Implementing Cyber Security Requirements and Mechanisms in Microgrids

Apurva Mohan, Himanshu Khurana

Chapter 14

IMPLEMENTING CYBER SECURITY REQUIREMENTS AND MECHANISMS IN MICROGRIDS

Apurva Mohan and Himanshu Khurana

Abstract A microgrid is a collection of distributed energy resources, storage and loads under common coordination and control that provides a single functional interface to enable its management as a single unit. Microgrids provide several advantages such as power quality control, uninterrupted power supply and integration of renewable resources. However, microgrids are increasingly connected to the Internet for remote control and management, which makes them susceptible to cyber attacks. To address this issue, several pilot deployments have implemented bolt-on security mechanisms, typically focused on securing the protocols used in microgrids. Unfortunately, these solutions are inadequate because they fail to address some important cyber security requirements.

This chapter describes the μGridSec methodology, which is intended to provide comprehensive cyber security solutions for microgrid deployments. First, cyber security requirements are derived from relevant industry standards and by studying pilot microgrid deployments. Next, the μGridSec methodology is applied to ensure that appropriate mechanisms are applied to microgrid architectures to meet the cyber security requirements. Finally, a high-level threat model for a representative microgrid architecture is used to identify security threats and demonstrate how μGridSec can address the threats.

Keywords: Microgrids, cyber security, NERC-CIP standards, threat modeling

1. Introduction

A microgrid is a collection of local electricity generation and energy storage systems, and electrical loads that are under common coordination and control. Although a microgrid consists of multiple entities, it can be controlled as if it were a single entity. The integration of distributed energy resources (DERs), storage and loads increases the efficiency of the entire system. It also makes it

possible to connect multiple microgrids to create a "power enclave" with high voltage capacity [21]. A single microgrid can function in the "grid connected" mode in which the microgrid is connected to the main power grid and jointly provides power. Alternatively, a microgrid can operate in the "islanded" mode where the microgrid functions autonomously as a self-contained system that provides power to a local site.

Microgrids offer advantages such as enhanced power quality via voltage sag correction, increased power factors, enhanced reliability for critical loads, greater energy security, higher local power distribution efficiency due to shorter distances, better sustainability by integrating renewable resources and clean fuel sources, and the potential for greater physical and cyber security. Due to these advantages, microgrids are being hailed as critical components of future energy systems. Microgrids are in operation around the world and the adoption and deployment of microgrids is increasing [18].

Microgrids are currently deployed at a variety of organizations, including university campuses, military bases, hospitals, residential communities and rural areas. They provide energy security and constitute an important part of the critical energy infrastructure. At sensitive sites such as military bases, hospitals and safety-critical facilities, it is vital to ensure that the power supply is not disrupted by adversaries. For example, a military base may rely on a microgrid for uninterrupted power supply during periods of grid downtime or grid peak loads, and its operational capability can be significantly affected by physical or cyber attacks on the microgrid. This chapter focuses on the cyber security of microgrids; securing microgrids from physical attacks is outside the scope of this work.

This chapter formulates cyber security requirements for microgrids. Some of the relevant standards that can be used to derive smart grid cyber security requirements are: NIST IR 7628 [19], NERC-CIP-002 to CIP-009 [14], NIST 800-53 [12], NIST 800-82 [20], ISO 27002 [7] and the Department of Homeland Security (DHS) Catalog of Control Systems Security [3]. In this chapter, the NERC-CIP Standards CIP-002-1 through CIP-009-2 [14] are used to derive the cyber security requirements. Although the NERC-CIP standards are widely used in the bulk electricity generation infrastructure and are not directly applicable to microgrids, they are, nevertheless, among the most relevant standards for electrical systems. Additional cyber security requirements are derived by considering microgrid pilot project deployments [18]. This chapter presents the μGridSec methodology, which ensures that appropriate mechanisms are applied to microgrid architectures to meet the cyber security requirements. A high-level threat model for a representative microgrid architecture is used to identify security threats and demonstrate how μGridSec can address the threats.

2. Security Requirements for Microgrids

This section articulates the cyber security requirements for microgrids. The requirements are derived from the North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC-CIP) Standards CIP-002-1

through CIP-009-2 [14] and from pilot microgrid deployments [18]. Note that the NERC-CIP requirements are formally defined for electric power infrastructure assets such as utilities, but they are re-interpreted for microgrids in this work. In particular, each requirement was formally analyzed and applied to a microgrid environment. A number of NERC-CIP requirements are administrative in nature and only the technical requirements are considered in this work. An analysis of pilot microgrid deployments revealed that the NERC-CIP requirements do not completely cover the cyber security requirements for microgrids. To address this gap, additional cyber security requirements for microgrids were formulated by studying some pilot microgrid deployments [18].

The enhanced set of cyber security requirements for microgrids includes:

1. **Critical Asset Identification:** The critical assets related to microgrid operations and communications should be identified. This is done to ensure adequate protection of critical assets.

2. **Cyber Vulnerability Assessment:** Cyber vulnerability assessments should be performed for: (i) electronic access points; (ii) electronic security perimeters; and (iii) critical assets. A comprehensive architectural risk analysis should be performed to identify the cyber security threats in the architecture and the security controls to address the threats.

3. **Electronic Security Perimeter:** Every critical cyber asset should be within the electronic security perimeter.

4. **Identity Management:** The microgrid system should provide digital identity management to all internal and external entities. This is important for all communications, coordination and control activities in a single microgrid and when multiple microgrids interact.

5. **Access Control:** Appropriate access control should be enforced to mediate access to: (i) all critical assets; and (ii) all electronic access points at the perimeter. This includes the implementation of secure authentication mechanisms.

6. **Information Protection:** Appropriate measures should be taken to identify, classify and protect sensitive information associated with microgrid operations and communications.

7. **Anomaly Detection:** Remote entities should be allowed to perform only a well-defined set of actions associated with their accounts or roles. The sets of actions may be further broken down into sequences of commands that can be executed by remote entities. Any deviation from a sequence should be rejected and the anomaly should be logged.

8. **Critical Asset Protection:** Critical assets should be identified and protected from damage due to the actions of remote entities. The mechanisms should work in conjunction with the safety features of the identified critical assets.

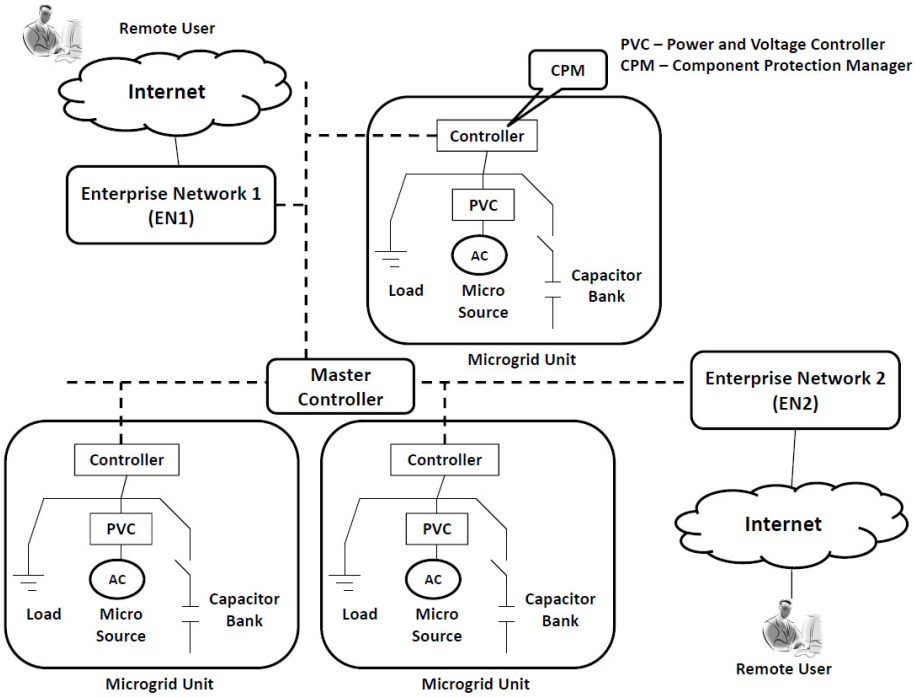

Figure 1. Architecture with coupled microgrids.

3. μGridSec Methodology

This section discusses some representative microgrid architectures and provides details about their operation along with their information and communication components. Following this, the μGridSec methodology is described in detail.

3.1 Information and Communications

Figures 1 and 2 show two microgrid architectures. Figure 1 shows an architecture where multiple microgrids are coupled together in a large deployment. Figure 2 shows a microgrid bank with multiple microgrid campuses connected together to create an energy farm along the lines of the architecture proposed in [2]. These large and complex deployments are considered because the proposed methodology is intended to cover the security requirements for large, complex, current and future architectures.

Figure 1 shows a large deployment with multiple microgrids coupled together to meet the demands of a large campus. EN1 and EN2 are enterprise networks that provide electronic entry points to the microgrid. EN1 and EN2 are connected to the Internet and host a range of enterprise services for campus users.

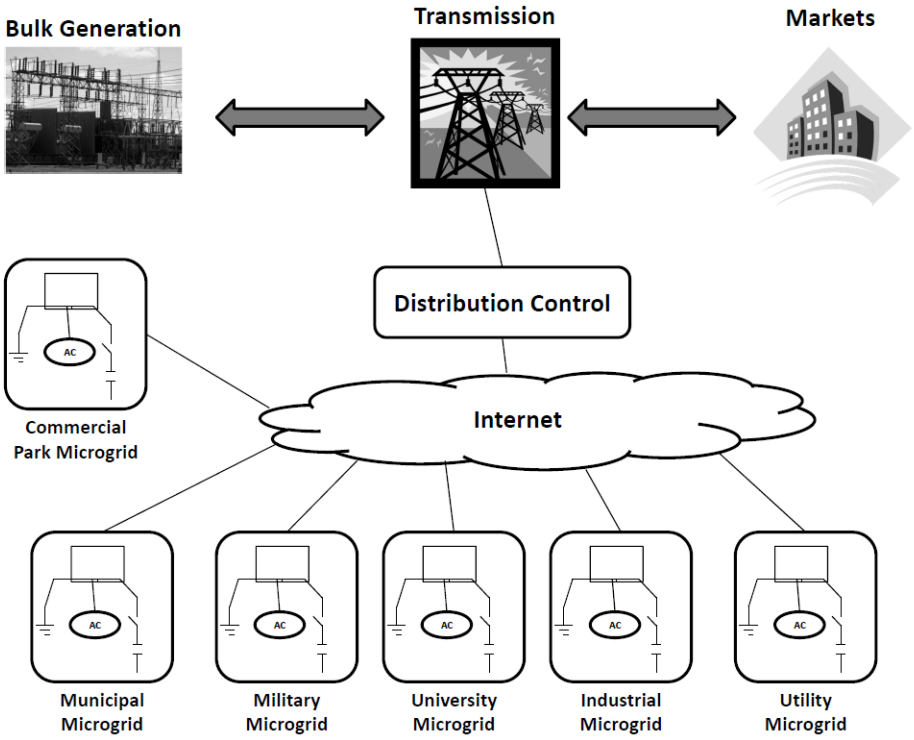

Figure 2. Architecture with an energy bank comprising independent microgrids.

They also host control centers that enable users such as operators, technicians and administrators to control and manage the microgrids. The microgrids have two types of connections: (i) electrical wires for power flow; and (ii) network cables for communications and control. The network cables, which connect the microgrid controllers (Figure 1), typically use smart grid protocols such as DNP3 or IEC 61850. Information flowing along the channels is rarely encrypted and access control mechanisms are rarely used to access information and resources in the microgrids. The enterprise networks host control centers, which typically implement weak or no authentication mechanisms. The controllers execute the commands they receive without any authentication and a requestor can see information or access any component without any access control checks.

Figure 2 shows a futuristic energy farm in which multiple microgrid deployments coordinate to supply power to a utility by connecting to its distribution system. At this time, several technical limitations exist related to the power engineering aspects of such a deployment; however, research efforts are underway to address the challenges. The microgrids in Figure 2 connect to each other and to the utility distribution system using electrical wires for power flow and

network cables for communications and control. Since microgrid based energy farms are not deployed as yet, an initial architecture is expected to be developed to meet the cyber security requirements.

3.2 μGridSec Components and Details

μGridSec is a methodology for providing comprehensive cyber security to microgrids. It incorporates security processes and mechanisms to meet the cyber security requirements identified in Section 2. The μGridSec methodology involves the four main steps described below.

Step 1: Refinement of High-Level Requirements. The first step considers the high-level cyber security requirements derived from industry standards and pilot deployments and breaks them down into low-level requirements for specific microgrid deployments. The security mechanisms needed to secure a microgrid deployment depend on the characteristics of the specific site and, hence, breaking down the requirements into low-level requirements based on the deployment environment helps select the right security mechanisms.

Step 2: Detailed Risk Analysis via Threat Modeling. The second step conducts an architectural cyber security risk analysis using threat modeling. The goal is to identify the security threats that the microgrid architecture faces and to select the appropriate security controls. In μGridSec, the threat modeling process is also used to identify the critical cyber assets in the architecture. Threat modeling is then performed on the critical cyber assets to identify the threats and vulnerabilities in the architecture that an adversary can exploit to attack the system. Finally, security controls are selected and implemented to effectively address the security threats and vulnerabilities. Threat modeling can be performed using the Microsoft SDL tool [9] or other popular threat modeling tools. The next section presents a threat modeling process assuming that the SDL tool is used to achieve Requirements 1 and 2 listed in Section 2.

Threat modeling involves the following steps:

- Identify the main components responsible for microgrid operation and communications. For example, in Figure 1, the components are the power generation resources, storage and loads. The communications and control components are the controllers, communications channels and master controller. These components can be modeled using a threat modeling tool such as SDL [9].

- Draw the trust boundaries. Boundaries are drawn for the security zones and conduits model, which creates trust zones in the system architecture that communicate through channels called conduits.

- Execute the threat modeling tool and work on the STRIDE questions that explore the security threats in the architecture. The STRIDE threat

model was developed by Microsoft to help categorize security threats. STRIDE refers to six threat categories: (i) spoofing; (ii) tampering; (iii) repudiation; (iv) information disclosure; (v) denial of service; and (vi) privilege escalation.

- (Optional) Prioritize the threats using the CVSS2 system [13].

- Select security controls that address the identified threats. Standards such as NIST SP 800-53 [12], NIST SP 800-82 [20] and ISA-99 [6] can be used to select the appropriate security controls.

Step 3: Information Protection Mechanisms. The third step in the μGridSec methodology defines security mechanisms for information protection. These mechanisms, which help comply with Requirements 3 through 6, protect information in transit and at rest, and implement network security, identity management, and authentication and access control to secure information and critical assets.

The first mechanism defines the trust domains in the architecture. The zones in Figure 1 represent different trust domains. Each trust domain is protected by systems such as firewalls and access control lists. The level of perimeter protection depends on the level of trust associated with each domain. For example, in Figure 1, each microgrid is at the same trust level, therefore, some access-control-list-based perimeter protection should suffice. For conduits that connect microgrid trust domains to the enterprise network, firewalls with advanced capabilities are recommended. This architecture provides a layered approach with strong perimeter protection and additional layers of protection within the main perimeter.

The second mechanism enforces strong authentication and access control in a microgrid system. Strong authentication is enforced for users who access information and/or resources. Several authentication technologies can be used as outlined in NIST SP 800-53 [12]. Role-based access control [17] is recommended for access control. Since a small number of roles exist in microgrid systems, the management of access control policies would be efficient and less prone to errors. Authenticated subjects are mapped to one or multiple roles. The access control policy defines each role and its level of access to the information and microgrid components.

The third mechanism protects information at rest and in transit. μGridSec engages standard cryptographic mechanisms to protect information. The networks are protected using TLS 1.2 for channel encryption and AES-256 for message encryption; AES-256 is used to encrypt all data at rest. Messages incorporate sequence numbers to guarantee message freshness. Public-key certificates based on the X.509 v3 standard are used; depending on the deployment, the certificates are either self-signed or certificate-authority-provided. Certificate management and key management are performed according to best practices [1]. Digital signatures can be used optionally for messages to ensure non-repudiation. The ability to affix and verify digital signatures is provided,

but is not mandatory. Also, hash message authentication codes may be used to provide message authenticity at the application level.

The fourth and final mechanism provides digital identity management in μGridSec. Each component that is addressable by a communication has a unique identity in a microgrid and the corresponding mapping is stored in a database. Each microgrid has a unique identifier that is appended to the component identity in the case of multiple connected microgrids to resolve namespace clashes. The database also contains other information about microgrid components that might aid in providing identity management services.

Step 4: Anomaly Detection and Component Protection Mechanisms. The fourth and final step of the methodology provides anomaly detection and microgrid component protection. This involves two phases. In the first phase, μGridSec proposes command validation such that only validated commands can be executed on critical assets. This functionality can be achieved by command whitelisting. The access control engine can perform whitelist checking or a commercial whitelisting product may be integrated with μGridSec to assist with command whitelisting. Whitelisting of commands can be performed per role to enhance its effectiveness. The access control engine can also track entities (and roles) that repeatedly send commands that are prohibited and raise alarms. Logs should be analyzed to identify entities that display erroneous or potentially malicious behavior.

In the second phase, the component protection manager (CPM), which is inside the controller, communicates with the power and voltage controller (PVC) (Figure 1). A command to a microsource is executed only after the power and voltage controller verifies that it does not violate the safety limits of the microsource. The component protection manager along with the whitelist manager in the access control engine ensure that the setpoints of the power and voltage controller are not modified by unauthorized entities. These two steps guarantee the integrity of setpoints and that microsources are not damaged by adversaries who execute arbitrary commands on the microsources.

4. Implementing μGridSec

This section discusses some widely-available commercial and open-source technologies that can be used to implement the security controls listed above.

Threat modeling for a microgrid architecture can be performed using a manual approach or an automated tool. The popular Microsoft SDL tool [9] may be used for modeling the threats to a microgrid architecture or system.

μGridSec recommends the use of network firewalls for perimeter protection. Several vendors provide network firewalls with advanced features that can be used for microgrid deployments. While it is important to find the right vendor to meet the deployment requirements, it is even more important to maintain secure configurations of the firewalls. Most firewalls allow remote configuration and maintenance by administrators; this feature should be protected very carefully if it is employed.

Authentication and access control are two other features that can be deployed using a combination of commercial technologies and custom implementation. Authentication is supported by protocols such as IEC 62351 [5] and OLE for Process Control Unified Architecture (OPC UA) [15]. Standard username-password based authentication is provided by these protocols. Secure authentication can be implemented for privileged users such as administrators via two-factor authentication mechanisms. The second factor can be implemented using a commercial solution.

Access control should be implemented on microgrid devices and in the network. In the case of microgrid devices, access control lists on Linux platforms can be leveraged to provide fine-grained access control to resources and operations. In the case of a network, role-based access control may be implemented to provide strong access control. One solution is OpenRBAC, an open-source implementation of the ANSI/INCITS Standard 359-2004 (Role Based Access Control) [4]. This solution is flexible, configurable and easily integrated into microgrid networks.

μGridSec proposes TLS 1.2 for channel protection and AES-256 for message protection. The popular OpenSSL library [16] may be integrated in a microgrid system to provide TLS 1.2 and AES-256 mechanisms.

Finally, command validation may be implemented via command whitelisting. This can be performed by custom software integrated with the access control engine or by a commercial whitelisting product. Whitelisting of commands can be performed per role to enhance its effectiveness. Command validation provides protection from command injection attacks and also limits the invocation of sensitive executables to certain roles.

5. Cyber Security Requirements

This section revisits the cyber security requirements laid out in Section 2 and discusses how they are met by different μGridSec components.

1. **Critical Asset Identification:** This requirement is met by the threat modeling process in μGridSec, where the first step is to identify the critical assets in a microgrid.

2. **Cyber Vulnerability Assessment:** This requirement is also met by the threat modeling process in μGridSec, where the potential cyber vulnerabilities and threats are identified in a microgrid architecture after the critical assets have been identified. The vulnerability assessment is performed using the SDL tool, which engages an attack library based on the STRIDE model.

3. **Electronic Security Perimeter:** A strong electronic security perimeter is built into a microgrid system using external firewalls with advanced features and secure configurations. Additionally, trust domains are created within the perimeter for additional defense. The internal trust domain boundaries can be based on access control lists.

4. **Identity Management:** The digital identity of each resource in a microgrid is stored in a database and is used whenever the resource is referred to by a communications or control message. When multiple microgrids are integrated in a microgrid bank, the domain name of a specific microgrid is appended before an asset name to avoid namespace clashes. This identity is used as the primary username by the authentication mechanism.

5. **Access Control:** Strong authentication and access control are enforced in a microgrid system. Role-based access control is prescribed for accessing all sensitive information and critical physical assets.

6. **Information Protection and Authenticity:** Strong mechanisms are in place to protect sensitive information in transit or at rest. μGridSec uses a combination of standard symmetric and asymmetric cryptographic algorithms such as AES-256 and ECC/RSA with strong key management to provide the required functionality. Hash message authentication codes are proposed to ensure message-level authenticity and digital signatures are used to achieve non-repudiation. A public-key infrastructure is employed to enable trust based on digital signatures.

7. **Anomaly Detection:** Anomaly detection is implemented at the command interface based on whitelisting. The whitelist is manually populated by the administrator and is used to verify that each role is only allowed to execute authorized commands. An anomaly is reported if a role attempts to execute unauthorized commands repeatedly.

8. **Critical Asset Protection:** A component protection manager is implemented on controllers. The component protection manager ensures the integrity of setpoints in power and voltage controllers and that the safety limits of microsources are not violated. The component protection manager and access control lists prevent unauthorized access to configuration and safety data, and, even in the case of authorized access, ensure that the safety limits of the microsources are not violated.

6. Threat Model

This section presents a cyber security threat model for the microgrid architectures presented in Figures 1 and 2. The threats are divided into seven categories. The manner in which μGridSec protects a microgrid against each of the identified threat categories is also discussed.

6.1 Unauthorized Access

In this threat category, the attacker can:

- Access the setpoints in a power and voltage controller in an attempt to violate the safety limits and damage equipment.

- Access the energy manager and send malicious messages to microgrid components in order to consume resources or damage the components.
- Access sensitive information in transit or at rest, and remove traces from the system by deleting entries from the access log.

Mitigation: The μGridSec methodology uses strong authentication to determine the identity of a remote user and to map the user identity to the associated roles. A user can only assume roles that are associated with his/her identity. Each asset in the system has an access control list that determines the access rights of a given role for the asset (an asset is any physical component of a microgrid or any information that is protected). This prevents unauthorized access to assets. Since the number of assets and the number of roles in a microgrid are limited, the access control lists would be limited in size and easily manageable by system administrators.

6.2 Privilege Escalation

In this threat category, the attacker can:

- Gain higher privileges in the system. For example, an attacker can leverage implementation weaknesses or lenient access control lists to elevate his/her privilege level and abuse the new access rights gained as a result.
- Gain access to privileged information. For example, an attacker can launch an SQL injection attack on a controller that uses an SQL database to access privileged information stored in the database.

Mitigation: The μGridSec methodology uses role-based access control and implements a least-privilege access control architecture. Thus, each role is granted the minimum privileges to perform the required tasks; this prevents unauthorized or unintended access. It is still necessary to protect against other implementation weaknesses such as those exploited by SQL injection attacks. However, using a least-privilege architecture ensures that higher privileges than are absolutely necessary are not provided by default.

6.3 Spoofing

In this threat category, the attacker can:

- Spoof accounts by stealing credentials or exploiting storage, guessing credentials by exploiting weak account management, brute-forcing user passwords and recovering passwords by exploiting weak password policies.

Mitigation: The μGridSec methodology defines secure account and password management policies. Some of the principal features are:

- Strong and secure authentication mechanisms that always use secure channels to perform authentication.

- Strong password policies covering password entropy, password resets, password expiry, etc.
- Passwords are stored as hashes generated by the PBKDF2 function.

6.4 Denial-of-Service

In this threat category, the attacker can:

- Launch denial-of-service attacks on a microgrid system. A common example is a network flooding attack using SYN or ICMP packets. Another common denial-of-service attack (at the application layer) is flooding an application with service requests that cannot be filtered at the network layer.

Mitigation: The μGridSec methodology enforces firewalls with advanced features at the network perimeter for effective perimeter protection. Also, the various trust domains are protected by firewalls and access control lists that provide an additional layer of defense. Additionally, access control lists restrict the roles that can send requests to an asset. Note that applications typically use additional mechanisms such as rate limitation or context-based request processing to handle flooding attacks at the application layer.

6.5 Software and Firmware Integrity

In this threat category, the attacker can:

- Download malware-infected firmware on a device such as a controller and gain complete control of the device.

Mitigation: The μGridSec methodology uses a public-key infrastructure to enforce digital signatures on hashes of firmware. Each device verifies the integrity of the firmware before it is downloaded.

6.6 Unauthorized Network Access

In this threat category, the attacker can:

- Access confidential information in the absence of adequate transport layer protection.

Mitigation: The μGridSec methodology uses TLS 1.2 for transport layer protection. This ensures strong network level protection for communications both within and outside a microgrid system.

6.7 Repudiation

In this threat category, the attacker can:

- Deny sending or receiving certain messages. This can be critical for financial transactions (e.g., market price data and units of electricity sold

or purchased). This type of attack can be launched by compromising a microgrid component or by relying on a dishonest or compromised employee.

Mitigation: The μGridSec methodology mandates the use of digital signatures for financial and other sensitive transactions. The use of digital signatures is optional for non-sensitive transactions, but they can be used at the discretion of an administrator. μGridSec supports a public-key infrastructure in which each entity has a public-key certificate and a corresponding private key. The private key is used to sign the hash of a sensitive message or transaction.

7. Related Work

The Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) Project is executed jointly by the Department of Energy, Department of Defense and Department of Homeland Security [18]. The goal of the SPIDERS microgrid demonstration project is to provide secure control of electricity generation at U.S. military bases. This will be achieved by building smart, secure and robust microgrids that incorporate renewable resources. The SPIDERS Project is the first of its kind to provide cyber security for microgrid control and operations. Cyber security is provided by commercially-available technologies and, therefore, the SPIDERS cyber security technology itself is not novel. Also, SPIDERS does not provide a methodology that comprehensively addresses the possible attack vectors as in the case of μGridSec.

The CERTS MicroGrid concept integrates distributed energy resources in a microgrid to seamlessly separate or island them from the grid and reconnect them to the grid [8]. To the external entity, the entire microgrid appears as a single entity instead of a collection of distributed energy resources. The traditional method has been to integrate a small number of distributed energy resources and to shut down a microgrid when a problems arises, as detailed in the IEEE P1547 standard. The CERTS MicroGrid architecture serves as the base model for μGridSec with respect to microgrid architecture and operations. However, the CERTS model does not consider cyber security issues whereas μGridSec is focused on entirely on cyber security for microgrids.

Wang and Lemmon [21] have proposed a method for coupling low voltage microgrids into mid-voltage distribution systems. They propose a hierarchical control architecture to maximize the real power exported to a mid-voltage distribution network by coupling low voltage microgrids. Their architecture is similar to the microgrid coupling architecture considered in this work. However, Wang and Lemmon consider the electrical architecture of microgrids whereas μGridSec is focused on cyber security for microgrids. Note that the work of Wang and Lemmon as well as other efforts related to microgrid infrastructures could serve as platforms on which μGridSec could be deployed.

Mueller [11] has published details of the NSF ERC FREEDM Project on microgrids. This project investigates the challenges of the cyber-physical aspects of microgrids and highlights novel opportunities for selective power delivery

during power outages. It also recognizes the need to secure microgrids because distributed control systems are highly vulnerable to cyber attacks. Mueller makes a case for securing microgrids, but does not propose any solutions. In contrast, μGridSec recognizes the need and challenges involved in implementing cyber security for microgrids. μGridSec also derives requirements from established standards and deployments and presents a comprehensive methodology that meets the requirements.

8. Conclusions

Microgrids are an important component of current and future energy systems. They provide several benefits, including enhanced power quality, uninterrupted power supply and integration of renewable sources in the power distribution system. Since microgrids are a key component of the energy critical infrastructure, it is important that they are not disrupted or damaged by cyber attacks. The μGridSec methodology presented in this chapter is an architecture-agnostic approach that provides standards-based high security for microgrid deployments. In particular, the methodology can be applied to ensure that appropriate mechanisms are applied to microgrid architectures in order to meet cyber security requirements derived from the NERC-CIP standards and pilot microgrid deployments. A security evaluation of a representative microgrid architecture demonstrates that the μGridSec methodology can comprehensively address the identified threats. In cases where legacy devices in a microgrid do not support cryptographic mechanisms such as TLS or integrity validation, security can be implemented in the form of bump-in-the-wire hardware solutions; this concept is illustrated in a companion chapter in this volume [10]. The μGridSec methodology can enable the wider adoption of microgrids, especially in sensitive installations such as military bases and hospitals, thus enhancing energy security.

Future research will explore other relevant standards and derive additional cyber security requirements that will extend the μGridSec methodology. Although the threat modeling and architectural risk analysis presented in this chapter demonstrate that μGridSec effectively addresses cyber threats, the incorporation of requirements from additional standards will render the methodology more comprehensive and will help achieve compliance with smart grid standards.

References

[1] E. Barker, W. Barker, W. Burr, W. Polk and M. Smid, Recommendation for Key Management, NIST Special Publication 800-57 (Part 1, Revised), National Institute of Standards and Technology, Gaithersburg, Maryland, 2007.

[2] S. Bossart, DoE perspective on microgrids, presented at the *Advanced Microgrid Concepts and Technologies Workshop*, 2012.

[3] Department of Homeland Security, Catalog of Control Systems Security: Recommendations for Standards Developers, Washington, DC, 2011.

[4] Directory Applications and Advanced Security and Information Management International, OpenRBAC, Tubingen, Germany (daasi.de/en/daasi-knowledge-base/openrbac), 2014.

[5] International Electrotechnical Commission, IEC/TS 62351-1 to 62351-7, Power Systems Management and Associated Information Exchange – Data and Communications Security, Geneva, Switzerland, 2012.

[6] International Society of Automation, ISA99: Industrial Automation and Control Systems Security, Research Triangle Park, North Carolina (www.isa.org/isa99), 2015.

[7] International Standards Organization, ISO 27002:2013, Information Technology – Security Techniques, Code of Practice for Information Security Controls, Geneva, Switzerland, 2013.

[8] R. Lasseter, A. Akhil, C. Marnay, J. Stephens, J. Dagle, R. Guttromson, A. Meliopoulous, R. Yinger and J. Eto, Integration of Distributed Energy Resources: The CERTS MicroGrid Concept, P500-03-089F, California Energy Commission, Sacramento, California (certs.lbl.gov/pdf/50829.pdf), 2003.

[9] Microsoft, SDL Threat Modeling Tool, Redmond, Washington (www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx), 2014.

[10] A. Mohan, G. Brainard, H. Khurana and S. Fischer, A cyber security architecture for microgrid deployments, in *Critical Infrastructure Protection IX*, M. Rice and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 245–259, 2015.

[11] F. Mueller, Cyber-Physical Aspects of Energy Systems for the 21st Century: A Perspective from the NSF ERC FREEDM Project, Department of Computer Science, North Carolina State University, Raleigh, North Carolina (moss.csc.ncsu.edu/~mueller/ftp/pub/mueller/papers/cps09.pdf), 2009.

[12] National Institute of Standards and Technology, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800–53 (Revision 4), Gaithersburg, Maryland, 2013.

[13] National Institute of Standards and Technology, NVD Common Vulnerability Scoring System Support v2, Gaithersburg, Maryland (nvd.nist.gov/cvss.cfm), 2014.

[14] North American Electricity Reliability Corporation, Standards, Washington DC (www.nerc.com/pa/stand/Pages/default.aspx), 2014.

[15] OPC Foundation, Unified Architecture, Scottsdale, Arizona (opcfoundation.org/developer-tools/specifications-unified-architecture), 2015.

[16] OpenSSL Project, Welcome to the OpenSSL Project (www.openssl.org), 2014.

[17] R. Sandhu, D. Ferraiolo and R. Kuhn, The NIST model for role-based access control: Towards a unified standard, *Proceedings of the Fifth ACM Workshop on Role-Based Access Control*, pp. 47–63, 2000.

[18] Sandia National Laboratories, SPIDERS Microgrid Project secures military installations, Sandia Labs News Release, Albuquerque, New Mexico (share.sandia.gov/news/resources/news_releases/spiders/#.VW2kCq3bKEJ), February 22, 2012.

[19] Smart Grid Interoperability Panel, Cyber Security Working Group, Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security, National Institute of Standards and Technology, Gaithersburg, Maryland, 2010.

[20] K. Stouffer, J. Falco and K. Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.

[21] Z. Wang and M. Lemmon, Task 1: Coupling Low-Voltage Microgrids into Mid-Voltage Distribution Systems, Department of Electrical Engineering, University of Notre Dame, Notre Dame, Indiana (www3.nd.edu/~lemmon/projects/GE-project-2010/Vault/Publications/algorithm_develop_report_01302012.pdf), 2012.