
- **Renewables**: disconnection and reconnection of inverter-based renewables
- **Generation**: starting, syncing, power control, and unloading of microgrid generators

Based on the microgrid system functions and data exchanges necessary for their reliable operation, Figure 5.4 illustrates the four functional domains created:

- **Domain A**: power data, meter data, breaker/switch positions, alarms, and operator control signals are sent between the operator HMI client in the Operator enclave and the HMI server/EMS in the Server enclave.
- **Domain B**: microgrid isolation controls, re-syncing commands, and breaker controls are sent between actors in the Isolation enclave and the EMS in the Server enclave
- **Domain C**: disconnect and connect commands are sent between switches in the Renewables enclave and the EMS in the Server enclave
- **Domain D**: generator starting, syncing, power control, and unloading commands are sent between generator controllers and breakers in the Generation enclave and the EMS in the Server enclave

Given the identified enclaves and functional domains, the flat microgrid control system network depicted in Figure 5.1 can be reconfigured using the reference architecture as shown in Figure 5.5. In this example reference architecture implementation, the network has been segmented to incorporate the five different enclaves. The underlying physical network does not necessarily need to change. Methods of configuring access controls to enforce the enclave segmentation may include using additional layer 3 switches/routers or implementing virtual

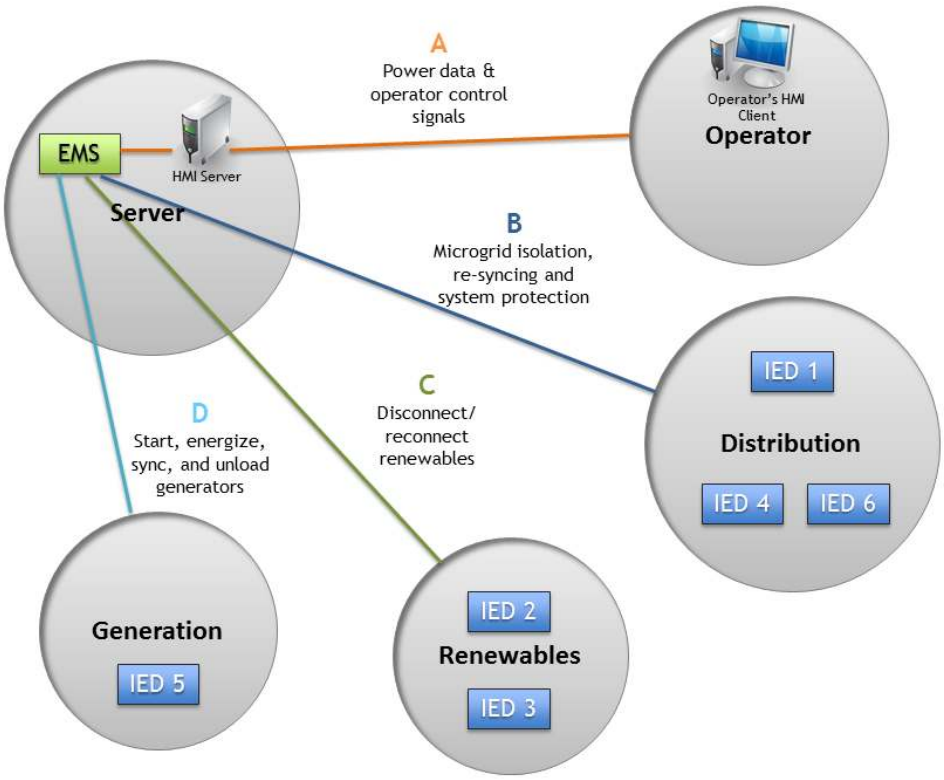

Figure 5.4. Implementation of enclaves and functional domains to segment the microgrid control system network.

local area networks (VLANs) on a single router. The important aspect of the network segmentation is the restriction of network communications (i.e., data exchanges) between enclaves to only that which is necessary for the respective functional domains (as shown in Figure 5.4). Other cyber actors, including intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), can also be included to detect and prevent unauthorized communications between enclaves or bump-in-the-wire (BITW) devices can be used to provide encryption services. Lastly, depending on the sensitivity of the microgrid control system network, certain information assurance (IA) controls must also be applied to strengthen the security posture of the network.

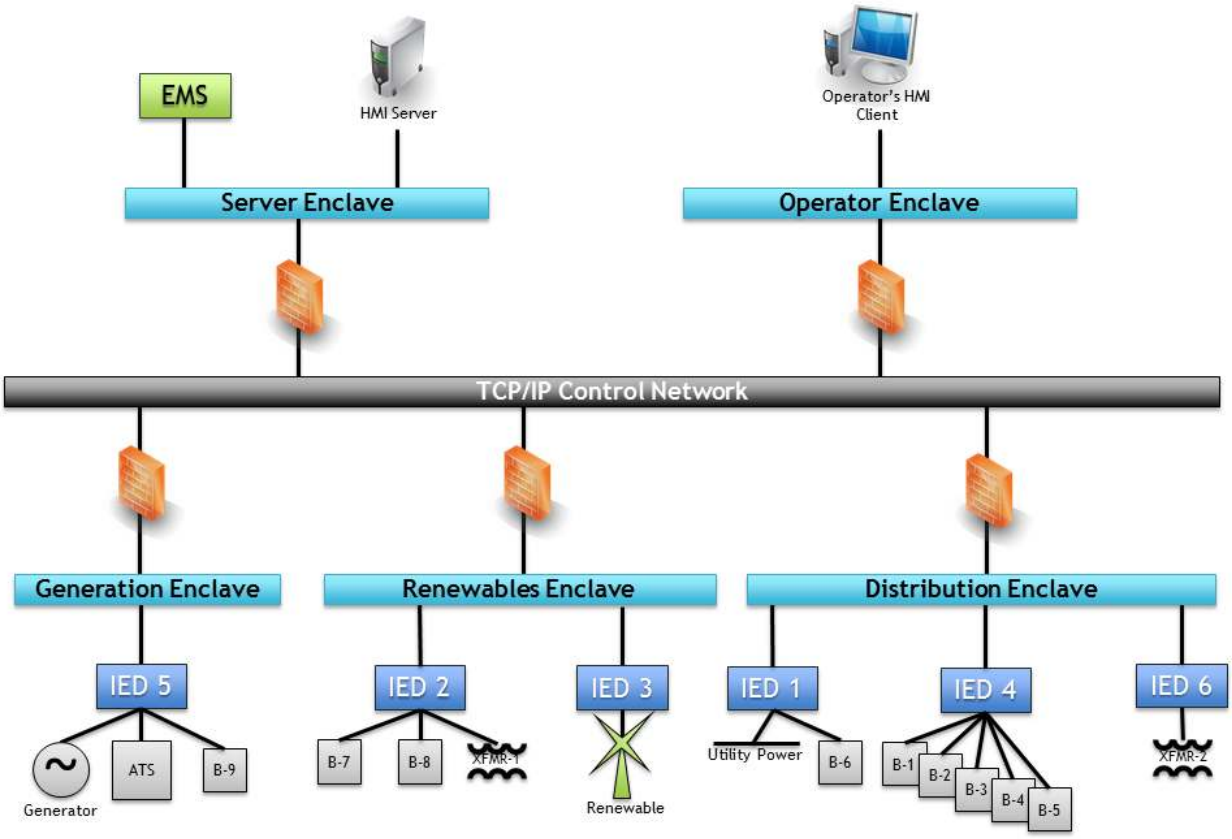

Figure 5.5. Reference architecture implementation of microgrid control system network.

This page intentionally left blank.

Chapter 6

Future Work

This document summarizes the on-going cyber security work and resulting cyber security reference architecture for a secure microgrid control system network. The architecture presented here provides guidelines and security recommendations for the implementation of a secure microgrid control system at Department of Defense (DOD) installations. Our design approach supports the management of a secure control system for the microgrid using functional segmentation to provide defense-in-depth at the control system level. In its current form, this document is considered version 1.0. We plan to continue work on the microgrid cyber security reference architecture. Future versions of this document will include a stronger focus on the design principles of monitoring and reconfiguration, in addition to an assessment of information assurance (IA) controls and how they can be met using the reference architecture and industry best practices for securing control systems.

This page intentionally left blank.

References

[1] Control System Security Program (CSSP), "Recommended practice: Improving industrial control systems cybersecurity with defense-in-depth strategies," tech. rep., National Cyber Security Division (NCSD), Department of Homeland Security (DHS), October 2009.

[2] Smart Grid Interoperability Panel (SGIP)–Cyber Security Working Group (CSWG), "Guidelines for smart grid cyber security," NIST Interagency Report (NISTIR) 7628, Vol. 1–3, National Institute of Standards and Technology (NIST), August 2010.

[3] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security," NIST Special Publication (SP) 800-82, NIST, Gaithersburg, MD, June 2011.

[4] DOD, "Information assurance (IA) implementation," DOD Instruction (DODI) 8500.2, DOD, February 2003.

[5] DOD, "DOD information assurance certification and accreditation process (DIACAP)," DODI 8510.01, DOD, November 2007.

[6] Joint Task Force Transformation Initiative Interagency Working Group, "Recommended security controls for federal information systems and organizations," NIST SP 800-53, Revision 3, NIST, Gaithersburg, MD, August 2009.

[7] Systems and Network Analysis Center (SNAC), "A framework for assessing and improving the security posture of industrial control systems (ICS), Version 1.1," tech. rep., National Security Agency (NSA), August 2010.

[8] B. Van Leeuwen, "Impacts of IPv6 on infrastructure control systems," Sandia Report SAND2007-0383P, Sandia National Laboratories (SNL), Albuquerque, NM, September 2007.

[9] CSSP, "Catalog of control systems security: Recommendations for standards developers," tech. rep., NCSD, DHS, September 2009.

[10] CSSP, "Common cybersecurity vulnerabilities in industrial control systems," tech. rep., NCSD, DHS, May 2011.

[11] Institute of Electrical and Electronics Engineers (IEEE) Standards Coordinating Committee 21 on Fuel Cells, Photovoltaics, Dispersed Generation, and Energy Storage, "IEEE standard for interconnecting distributed resources with electric power systems," IEEE Std 1547™-2003 (R2008), IEEE, New York, NY, July 2003. Reaffirmed 25 September 2008.

[12] SNAC, "Defense in depth: A practical strategy for achieving information assurance in today's highly networked environments," tech. rep., NSA. http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

[13] Supply Chain Management Center, "The ICT SCRM community framework development project: Final report," tech. rep., University of Maryland, College Park, MD, December 2011.

[14] "Architecture and design considerations for secure software." Software Assurance Pocket Guide Series: Development, Volume V, February 2011.

[15] S. Frankel, B. Eydt, L. Owens, and K. Scarfone, "Establishing wireless robust security networks: A guide to IEEE 802.11i," NIST SP 800-97, NIST, Gaithersburg, MD, February 2007.

[16] D. P. Duggan, S. R. Thomas, C. K. Veitch, and L. Woodard, "Categorizing threat: Building and using a generic threat matrix," Sandia Report SAND2007-5791, SNL, Albuquerque, NM, September 2007.

[17] DOD, "Information assurance (IA)," DOD Directive (DODD) 8500.01E, DOD, October 2002. Certified current as of April 23, 2007.

[18] J. A. Rome, "Enclaves and collaborative domains," tech. rep., Oak Ridge National Laboratory (ORNL), Oak Ridge, TN, 2003. http://www.ornl.gov/~webworks/cppr/y2001/pres/117259.pdf.

[19] IEEE Standards Coordinating Committee 21 on Fuel Cells, Photovoltaics, Dispersed Generation, and Energy Storage, "IEEE guide for smart grid interoperability of energy technology and information technology operation with the electric power system (EPS), end-use applications, and loads," IEEE Std 2030™-2011, IEEE, New York, NY, September 2011.

Appendix A

Cyber Security Example Implementation

In this appendix, we describe a cyber security reference implementation. The intent of the reference implementation was to exercise the reference architecture process and illustrate the architecture's ability to increase the elevated security of a microgrid control system by comparing red teaming activities performed on a flat microgrid control system network to those performed on a segmented microgrid control system network based on the cyber security reference architecture. Components of the reference implementation include a power system model that simulates notional microgrid power components, a front-end processor (FEP), remote terminal units (RTUs), operator human-machine interfaces (HMIs), an HMI server, networking equipment such as routers and firewalls, and an intrusion detection system (IDS). In the following appendix, we also provide data exchange worksheets (Appendix B).

Segmentation Using the Reference Architecture

To test the reference architecture process, a notional microgrid and microgrid control system network was designed based on Sandia's ESM experience. The notional microgrid consists of several diesel generators, a photovoltaic (PV) array, a wind turbine, automatic transfer switches, and controllers/intelligent electronic devices (IEDs)/remote terminal units (RTUs), primary and backup HMIs, an HMI server, and distribution equipment such as transformers, breakers, and switches. Based on this design and the identified system functions, the microgrid was segmented into the following three enclaves:

- **Operator**: primary and backup HMIs and a Snort IDS
- **Server**: HMI server and a Snort IDS
- **Manager**: all intelligent power controllers (IPCs) and a Snort IDS

Although the breakdown of system functions would warrant more enclaves and greater segmentation, just three enclaves were established to limit the reference implementation complexity and conserve resources. Segmentation into three enclaves is enough to sufficiently evaluate the efficacy of the reference architecture. The three enclaves also form two func-

tional domains. Domain A exists for communications between the HMI clients and the HMI server and Domain B exists for communications between the HMI server and the IEDs.

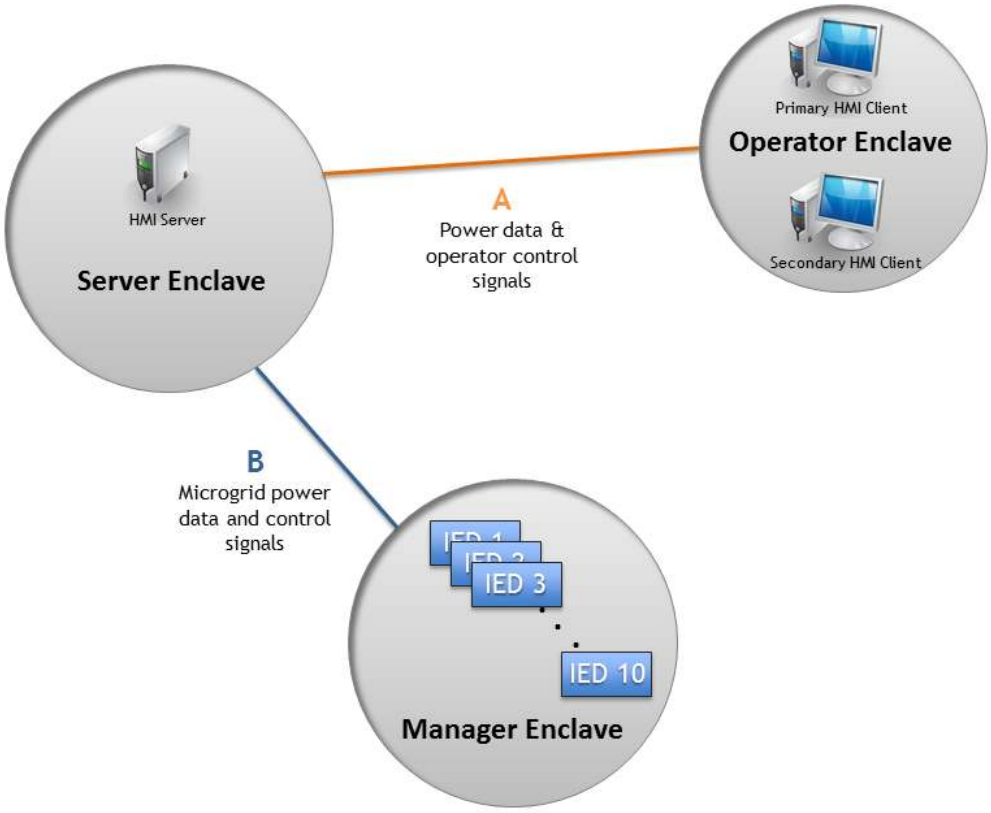

Figure A.1. Test bed enclaves and functional domains.

Reference Implementation Configurations

To thoroughly evaluate the effects of the reference architecture and correlate results of different operating conditions, the following four reference implementation configurations were created for the red team to evaluate:

1. Flat microgrid control network
2. Segmented microgrid control network
3. Flat microgrid control network with hardened devices

4. Segmented microgrid control network with hardened devices

The flat microgrid control network (Figure A.2) is a simple network with no segmentation where all devices on the network can directly communicate with one another without the need for routing. In this configuration, communications are not encrypted, access controls do not exist, and system patches are not up-to-date.

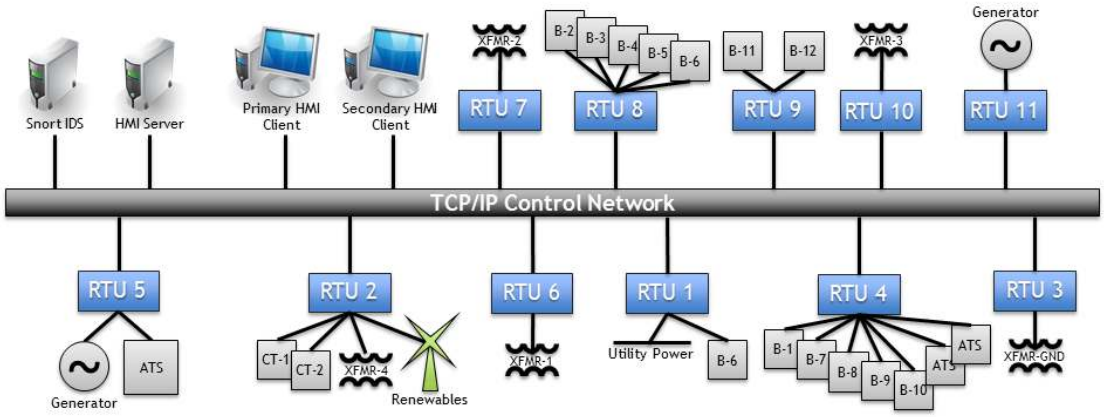

Figure A.2. Logical view of flat test bed implementation.

The segmented microgrid control network (Figure A.3) compartments the control network into the three enclaves described above. In this configuration, routers and firewalls with access controls exist in each enclave to restrict communications between the enclaves and enforce the functional domains. Similar to the flat network, there is no encryption and devices in the control network do not have up-to-date patches.

The flat and segmented microgrid control networks with hardened devices are similar to their predecessors, but all devices and operating systems are fully patched and communications between devices are encapsulated in secure shell (SSH) or Transport Layer Security/Secure Sockets Layer (TLS/SSL) tunnels.

Additionally, for the segmented control networks, red team members were granted the following levels of access:

- **High**: red team members have access to all devices in all the enclaves (as well as access to the network connecting the enclaves)
- **Medium**: red team members have access to all devices in the Operator enclave (as well as access to the network connecting the enclaves)
- **Low**: red team members do not have direct access to any of the enclaves (they only have access to the network connecting the enclaves)

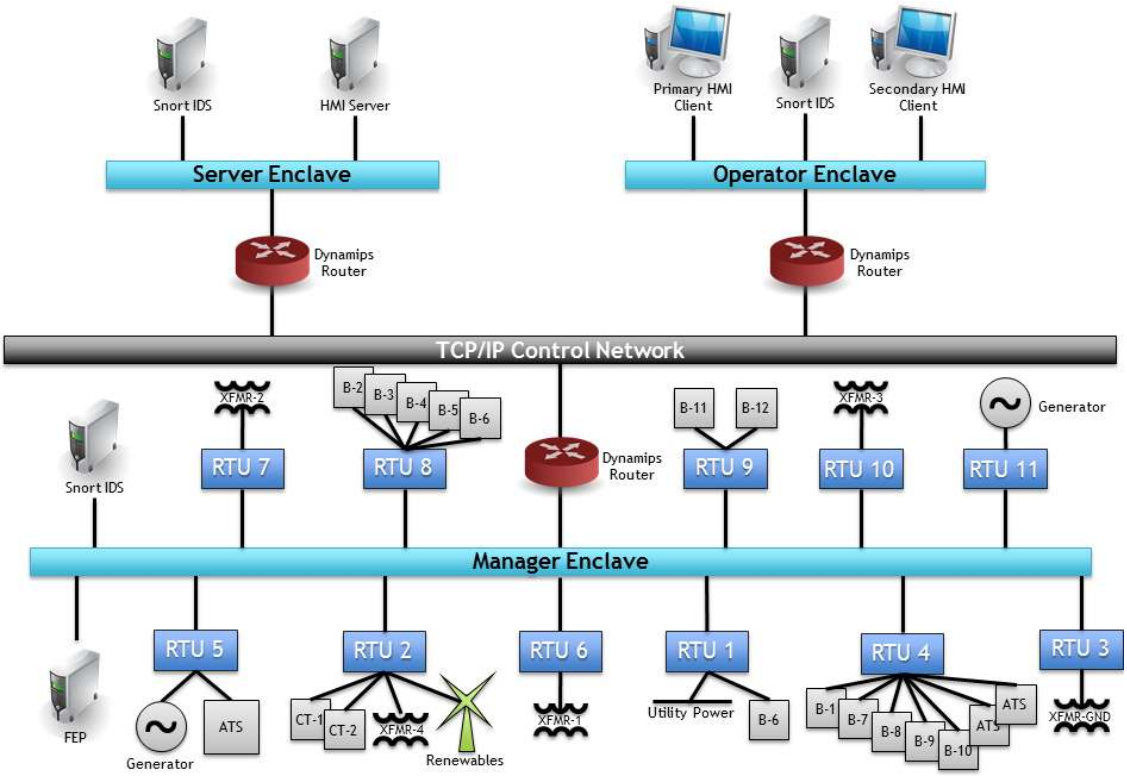

Figure A.3. Logical view of segmented test bed implementation.

Each reference implementation configuration of the notional microgrid and microgrid control system was implemented using a combination of simulated and emulated devices. The power system components were modeled using a power solver program to simulate the two generators, the distribution lines, the PV array, wind turbines, and all transformers. Each IPC used to control and monitor power components was modeled as an RTU using Sandia National Laboratories (SNL)'s Virtual Control System Environment (VCSE). A single RTU was created for each IPC in the designed and mapped to the same power components. A FEP, also implemented in the VCSE, was used to transfer power data and control signals between each RTU and an HMI server that communicates with the operator HMIs.

Cyber actors included switches, routers, and IDSs. A single, virtual local area network (VLAN)-capable switch was used to create each of the three network segments, as well as a fourth router backbone network. Routers for each enclave were emulated using Dynamips[7] and the devices in each enclave were placed on the appropriate VLAN (with each of the three routers being connected to the router backbone VLAN as well). Snort was used as the IDS in each enclave and configured with Modbus signatures to detect malevolent Modbus traffic in the manager enclave.

[7] `http://www.gns3.net/dynamips/`

This page intentionally left blank.

Appendix B

Data Exchange Worksheets

In this appendix, we provide completed worksheets for the data exchanges used as part of the notional architecture (Appendix A). As described in Section 4.3, data exchange worksheets are used to define communication between actors within enclaves and functional domains. Within an enclave, data exchange attributes describe—

- latency, bandwidth, and quality of service (QoS) for intra-enclave communications
- types of network traffic to expect
- necessary level of enclave cyber security

Within a functional domain, data exchange worksheets help to identify—

- which enclaves need to communicate
- types of network traffic that will be communicated between enclaves
- latency, bandwidth, and QoS for inter-enclave communications
- cyber security concerns for inter-enclave communications

The data exchange worksheet assists in identifying the operational necessities for data exchange between actors and cyber security needs for information assurance (IA). A template data exchange worksheet is provided in Table 4.1. Each field of the worksheet has specific values that can be used to describe the data exchange attributes. Table 4.2 presents each attribute, its definition, and example values used to complete that field.

The following data exchange worksheets define communication between automated grid management and control (AGMC) operations actors as described in Section 4.2.1. To summarize, AGMC operations include interactions between the energy management system (EMS), aggregators, inverters, relays, and nearly every other power actor in the microgrid control system network (e.g., remote terminal units (RTUs) and other intelligent electronic devices (IEDs)).

Table B.1. Attributes for data exchanges related to AGMC operations between a FEP and an RTU.

Data Exchange Attributes for *Automated Grid Management and Control (AGMC) Operations*		
Source	*Remote terminal unit*	*Front-end processor*
Destination	*Front-end processor*	*Remote terminal unit*
Exchange		
Type	monitor	control
Interval	seconds	minutes to hours
Method	unicast	unicast
Priority	medium	high
Latency Tolerance	medium	low
Data		
Type	breaker status, kW output, kVAr output, voltage magnitude and angle phase, line flow	breaker control, kW output control, voltage control
Accuracy	2 decimal places	2 decimal places
Volume	bytes	bytes
Reliability	important	critical
Information Assurance		
Confidentiality	low	medium
Integrity	high	high
Availability	high	high

Table B.2. Attributes for data exchanges related to AGMC operations between an HMI server and a FEP.

Data Exchange Attributes for *Automated Grid Management and Control (AGMC) Operations*		
Source	*Front-end processor*	*HMI server*
Destination	*HMI server*	*Front-end processor*
Exchange		
Type	monitor	control
Interval	seconds	minutes to hours
Method	unicast	unicast
Priority	medium	high
Latency Tolerance	medium	low
Data		
Type	breaker status, kW output, kVAr output, voltage magnitude and angle phase, line flow	breaker control, kW output control, voltage control
Accuracy	2 decimal places	2 decimal places
Volume	bytes	bytes
Reliability	important	critical
Information Assurance		
Confidentiality	medium	medium
Integrity	high	medium
Availability	medium	medium

Table B.3. Attributes for data exchanges related to AGMC operations between an HMI client and an HMI server.

Data Exchange Attributes for *Automated Grid Management and Control (AGMC) Operations*		
Source	*HMI server*	*HMI client*
Destination	*HMI client*	*HMI server*
Exchange		
Type	monitor	control
Interval	seconds	minutes to hours
Method	unicast	unicast
Priority	low	medium
Latency Tolerance	high	medium
Data		
Type	breaker status, kW output, kVAr output, voltage magnitude and angle phase, line flow	breaker control, kW output control, voltage control
Accuracy	2 decimal places	2 decimal places
Volume	bytes	bytes
Reliability	informative	important
Information Assurance		
Confidentiality	medium	medium
Integrity	high	medium
Availability	medium	medium

DISTRIBUTION:

1	MS 0671	Jordan H. Henry, 05628 (electronic copy)
1	MS 0671	Bryan T. Richardson, 05628 (electronic copy)
1	MS 0671	Derek H. Hart, 05628 (electronic copy)
1	MS 0672	Cynthia K. Veitch, 05621 (electronic copy)
1	MS 0751	Richard P. Jensen, 06914 (electronic copy)
1	MS 1108	Jason E. Stamp, 06111 (electronic copy)
1	MS 0899	Technical Library, 9536 (electronic copy)

This page intentionally left blank.

Sandia National Laboratories