SAND2020-13723

SANDIA REPORT
SAND #
Printed TBD

Cybersecurity of Networked Microgrids: Challenges, Potential Solutions, and Future Directions

Shamina Hossain-McKenzie, Matthew J. Reno, Russell Bent*, and Adrian Chavez

*Los Alamos National Laboratory

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

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

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

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

Available to DOE and DOE contractors from

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

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

Available to the public from

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

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

ABSTRACT

Networked microgrids are clusters of geographically-close, islanded microgrids that can function as a single, aggregate island. This flexibility enables customer-level resilience and reliability improvements during extreme event outages and also reduces utility costs during normal grid operations. To achieve this cohesive operation, microgrid controllers and external connections (including advanced communication protocols, protocol translators, and/or internet connection) are needed. However, these advancements also increase the vulnerability landscape of networked microgrids, and significant consequences could arise during networked operation, increasing cascading impact. To address these issues, this report seeks to understand the unique components, functions, and communications within networked microgrids and what cybersecurity solutions can be implemented and what solutions need to be developed. A literature review of microgrid cybersecurity research is provided and a gap analysis of what is additionally needed for securing networked microgrids is performed. Relevant cyber hygiene and best practices to implement are provided, as well as ideas on how cybersecurity can be integrated into networked microgrid design. Lastly, future directions of networked microgrid cybersecurity R&D are provided to inform next steps.

ACKNOWLEDGMENT

This work was performed with the support of the Department of Energy (DOE) Office of Electricity's (OE) Microgrid Research and Development Program and its program manager, Dan Ton. The views expressed in the article do not necessarily represent the views of the DOE or the United States Government.

The research work conducted at Los Alamos National Laboratory is done under the auspices of the National Nuclear Security Administration of the U.S. Department of Energy under Contract No. 89233218CNA000001.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

To increase grid resilience and reliability, networked microgrids are being investigated as a promising solution. Networked microgrids are clusters of geographically-close, islanded microgrids that can flexibly function as a single, aggregate island. This flexibility enables customer-level resilience and reliability improvements during extreme event outages and also reduces utility costs during normal grid operations. The coordinated cluster of microgrids would increase the amount of available resources and extend service availability; this coordination can be performed through an energy management system (EMS), distribution management system (DMS), or a central microgrid controller [3].

In previous work, the Department of Energy Office of Electricity scoped networked microgrid design and operation, and the need for tools to simulate/evaluate networked microgrids in a quantitative and systematic manner was identified [1, 4]. The study proposed a tool that encompassed design and planning, including aspects such as regulatory environment, business case evaluation, architecture design and use cases, and dynamical system interactions, as well as system operations, including networked controller development and system and network state estimation.

This scoping study led to the ongoing DOE Advanced Grid Microgrid Research Program Resilient Operation of Network Microgrids (RONM) project that is developing a design and planning tool for networked microgrids that achieves the aforementioned principles. Further details on the preliminary design process for networked microgrids can be found in [5]. This project addresses various networked microgrid needs, from protection design to testing recovery scenarios to defining resilience goals. However, one direction the RONM project, in collaboration with its industrial advisory board, has identified as a gap is networked microgrid cybersecurity.

While there are various challenges to address for a full, comprehensive implementation of networked microgrids, a prominent concern that needs to be addressed from the design stage is networked microgrid cybersecurity. The networking of the microgrids is dependent on the operation of communicative microgrid controllers that enable the quick reconfiguration of the aggregate system. Furthermore, individual microgrids could employ communication-assisted control and protection schemes that expand operational capabilities but also broaden the cyber attack landscape [6]. Additional complexity is derived from the potential for each microgrid to have different levels of cybersecurity defenses; an integral question is if the connection of a cyber-secure microgrid to a microgrid with less or nonexistent cybersecurity decreases overall, networked security and increases cascading impacts.

In this document, we investigate networked microgrid communications, components, and functions to understand what cybersecurity risks and consequences require attention. A review of state of the art research pertaining to networked microgrid cybersecurity is performed and a subsequent gap analysis of what future directions need to be pursued for enhanced networked microgrid cybersecurity. These future directions include straightforward cyber hygeine principles that can be adopted as well as more complex research questions that need to be addressed.

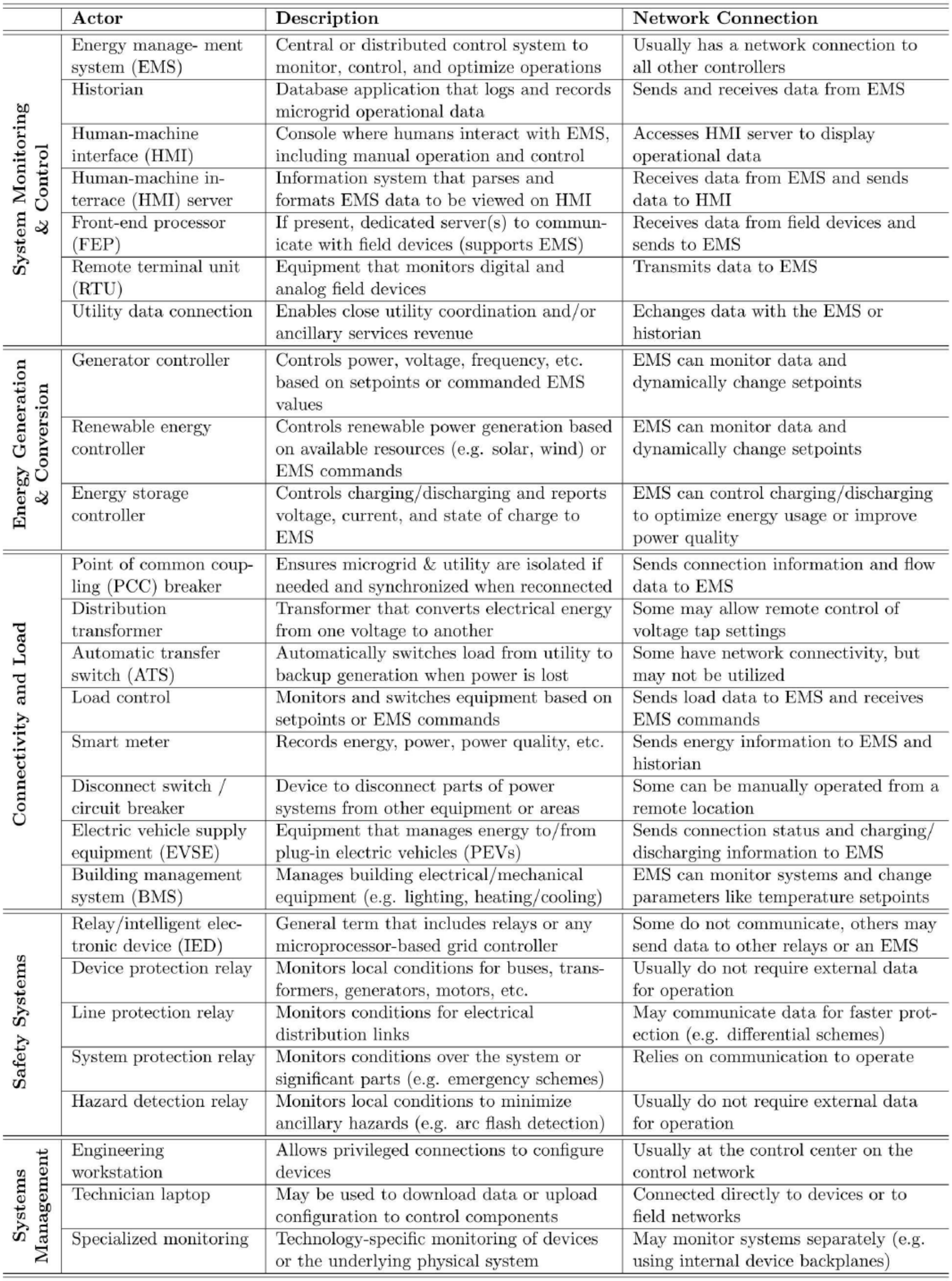
2. NETWORKED MICROGRID COMMUNICATIONS, COMPONENTS, AND FUNCTIONS

Individual microgrids within a network may vary in the types of communications supported, the physical and network components, and functions. It is important to understand the different processes supported to glean what type of cybersecurity vulnerabilities and consequences are plausible. For the communication network, Stamp et al. defined the common actors in microgrid data exchange in Table 2-1 [2].

This list of actors provides insight into the types of network components and characteristics required to support microgrid functions. In the report “Microgrid Cyber Security Reference Architecture (V2)" by Stamp et. al, cybersecurity improvements to the microgrid communication network are proposed [2]. Specifically, segmentation of the network into enclaves and grouping those enclaves in terms of functional domains. This approach is further discussed in the next chapter.

Although many microgrid cybersecurity principles map naturally to cybersecurity principles for networked microgrids, it is important to consider what are the unique properties of networked microgrids that require further analysis. For example, in networked microgrids, the participating microgrids are “networked" at the physical layer (connected by the distribution system), the control layer (independent local controllers manage the connection), or both [1]. If connected at the control layer, a central controller that has some visibility into each of the networked microgrids is needed to coordinate objectives and operations of independent controllers at a higher level, as pictured in Figure 2-1 [1].

The visibility each networked microgrid needs to provide may include information such as available generation and present loading status. Various control architectures may exist, with and without central controllers for high-level coordination, which can vary the information shared between independent controllers. Furthermore, transactional information may need to be shared between microgrids participating in a networked operation. This information may need to be shared over encrypted channels and/or other secure mechanisms.



	Actor	Description	Network Connection
System Monitoring & Control	Energy manage- ment system (EMS)	Central or distributed control system to monitor, control, and optimize operations	Usually has a network connection to all other controllers
	Historian	Database application that logs and records microgrid operational data	Sends and receives data from EMS
	Human-machine interface (HMI)	Console where humans interact with EMS, including manual operation and control	Accesses HMI server to display operational data
	Human-machine interrace (HMI) server	Information system that parses and formats EMS data to be viewed on HMI	Receives data from EMS and sends data to HMI
	Front-end processor (FEP)	If present, dedicated server(s) to communicate with field devices (supports EMS)	Receives data from field devices and sends to EMS
	Remote terminal unit (RTU)	Equipment that monitors digital and analog field devices	Transmits data to EMS
	Utility data connection	Enables close utility coordination and/or ancillary services revenue	Echanges data with the EMS or historian
Energy Generation & Conversion	Generator controller	Controls power, voltage, frequency, etc. based on setpoints or commanded EMS values	EMS can monitor data and dynamically change setpoints
	Renewable energy controller	Controls renewable power generation based on available resources (e.g. solar, wind) or EMS commands	EMS can monitor data and dynamically change setpoints
	Energy storage controller	Controls charging/discharging and reports voltage, current, and state of charge to EMS	EMS can control charging/discharging to optimize energy usage or improve power quality
Connectivity and Load	Point of common coupling (PCC) breaker	Ensures microgrid & utility are isolated if needed and synchronized when reconnected	Sends connection information and flow data to EMS
	Distribution transformer	Transformer that converts electrical energy from one voltage to another	Some may allow remote control of voltage tap settings
	Automatic transfer switch (ATS)	Automatically switches load from utility to backup generation when power is lost	Some have network connectivity, but may not be utilized
	Load control	Monitors and switches equipment based on setpoints or EMS commands	Sends load data to EMS and receives EMS commands
	Smart meter	Records energy, power, power quality, etc.	Sends energy information to EMS and historian
	Disconnect switch / circuit breaker	Device to disconnect parts of power systems from other equipment or areas	Some can be manually operated from a remote location
	Electric vehicle supply equipment (EVSE)	Equipment that manages energy to/from plug-in electric vehicles (PEVs)	Sends connection status and charging/ discharging information to EMS
	Building management system (BMS)	Manages building electrical/mechanical equipment (e.g. lighting, heating/cooling)	EMS can monitor systems and change parameters like temperature setpoints
Safety Systems	Relay/intelligent electronic device (IED)	General term that includes relays or any microprocessor-based grid controller	Some do not communicate, others may send data to other relays or an EMS
	Device protection relay	Monitors local conditions for buses, transformers, generators, motors, etc.	Usually do not require external data for operation
	Line protection relay	Monitors conditions for electrical distribution links	May communicate data for faster protection (e.g. differential schemes)
	System protection relay	Monitors conditions over the system or significant parts (e.g. emergency schemes)	Relies on communication to operate
	Hazard detection relay	Monitors local conditions to minimize ancillary hazards (e.g. arc flash detection)	Usually do not require external data for operation
Systems Management	Engineering workstation	Allows privileged connections to configure devices	Usually at the control center on the control network
	Technician laptop	May be used to download data or upload configuration to control components	Connected directly to devices or to field networks
	Specialized monitoring	Technology-specific monitoring of devices or the underlying physical system	May monitor systems separately (e.g. using internal device backplanes)

Table 2-1. Common microgrid data exchange actors from [2].

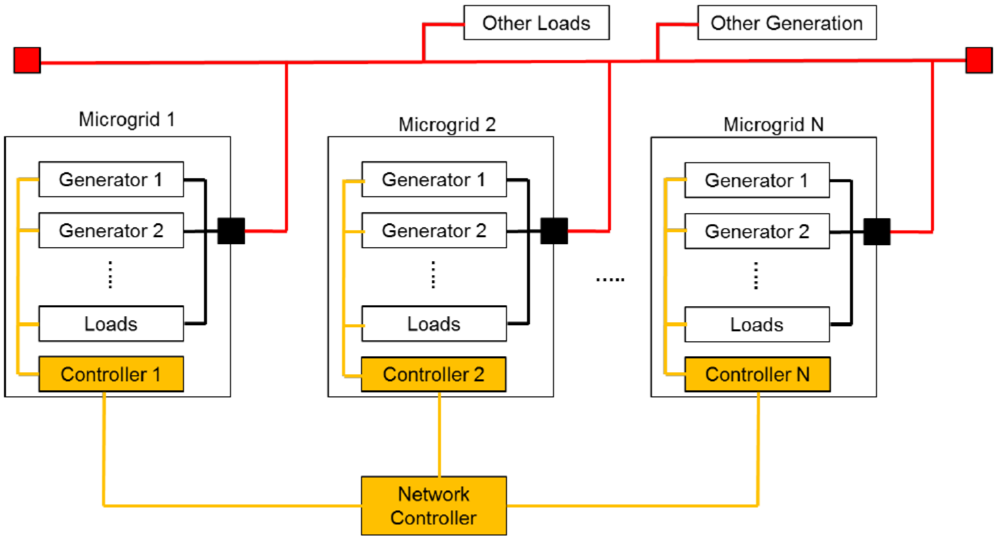


Figure 2-1. Example networked microgrid architecture at both physical and control layers [1].

Therefore, some unique networked microgrid functions as well as challenges that may require additional development include:

- Independent microgrid controllers may be able to make decisions regarding energizing conductors (to successfully network with another system)
- Inter-microgrid communications and controls may be different, due to the lack of standardization, and incompatibility may arise; similar issues may arise for utility to microgrid interactions
  - Protocol translators and other technologies may be needed to facilitate communications
- Different microgrids may have different stability margins; networked operation may improve or detrimentally impact system stability without proper understanding
  - Tools such as RONM are needed to understand dynamic system interactions during the planning stage to avoid detrimental, cascading impacts if a disturbance occurs in networked operation
- Increased reliance on communications for control and optimization
- Regulatory functions include rules on transactions (e.g., utility-ownership issues)
- Importance of Quality of Service (QoS); must ensure significant penetration of networked microgrids does not affect QoS of surrounding customers

These functions and components are an example of the unique needs of networked microgrids, but are by no means comprehensive. However, these examples provide an idea of the types of components, communications, and functions that can occur in networked microgrid operation. As such, Table 2-2 provides an example augmentation to the table shown in Figure 2-1.

Table 2-2. Example of unique networked microgrid data exchange actors.

Networked Microgrids		
Actor	**Description**	**Network Connection**
Independent microgrid controller	Enables networking of individual microgrids (e.g., energizing conductors to achieve control layer connection)	EMS or DMS can monitor data and dynamically change setpoints
Central microgrid controller	Coordinates objectives and functions of networked microgrids for cohesive operation	EMS or DMS can monitor data and dynamically change setpoints
Protocol translator	Enables inter-microgrid communications	Intercepts all incoming and outgoing communications from connected microgrid and translates when necessary (if protocol supported)
External connections	Allows pricing information to be securely exchanged between microgrids; enables protection coordination; shares regulatory policies and rules	Sends and receives information from connected microgrid EMS or DMS

EMSs and DMSs are a large part of the network connection of the different actors listed in both Table 2-1 and Table 2-2, for both individual and networked microgrids. However, as Wang et al. proposed in their paper, decentralized EMSs may be more suitable to coordinate operation of networked microgrids [7]. In their work, stochastic optimization is leveraged to achieve cohesive operation with a mixture of dispatchable generation and distributed energy resources (DERs). Nonetheless, one unique function identified for this EMS was to conduct negotiations among all entities, which can include pricing information.

All in all, there are various devices and processes within microgrids that enable system operation and protection. In this report, we seek to investigate the components, functions, and communications unique to networked microgrids that require additional cybersecurity analysis. Though not comprehensive, this current section details a few networked microgrid actors to begin this analysis, including:

1. Microgrid controllers
    - Independent microgrid controller
    - Central microgrid controller
2. Communications
    - Protocol translators
        - Inter-microgrid transaction system
        - EMS/DMS control commands

3. MICROGRID CYBERSECURITY

Due to its application to critical services, such as military bases, microgrid cybersecurity has become a prominent concern in the recent years [2]. Microgrid infrastructure has an increasing reliance on communication-based systems (that could include multiple protocols), advanced technologies with new access interfaces, and internet connection. These new capabilities can broaden the attack surface of the microgrid and must be carefully assessed and protected.

3.1. Literature Review of Microgrid Cybersecurity

In the microgrid cybersecurity literature, there are two main perspectives considered. First, how cybersecurity of the microgrid can be improved, and second, how microgrids can increase the cyber resilience of the connected grid.

3.1.1. Improving Individual Microgrid Cybersecurity

For improving the cybersecurity of the microgrid, a large focus is upon its network architecture. In the report by Stamp et al., methods to secure a microgrid control system were investigated [2]. The authors focused on identifying the necessary data exchanges, as shown in Figure 2-1, network segmentation strategies, and tools to support the segmentation as well as increase the microgrid's cybersecurity. The aim of the report was to provide a reference architecture for securely implementing microgrid networks that focused on network segmentation and monitoring.

Commonly, microgrid networks are flat networks in which components have direct paths/accessibility to one another. There is usually little or no segmentation incorporated in microgrid networks; without adequate segmentation, an adversary with initial access to the network could easily attack other parts of the network, despite the entry point. Segmentation can defend against this and provide a defense-in-depth approach; in the report, the authors propose separating the network into enclaves defined by system functions, physical locations, and security concerns (i.e., criticality). A functional domain is then defined as a collection of interacting enclaves. The reference architecture proposed using these principles is shown in Figure 3-1; red team experiments were performed on a few case studies to demonstrate the security benefits of the reference architecture and are also included in the full report [2].

In the paper by Mohan et al., the microgrid network architecture was also studied [8]. This work focused on the cybersecurity external connections to the microgrid – which is of prominent concern for networked microgrids as well. The authors discuss the challenges of securing external connections, including the increased latency from adding encryption to communications and the

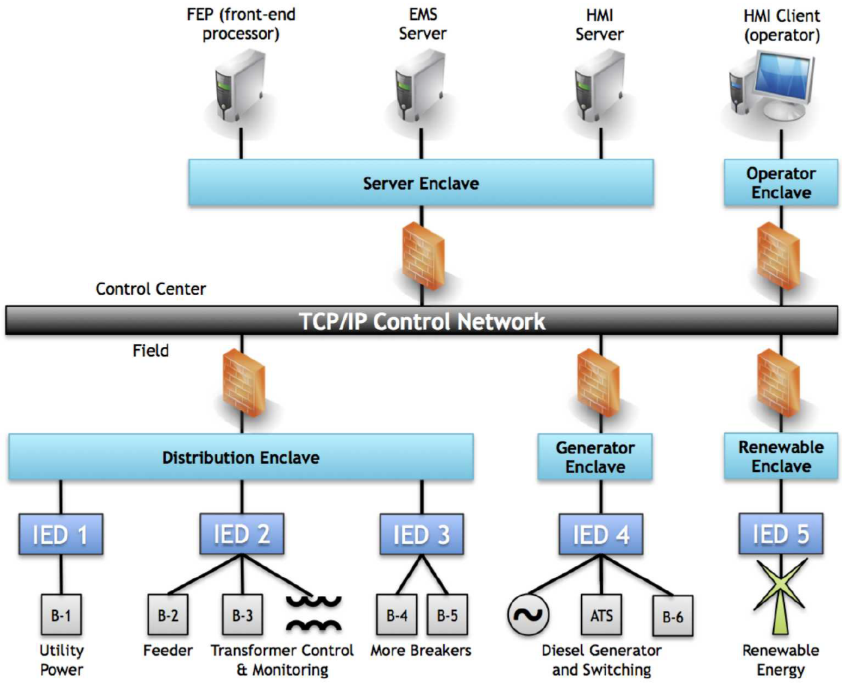


Figure 3-1. Reference microgrid network architecture proposed by Stamp et al. [2].

complexity of acquiring certificates. To combat this, the authors propose a network segmentation strategy based on separating the fast, real-time system and the external connections. This segregation would enable the use of encryption and certificates for external connections where security is paramount and more lightweight security mechanisms for the internal real-time system where speed is prioritized. Additionally, within their proposed secure network for assured power enclaves (where a power enclave consists of multiple microgrids being deployed together), more efficient communications are also utilized to lessen latency impact. Full details of their approach can be found in the full paper [8].

In an article discussing the need for standards adoptions for improving microgrid cybersecurity, the challenge of microgrid operators securing their equipment was discussed [9]. Particularly, the need to adopt cybersecurity standards such as the “UL Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1"; this standard is very relevant for microgrid devices that host advanced communication capabilities [10]. The article also discussed how communication ports of smart home controllers are a weak spot for microgrids; recently, a commercial smart home controller was found to have a vulnerability that the vendor then had to send new firmware downloads to patch.

Lastly, in a report by Accenture, the need for cyber-physical security for microgrids are discussed [11]. The report highlights the vulnerabilities that can stem for increased penetration of monitoring and control capabilities; this includes the usage of basic programmable logic controllers (PLCs) and remote terminal units (RTUs) to mass market components like sophisticated smart meters and in-home displays. To enable a more resilient, secure grid, four principles are proposed to protect critical power infrastructure: 1) harden the microgrid, 2) complete ongoing assessments of interconnection security controls, 3) plan and prepare for disaster recovery, and 4) resource the security strategy [11]. All in all, the report provides best practices to implement as well as useful case studies to demonstrate the critical need for microgrid cybersecurity.

3.1.2. Cyber Resilience Benefits of Microgrids

Switching perspectives, in the article by David Shadle in T&D World, the potential of microgrids aiding general grid cybersecurity is discussed [12]. The article discusses microgrids that are already built with a defense-in-depth approach and/or can undergo cybersecurity hardening, including network segmentation. With these trusted, distributed microgrids, redundant power can be supplied to the bulk power system when a cyber attack or any large disturbance occurs that disrupts generation. This article assumes that cybersecurity defenses are more likely to be considered and built into microgrids, thus rendering them reliable sources of back-up power with greater resiliency to cyber attacks.

This literature review demonstrated the focus on the cybersecurity of individual microgrids, which naturally applies to networked microgrids as well. Network segmentation, more efficient communication protocols, the use of cryptography and certificates, etc. are important features of a hardened, cyber-secure microgrid. However, in this document, we focus on the cybersecurity needs unique to networked microgrids, which has been identified as a gap through this literature review. As touched upon by Mohan et al. in [8], the focus must be extended to microgrid external connections. In the next chapter, vulnerabilities and consequences unique to networked microgrids are discussed.

4. NETWORKED MICROGRID CYBERSECURITY

Microgrid cybersecurity research is an ongoing effort with a thorough body of literature, as discussed in the last chapter. However, networked microgrids have unique characteristics that must also be investigated. Although there is work for developing design tools and restructuring EMSs/DMSs, cybersecurity analysis is lacking for networked operations. This report seeks to fill in that gap and provide a basis for future networked microgrid cybersecurity research.

In Chapter 2, two key networked microgrid actors were identified: microgrid controllers and external connections. Next, we will delve deeper into each of these actors to understand the vulnerabilities and consequences that are threats to networked microgrids.

4.1. Networked Microgrid Vulnerabilities

For networked microgrids, vulnerability analysis of the external connections and devices that enable those connections is needed. In this document, we will not conduct a full vulnerability analysis, but provide an example of the types of vulnerabilities that could arise. For this purpose, we will examine communications over external connections, protocol translators, and microgrid controllers. These communications could stem from operational functions such as inter-microgrid transactions as well as protection schemes (either individual microgrid communication-assisted protection or exchange of protection settings with networked microgrids).

4.1.1. Microgrid Controllers

Microgrid controllers are integral to an operation of an individual microgrid and for networked operation. The controllers are used to balance distributed energy resources and optimize on important factors such as cost. They enable switching between grid-connected and islanded control by automating the microgrid component and macrogrid interconnections.

Communications can occur every 1 s to 100 ms and include protocols such as IEC 61850, Modbus (RS485/TCP/IP), IEC 60870-5-104, OPC, Ethernet, and DNP3 [13]. Overall, microgrid controllers can detect disturbances, such as points out of range, digital state changes, open/close breaker status, and drop time-outs, and implement response to maintain stability. These controllers can be standalone devices or a function within real-time automation controllers (RTACs) [14].

Considering microgrid controllers, either standalone or within an RTAC, the vulnerabilities that should be considered include:

- Open, unused ports
- Software/firmware updating procedure
- Internet/WiFi connection capabilities
- Use of third-party software
- Hardware supply chain

These example vulnerabilities are general for grid end-devices, especially those with additional communication capabilities. These advanced functions enable the microgrid controller to communicate quickly and host processes that would have otherwise been too burdensome (e.g., exchanging pricing information). These added functions can be achieved with third-party software, but without proper security mechanisms and analysis, the third-party software can broaden the vulnerability landscape. For example, the third-party software could include backdoor access or software Trojans, if not properly examined prior to installation (even if end-device is from a trusted source).

Similarily, for the microgrid controller software/firmware upgrade sequence, a secure manner to perform these upgrades must be implemented especially if it requires internet connection. Man-in-the-middle or injection attacks could occur that push malicious upgrades to enable adversary control of the microgrid controller or access to sensitive information. Open, unused ports can also enable adversaries to manipulate the controller configuration and/or eavesdrop. Hardware supply chain compromises should also be considered to protect against hardware-based attacks. Finally, any external devices, such as laptops and USB drives, should meet the same cybersecurity requirements and standards as the microgrids.

4.1.2. Communications over External Connections and Protocol Translators

External connections from the microgrid controller or other microgrid devices are another crucial factor that need to be considered for vulnerability assessment. These connections could include exchange of load setpoints, available generation, protection schemes (for overall coordination), and pricing information; regulatory information for individual microgrids could also be shared to achieve cohesive operation of the networked microgrids that comply with rules on transactions.

Thus, critical information must be communicated over these external connections; to ensure QoS, there is a potential for customer personal identifiable information (PII) to be shared as well. Vulnerabilities that are relevant to consider are:

- Insecure communication protocols
  - Protocols without authentication mechanisms
  - Protocols that can be easily subject to flooding attacks
  - Protocols without built-in encryption capabilities (e.g., Modbus)
- Insecure protocol translators

  - Similar to end-point device vulnerabilities, could include third-party software, open ports, public internet connection, etc.

- Lack of firewalls and intrusion detection/prevention systems at individual microgrids
  - Cannot block or detect malicious communications
- Poor communication network design leading to high latency within external connections
  - Can impede critical information such as protection settings from being communicated in a timely manner

4.2. Networked Microgrid Consequences

There are various vulnerabilities inherent within external connections, protocol translators, and microgrid controllers. These vulnerabilities stem from the low/nonexistent device-level security as well as the use and dependence upon insecure communications. When these vulnerabilities are exploited by adversaries, various cyber-physical consequences can occur. In this section, we focus on the physical consequences that could occur, specific to networked microgrid operation. For more detail on grid cyber-physical consequences, please see [15–18].

One important cyber impact to consider is compromise propagation. For example, if a central microgrid controller is compromised, can the compromise propagate to the independent microgrid controllers? This could be through pushing malicious updates/settings or viruses to the independent microgrid controllers through direct communication channels, especially if connected microgrids have low/non-existent security mechanisms in place. Furthermore, could this spread of cyber compromise in different microgrids then lead to more significant cascading failures? These are critical concerns to mitigate such that resilient operation of the networked microgrids can be achieved.

Physical consequences that could occur in individual microgrids include limit violations and potential instabilities. Furthermore, if the protection system is compromised (whether from blocking communications or causing misoperation), equipment damage could occur from sustained faults. Both instabilities and damage can lead to the loss of service, degrading QoS, and potentially cause cascading impacts through the networked microgrids. Depending on the penetration of networked microgrids, the bulk power system (BPS) may be detrimentally impacted as well.

In fact, when embedded microgrids are considered that also leverage networking but have more interaction with the BPS, unique consequences can arise where both cyber and physical impacts can progress at faster rates and even simultaneously. Microgrid controllers, protocol translators, and external connections live in the intersection of microgrids and/or microgrids and the BPS, their ability to impact multiple systems is increased. Thus, it is critical to secure these essential networked microgrid technologies and ensure both cyber compromise and cyber-physical consequences do not propagate and reduce/eliminate system impact.

In Table 4-1, the example actors unique to networked microgrid operations and the possible vulnerabilities and subsequent consequences for each are presented. These provide an idea of the types of cybersecurity concerns to consider for networked microgrids. In the next chapter, potential cybersecurity solutions are discussed to mitigate some of these risks as well as identification of future research needs.

Table 4-1. Example networked microgrid data exchange actors and associated vulnerabilities and consequences.

Networked Microgrids				
Actor	**Description**	**Network Connection**	**Vulnerabilities**	**Physical Consequences**
Independent microgrid controller	Enables networking of individual microgrids (e.g., energizing conductors to achieve control layer connection)	EMS or distributed energy resource management system (DERMS) can monitor data and dynamically change setpoints	Open, unused ports; update procedure; WiFi connection; third-party software	Loss of stability; limit violations; equipment damage; loss of service, low QoS
Central microgrid controller	Coordinates objectives and functions of networked microgrids for cohesive operation	EMS or DERMS can monitor data and dynamically change setpoints	Open, unused ports; update procedure; WiFi connection; third-party software	Loss of stability; limit violations; equipment damage; loss of service, low QoS; compromise of independent microgrid controllers; compromise of BPS
Protocol translator	Enables inter-microgrid communications	Intercepts all incoming and outgoing communications from connected microgrid and translates when necessary (if protocol supported)	Open, unused ports; update procedure; WiFi connection; third-party software	Loss of stability; limit violations; equipment damage; loss of service, low QoS
External connections	Allows pricing information to be securely exchanged between microgrids; enables protection coordination; shares regulatory policies and rules	Sends and receives information from connected microgrid EMS or DMS	Insecure communications; lack of firewalls; high latency	Unsuccessful networking of microgrids; loss of protection capabilities; loss of stability; limit violations; equipment damage; loss of service, low QoS

4.3. Use Case Examples

To demonstrate how networked microgrid vulnerabilities and consequences can vary significantly depending on implementation, we can explore two use case examples. It is important to assess the trade-offs between operation and security and find a balance most suitable for different use cases and specific needs. The following two use cases are very simple but exemplify this trade-off.

4.3.1. Use Case 1

Consider two microgrids that have been networked together; full communication and control capabilities between the two has been enabled between the two systems.

In this case, the operational benefits are:

- Flexible operation of the networked microgrids with ability to adjust connected system's generation and load setpoints
- Increased reliability and resilience to sudden changes/outages with full control of two systems
- Straightforward protection coordination with direct communication and ability to control connected microgrid's protection devices

However, the vulnerabilities and consequences that would result from this implementation could include:

- Compromise of one independent microgrid's controller could propagate compromise to the connected microgrid's devices (including control and protection)
- Compromise of one independent microgrid's controller could negatively impact the operation of the connected microgrid; could cause more significant limit violations, greater potential for equipment damage, and loss of stability concerns
- Compromise could lead to loss of protection capabilities of both microgrids
- Since compromise/impact is not isolated, lower QoS that could lead to more customers affected/outaged
- Since compromise/impact is not isolated, greater potential for detrimental impact on BPS

4.3.2. Use Case 2

Consider two microgrids that have been networked together; a subset of communication and control capabilities between the two has been enabled between the two systems. Restricted capabilities could include no access to the other microgrid's protection system and no control capabilities over certain critical generation sources.

In this case, the operational impact is:

- Less flexible operation of the networked microgrids, more coordination is needed between the microgrids to properly adjust generation and load setpoints to satisfy both system needs
- May not be able to respond as quickly to sudden changes/outages, reduced reliability and resilience for fast-acting events
- More complicated protection coordination that may require more sophisticated analysis to ensure adequate protection of networked system

However, the vulnerabilities and consequences that would result from this implementation could include:

- Compromise of one independent microgrid's controller would only impact one microgrid and would not affect the operation of the other
- The uncompromised microgrid would have to adjust operation and protection functions/settings to ensure continued, stable operation
- Limit violations and loss of stability concerns may arise for compromised system but uncompromised microgrid may be able to reduce impact to BPS and overall stability

5. POTENTIAL CYBERSECURITY SOLUTIONS AND RECOMMENDATIONS

Networked microgrids have unique cybersecurity challenges that must be addressed to prevent cascading impacts, both cyber and physical. There are various levels of cybersecurity mechanisms that can be implemented to improve the resilience of the networked microgrid operation, from incorporating simple cyber hygeine principles to innovative R&D solutions specific to networked microgrids. In this section, an example of cyber hygiene principles microgrid operators can implement to help secure networked operation, ideas on how cybersecurity can be integrated in the design phase using tools such as RONM, and future directions for more sophisticated networked microgrid cybersecurity R&D solutions.

5.1. Cyber Hygiene Principles

Cyber hygiene and best practices can often be exchangeable phrases that essentially focus on what type of policy and configuration changes an individual/organization make with the technologies and system they have currently to improve cybersecurity. This topic has been heavily explored in general industrial control system (ICS) literature and the recommendations are very applicable to the electric grid, including networked microgrids. One useful resource is from the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) that discusses cybersecurity best practices for industrial control systems [19]. The topics covered include: risk management and cybersecurity governance, physical security, ICS network architecture, ICS network perimeter security, host security, security monitoring, supply chain management, and human elements.

Each of these topic areas provide recommendations to increase the system cybersecurity in a proactive manner [19]. A useful checklist for cyber hygiene is:

1. Check, prioritize, test, and implement ICS security patches
2. Backup system data and configurations
3. Identify, minimize, and secure all network connections to ICS
4. Continually monitor and assess the security of ICS, networks, and interconnections
5. Disable unnecessary services, ports, and protocols
6. Enable available security features and implement robust configuration management practices
7. Leverage both application whitelisting and antivirus software

8. Provide ICS cybersecurity training for all operators and administrators
9. Maintain and test an incident response plan
10. Implement a risk-based defense-in-depth approach to securing ICS hosts and networks
11. Implement deny-by-default firewall policy
12. Include multi-factor authentication when possible

This checklist is a useful way to check that best practices are/can be implemented in a networked microgrid system. As echoed in Chapter 2, much of the microgrid cybersecurity literature has focused on network segmentation techniques and monitoring and assessing the system design. However, it is also critical to focus on operator/adminstrator training and the general human element. Another large focus is on performing risk analysis and planning response/capabilities in advance to increase resilience and understand both short-term and long-term impacts. CISA also provides more in-depth recommended practices for updating antivirus, creating a cyber forensics plan, securing control system modems, etc. on their website [20]. Further information related to the electric grid cybersecurity can be found in the DOE Office of Cybersecurity, Energy Security, and Emergency Response website [21].

DER specific recommendations and discussion of existing guidelines and standards in provided in the Sandia National Laboratories report “Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators" [15]. Introduction to cybersecurity principles, confidentiality, integrity, and availability, are provided and how each can be obtained with different security design techniques and defense tools. These techniques and tools include encryption, secure key storage, utilizing secure communication protocols, intrusion detection systems (IDSs), access controls, etc. Recommendations to improve security of different communication protocols (e.g., Modbus, IEC 61850) are provided as well as recommendations for grid operators and aggregators specifically.

Both ICS and DER cyber hygiene recommendations are very relevant for improving the cybersecurity of networked microgrids. Some general recommendations are listed below:

- **Perform risk analysis of microgrid controllers, protocol translators, and other networked microgrid devices; implement best practices before installation and continually assess**
  - Disable unused services, ports, and protocols
  - Inspect criticality of controller resources and how limited resources can be improved
  - Routinely check for tampering of firmware (e.g., check hash message authentication code (HMAC))
  - Define firmware/software updating procedure clearly, utilize integrity checks when possible
  - Require access controls for modifications to controller configuration and setting changes; practice principle of least privilege

  - Enforce strong password policies: require change from default password and do not store or transfer passwords in plain text
  - Include secure boot when possible to validate the initial state of each system is in a secure or known state (e.g., using a trusted platform module (TPM) chip)

- **Implement secure network architecture principles at the design stage and assess all external connection risks and impacts; implement best practices before enabling connection and continually assess**
  - Enable traffic and resource usage monitoring over external connections for network analysis and/or use within IDSs; keep logs such as user logins, information requests, commands, and measurements
  - Implement secure network architecture in the design stage, using network segementation techniques and firewalls
  - Assess time constraints: ensure data rate and latency constraints for time sensitive exchanges
  - Use encryption or lightweight encryption where appropriate (e.g., customer PII, pricing information, critical control settings)
  - Require credentials for different microgrids to initiate external connection for networked operation
  - Implement access controls for any network/connection configuration changes; use multi-factor authentication when possible

5.2. Incorporating Cybersecurity in Networked Microgrid Design

As a general principle, integrating cybersecurity from the beginning is recommended; additional assessments should be performed through out the system lifespan to ensure proper functionality and add further security layers if needed. All in all, a defense-in-depth approach with multiple layers of security is an efficient approach. Thus, it is important to consider networked microgrid cybersecurity in the first layer, the planning stage.

In the related project this report is a part of, a networked microgrid design tool is being developed called RONM, as discussed in Chapter 1. For the protection design between connected microgrids, an optimization algorithm has been developed to coordinate relays within connected microgrids. This optimization algorithm is subject to various power system constraints; these constraints provide a unique opportunity to incorporate cybersecurity principles within the design tool.

Although not all essential cybersecurity principles, even the simple cyber hygiene presented in the previous chapter, can be represented as an optimization algorithm constraint, even a few cybersecurity-oriented constraints can greatly improve secure networked microgrid design.

Specifically, network architecture security can be improved, as highlighted as a critical need in the literature review presented in Chapter 3.

Some cybersecurity-oriented constraints to include in the RONM methodology could include:

- Enforcing uni- or bi-directional communications from certain grid components
    - Utility to microgrid could be uni-directional, microgrid to microgrid bi-directional
    - Microgrid to DERs uni-directional, DER to DER bi-directional
- Restricting number of communication paths from specific grid components
    - No communication between one microgrid's controller and connected microgrid's relays
    - Microgrid controller can only have certain number of external connections (to ensure unplanned connections are not made)
- Implementing dispatch limits for different sources of generation to indicate when abnormal behavior is occurring (e.g., control setpoints sent to generation sources continually aim to violate dispatch limits)

The main requirement for incorporating these constraints is the ability to represent them in terms of a numerical bound as well as a connectivity model of the communication network. Furthermore, implementation within a software defined networking (SDN) platform could be explored for deployment Other essential cybersecurity principles, such as disabling unneeded, open ports, the use of secure communication protocols, and enabling post-event analysis logging may need to be incorporated as a part of the design assumptions or as a checklist in the RONM tool, as discussed in the previous section. However, these capabilities may require a more detailed, fine-granularity model of the communication network. Lastly, additional rules should also be developed specific to networked microgrid operation, these could include:

- An independent microgrid controller of one microgrid should not be able to control the protective relays of a connected, separate microgrid and vice versa
- Backup protection schemes for networked microgrid protection should be available to enable continued operation despite disturbances or failure of protection coordination

The above two points are examples of networked microgrid specific rules that can vary depending on operator and aggregator policies. Nonetheless, networked microgrid cybersecurity should be assessed from multiple perspectives (from both cyber- and physical-sides) and a defense-in-depth approach should be implemented.

5.3. Future Networked Microgrid Cybersecurity R&D Directions

The last two sections discuss cyber hygiene principles that can be implemented immediately for networked microgrids and ideas for incorporating cybersecurity-oriented constraints in design tools. However, for comprehensive security, further R&D is needed for more powerful solutions. Specifically, solutions that incorporate both cyber and physical characteristics of the networked microgrids are important.

Recent grid cybersecurity research has focused on combining features from both the communication network and the power system, such as for DER IDSs and cyber-physical EMSs [16, 22]. It is important to correlate physical power system data with collected cyber data for increased situational awareness. It is not sufficient to utilize purely enterprise network-designed security tools for ICS such as microgrids. For networked microgrids, solutions that incorporate the physical system data are needed and any unique characteristics of the networked operations.

For networked microgrids, pricing exchanges through a trusted transactions system are essential between different microgrids. However, to enable the trusted transaction system, encryption may be needed. Depending on the speed of data exchange needed, lightweight encryption may need to be explored as well; another challenge is secure key storage between multiple microgrid entities. Blockchain could also be studied to faciliate pricing exchanges [23, 24]. Additionally, the use of TPM for secure key storage can also be explored. Thus, one future R&D idea involves **the design and implementation of encryption and secure key storage for networked microgrids**.

Another area that needs further investigation is improving the security of microgrid controllers, as networked operation is dependent on them. Full risk analysis, mitigation strategies, and testing is needed of these microgrid controllers, especially when multiple are involved. Such an effort may **involve standardizing microgrid controller design, developing a cybersecurity test procedure for such controllers, and/or requiring controller certificates**. For the use of certificates, a certificate management system including a certificate authority would have to be developed to meet the needs of networked microgrids.

When networking independent microgrids, it is also important to consider changing access controls. Individual grid operators may have full access to their own microgrids but may need some level of access to a connected microgrid's to obtain smooth operation. However, it is important **to assess what level of access is needed and how dynamic access controls can be assigned depending on network configuration and participants involved** (e.g., utility-owned vs. private microgrids). Additionally, proactive/reactive reconfiguration techniques for networked microgrid components (e.g., protection devices) for responding to compromise and other events can be explored for this dynamic analysis.

These are just a few examples of the types of R&D that are still needed for future enhancements of networked microgrid cybersecurity. Although many purely cyber tools and microgrid network architecture recommendations exist, more development is needed for solutions specific to networked microgrids. By studying the characteristics that make networked microgrids unique and understanding the type of cyber-physical interactions within them, a stronger, more resilient, and cyber-secure design and operation can be achieved.

6. NEXT STEPS AND CONCLUSIONS

In this report, data exchanges and functions unique to networked microgrids were discussed and the potential vulnerabilities and consequences that could arise if effective cybersecurity defense were not implemented. Cyber hygiene or best practice recommendations were provided that could be broadly applied as well as examples of how cybersecurity could be incorporated into the planning and design stage (in the form of optimization constraints). Lastly, future directions for networked microgrid cybersecurity were provided to work toward an improved and resilient networked microgrid cybersecurity posture.

Networked microgrids have the potential to significantly improve overall grid resilience and reliability. To ensure the added reliance on microgrid controllers and external connections do not increase the vulnerability landscape, it is pertinent to assess and continually reassess cybersecurity. This report seeks to serve as a basis for beginning that assessment, implementing best practices, and working towards innovative, future solutions.

REFERENCES

[1] S. N. Backhaus, L. Dobriansky, S. Glover, C. Liu, P. Looney, S. Mashayekh, A. Pratt, K. Schneider, M. Stadler, M. Stark, J. Wang, and M. Yue, “Networked microgrids scoping study,” Los Alamos National Laboratory, Tech. Rep., 2016.

[2] J. Stamp, C. K. Veitch, J. Henry, D. H. Hart, and B. Richardson, “Microgrid cyber security reference architecture (v2),” Sandia National Laboratories, Tech. Rep., 2015.

[3] J. Eddy, N. E. Miner, and J. Stamp, “Sandia’s microgrid design toolkit,” *The Electricity Journal*, vol. 30, no. 4, pp. 62 – 67, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1040619017300544

[4] S. Hossain-McKenzie, M. J. Reno, J. P. Eddy, and K. P. Schneider, “Assessment of existing capabilities and future needs for designing networked microgrids,” Sandia National Laboratories, Tech. Rep., 2019.

[5] K. P. Schneider, H. Nagarajan, A. Pratt, M. J. Reno, B. Ollis, F. Tuffner, S. P. Nandanoori, S. Kundu, W. Du, H. Hijazi, R. Jain, F. Flores-Espino, J. Hambrick, and D. Ton, “Preliminary design process for networked microgrids,” Pacific Northwest National Laboratories, Tech. Rep., 2020.

[6] S. Hossain-McKenzie, M. J. Reno, J. Quiroz, P. Schulz, A. Summers, and C. Carter, “Cyber security issues and solutions for protective relaying and local monitoring,” Sandia National Laboratories, Tech. Rep. SAND2018-0406, 2018.

[7] Z. Wang, B. Chen, J. Wang, and J. kim, “Decentralized energy management system for networked microgrids in grid-connected and islanded modes,” *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 1097–1105, 2016.

[8] A. Mohan, G. Brainard, H. Khurana, and S. Fischer, “A cyber security architecture for microgrid deployments,” 03 2015, pp. 245–259.

[9] C. W. Thurston, “Microgrid cybersecurity tightens with standards adoption,” *CleanTechnica*, 2018.

[10] “Standard for software cybersecurity for network-connectable products, part 1: General requirements,” UL Standard, Tech. Rep., 2020. [Online]. Available: https://standardscatalog.ul.com/ProductDetail.aspx?productId=UL2900-1

[11] “Cyber-physical security for the microgrid: new perspectives to protect critical power infrastructure,” *Accenture*, 2016.

[12] D. Shadle, "Can microgrids help improve our cybersecurity?" *T&D World*, 2020. [Online]. Available: https://www.tdworld.com/smart-utility/grid-security/article/21120095/can-microgrids-help-improve-our-cybersecurity

[13] Emerson, "OvationTM Microgrid Control," Online. [Online]. Available: https://www.emerson.com/documents/automation/microgrid-control-system-en-1263362.pdf

[14] Schweitzer Engineering Laboratories, "SEL-3555 Real-Time Automation Controller (RTAC)," Online. [Online]. Available: https://selinc.com/products/3555/

[15] C. Lai, N. Jacobs, S. Hossain-McKenzie, P. Cordeiro, O. Onunkwo, and J. Johnson, "Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators," Sandia National Laboratories, Sandia Report SAND2017-13113, Dec. 2017.

[16] A. Chavez, C. Lai, N. Jacobs, S. Hossain-McKenzie, C. B. Jones, J. Johnson, and A. Summers, "Hybrid Intrusion Detection System Design for Distributed Energy Resource Systems," in *2019 IEEE CyberPELS (CyberPELS)*, 2019, pp. 1–6.

[17] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, "SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1790–1799, 2012.

[18] N. Jacobs, S. Hossain-McKenzie, A. Summers, C. B. Jones, B. Wright, and A. Chavez, "Cyber-Physical Observability for the Electric Grid," in *2020 IEEE Texas Power and Energy Conference (TPEC)*, 2020, pp. 1–6.

[19] Cybersecurity and Infrastructure Security Agency, "Recommended Cybersecurity Practices for Industrial Control Systems," Online. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

[20] ——, "Recommended practices," 2020. [Online]. Available: https://us-cert.cisa.gov/ics/Recommended-Practices

[21] Department of Energy, "Office of Cybersecurity, Energy, Security, and Emergency Response," 2020. [Online]. Available: https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response

[22] Texas A&M University, "Deep cyber physical situtational awareness for energy systems: A secure foundation for next-generation energy management," 2020. [Online]. Available: https://cypres.engr.tamu.edu/

[23] D. Sikeridis, A. Bidram, M. Devetsikiotis, and M. J. Reno, "A blockchain-based mechanism for secure data exchange in smart grid protection systems," in *2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC)*, 2020, pp. 1–6.

[24] K. Mannaro, A. Pinna, and M. Marchesi, "Crypto-trading: Blockchain-oriented energy market," in *2017 AEIT International Annual Conference*, 2017, pp. 1–5.

DISTRIBUTION

Email—Internal (encrypt for OUO)

Name	Org.	Sandia Email Address
Technical Library	01177	libref@sandia.gov