A Cyber Security Architecture for Microgrid Deployments

Apurva Mohan, Gregory Brainard, Himanshu Khurana, Scott Fischer

Chapter 15

A CYBER SECURITY ARCHITECTURE FOR MICROGRID DEPLOYMENTS

Apurva Mohan, Gregory Brainard, Himanshu Khurana and Scott Fischer

Abstract Microgrids enable the aggregation of various types of generating and non-generating sources as a unified control unit. Microgrid control networks are connected to external networks – SCADA networks for demand-response applications, enterprise networks and the Internet for remote monitoring and control. These external connections expose microgrids to serious threats from cyber attacks. This is a major concern for microgrids at sensitive installations such as military bases and hospitals. One of the challenges in protecting microgrids is that control networks require very low latency. Cryptographic protection, which adds additional latency to communications, is unacceptable in real-time control, especially with regard to synchronization and stability. Also, a complex network at a microgrid site with interconnected control and SCADA networks makes the process of acquiring security certifications (e.g., DIACAP) extremely difficult. To address these challenges, this chapter presents the SNAPE cyber security architecture, which segregates communications networks needed for fast, real-time control from networks used for external control signals and monitoring, thereby drastically reducing the attack surface of a microgrid control network. Network segregation is achieved by hardware devices that provide strong cryptographic separation. The segregation isolates control networks so that they can use lightweight cryptography to meet the low latency requirements. The novel approach minimizes the cyber security certification burden by reducing the scope of certification to a subset of a microgrid network.

Keywords: Microgrids, cyber security architecture, threat modeling

1. Introduction

A microgrid is a collection of distributed energy resources (DERs), storage and loads under common coordination and control that provides a functional

interface to enable its management as a single unit. The U.S. Department of Energy defines a microgrid as: "[A] group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in the grid-connected or island-modes" [1]. A microgrid acts as a single point of integration for generating (renewable and non-renewable) and non-generating sources. A microgrid accumulates all the generation capacity at a site and provides power to a local site not only in cases of blackouts, but also as ancillary capacity to lower energy usage from the main electric power grid. Microgrids are currently deployed at military bases, hospitals, universities, residential communities and government buildings to enhance energy efficiency and energy security. Microgrids can be deployed in a variety of architectures – as a single microgrid that provides power to a site, as multiple microgrids that function in isolation at a site, or as multiple microgrids deployed as power enclaves, where each enclave is served by a single microgrid unit, but all the units are connected via electrical power lines for load balancing and via communications lines for common control and coordination.

In many critical infrastructures, operations sites are often distributed and multiple sites are connected to a common control center. Also, the control center needs to communicate with the enterprise network. To enable all the required communications, microgrids/control centers are often connected to the Internet directly or via a control center. Typically, the control center to microgrid communications use distributed control system (DCS) protocols such as DNP3 and Modbus; IP-based protocols such as DCS IP or TCP/IP are typically used for longer distances. The Internet connectivity exposes microgrids to numerous cyber threats. Cyber attackers could target microgrid operations and potentially disrupt the power supply. Attacks on microgrids installed at sensitive sites such as military bases, hospitals or government buildings could have serious consequences.

This chapter describes the novel Secure Network of Assured Power Enclaves (SNAPE) cyber security architecture, which enforces network separation in microgrid communications to reduce the attack surface while enhancing communications efficiency and security. In particular, SNAPE segregates the communications networks needed for fast, real-time control from networks used for external control signals and monitoring. The SNAPE architecture was created for a large U.S. Army base where multiple power enclaves with secure communications were envisioned. A deployed microgrid system based on the SNAPE architecture would contribute to the energy security and net-zero goals of the U.S. Department of Defense. The architecture uses cryptographic mechanisms to enforce network separation and provide strong cyber security.

The research described in this chapter has three main contributions. The first is the development of a conceptual cyber security architecture for microgrids with a cryptographic network separation strategy that minimizes control network latency and the control network attack surface. The second is

a practical deployment architecture for microgrids that provides security and scalability. The third contribution is the use of certified hardware devices for cryptographic network separation, which significantly reduces the certification burden for microgrid deployments at U.S. military bases.

2. Problem Description

Current distributed control system and SCADA environments typically rely on the IEC 61850 standard for communications between power substations. It is also a natural choice for connecting power enclaves defined in the SNAPE architecture, where multiple microgrids coordinate command and control. This environment has a very strict timeframe of a few milliseconds for command-response messages and any additional latency adversely impacts system performance in terms of the established requirements.

As mentioned above, microgrid systems are being connected to external networks such as enterprise networks and the Internet, which significantly increases cyber threats. Cyber attackers can attack microgrid power enclaves and compromise critical operations by exploiting vulnerabilities at the network, system and/or application levels. Microgrid deployments are being planned with network and information technology security postures that are not compliant with standards such as NIST 800-53 [12] or IEC 62443 [5]. Most systems rely on perimeter protection with the internal systems designed with lower security because they were intended to be part of a closed network. As such, achieving defense-in-depth in these microgrid systems and networks is a major challenge.

Another related problem in power networks is that communications protocols (e.g., IEC 61850) were not designed for security and they do not inherently support security features. As a result, providing communications security for these protocols requires considerable ad hoc and ancillary security mechanisms. These mechanisms inadvertently introduce security vulnerabilities that are easily exploited by cyber attacks. Recent standards such as IEC 62351 focus on securing IEC 61850 based communications [4], but even IEC 62351 does not cover the entire gamut of security vulnerabilities in networked microgrid deployments. OLE for Process Control – Unified Architecture (OPC UA) [13] presents a framework with a standards-based communications backbone and built-in security that covers a larger set of cyber security threats. However, it does not address microgrid-specific threats such as the exposure of sensitive control networks, the integration of legacy components and the complexities involved in achieving cyber security certifications.

This chapter focuses on three problems. First, the internal networks in a microgrid deployment comprise several sub-networks such as the SCADA network and microgrid control network, and maintain connections to the enterprise network. Since these networks are interconnected, the exposure of microgrid control networks to attacks is increased. A malicious entity could exploit an attack vector to break into any one of the sub-networks and then attempt to disrupt operations elsewhere in the microgrid control network. Second, many legacy devices are unable to implement security mechanisms such as encryp-

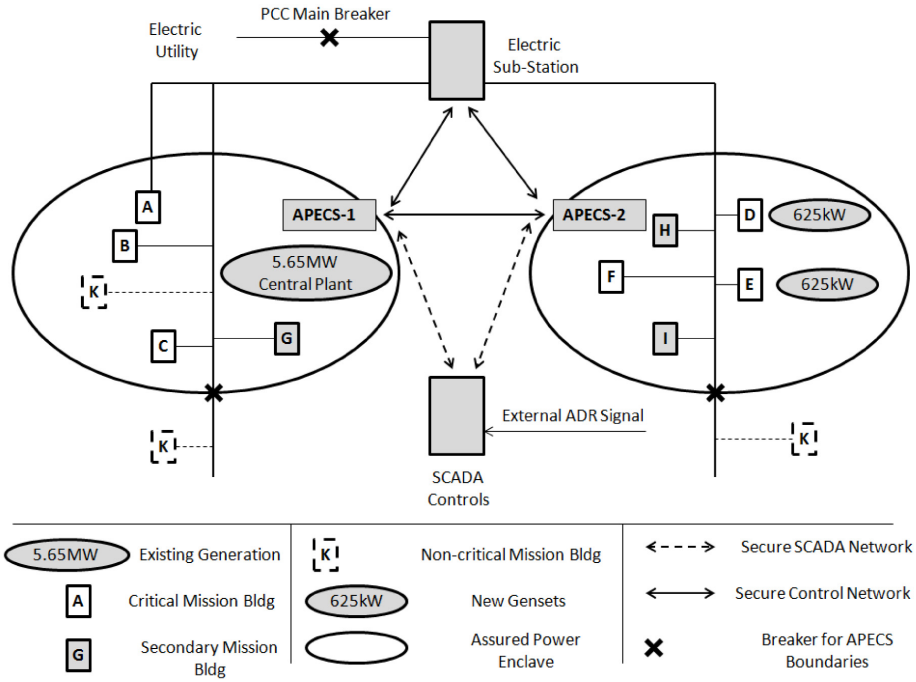

Figure 1. Conceptual architecture of a SNAPE microgrid.

tion, message signing and message hashing. This makes it difficult to enforce a strong and uniform security policy in the system. If the security policy is chosen for varying levels of security based on device capabilities, then attackers could compromise the lower-end devices with weaker security and then pivot to other networked devices. Third, in the case of microgrids at U.S. Department of Defense installations, the deployments have to obtain DIACAP or the more recent DIARMF (Department of Defense Information Assurance Risk Management Framework) certifications. Since a microgrid network comprises several sub-networks, the task of security assessment and certification of the microgrid control network becomes very complex and challenging.

3. SNAPE Cyber Security Architecture

The SNAPE architecture enables secure communications and control for multiple microgrid systems at a site, where each microgrid corresponds to a power enclave. A SNAPE microgrid can function in the grid connected mode or in the islanding mode to provide power to a local site. SNAPE SCADA control systems accept external automated demand response (ADR) signals and participate in automated demand response programs for energy efficiency.

Figure 1 presents a conceptual architecture of the SNAPE system. The system has two power enclaves, APECS-1 and APECS-2. Each enclave is at-

tached to critical and non-critical mission buildings. An enclave may have one or more diesel generators powering it. The microgrid has a point of common coupling (PCC) main breaker that can disconnect the microgrid from the main grid to bring it into the islanding mode. The lines connecting the substation to APECS-1 and APECS-2 correspond to the secure control network, whereas the lines connecting the SCADA controls to APECS-1 and APECS-2 correspond to the secure SCADA network. The control and SCADA networks are isolated from each other. The isolation can be physical or logical in nature.

3.1 Security Properties

The SNAPE architecture provides a number of security properties to address the cyber security concerns discussed above. The main security properties are:

- Confidentiality of information, command-response and power system operations.
- Channel integrity – integrity of data and communications flowing in and out of the microgrid.
- Message integrity – message level integrity protection in addition to channel protection.
- Application integrity – protection of the integrity of applications installed in the microgrid system.
- Availability of communication channels and microgrids to participate in command-response communications.
- Authenticity of information sources.
- Protection and isolation from the enterprise network and external networks.
- Auditing and forensic analysis capabilities.
- Reduction of the cyber attack surface.

3.2 Architecture

This section presents the details of the SNAPE cyber security architecture and describes its functioning via some use cases. Also, it discusses how the architecture acquires the security properties listed above.

The secure control network in Figure 1 is isolated from the secure SCADA network. This isolates the control network from access from the enterprise network and other external networks, including the Internet. The isolation also improves the response time in the control network, which is critical to synchronizing microgrids. Additionally, it reduces the attack surface of the control network because no direct communications path exists.

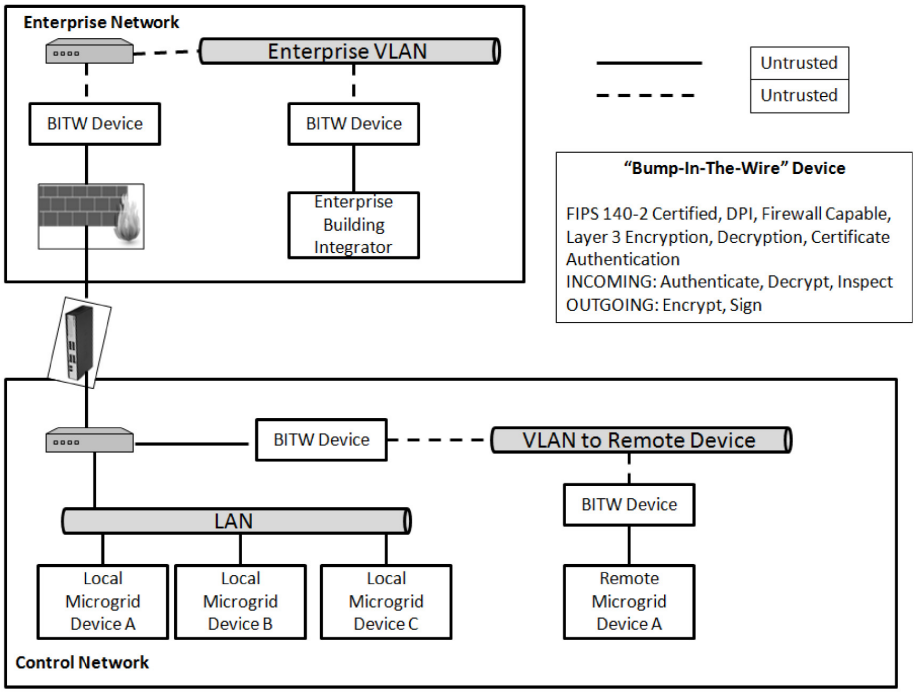

Figure 2. Communications security architecture based on the SNAPE concept.

Figure 2 presents the SNAPE architecture from the communications, network and system security point of view. It shows the external communications with the enterprise network and the local network that connects to the microgrid. "Bump-in-the-wire" devices are used to integrate legacy equipment or microgrid devices that cannot perform cryptographic operations required by secure communications networks. The bump-in-the-wire devices have the ability to encrypt communications using standard protocols. They also provide cryptographic isolation of the networks.

In the SNAPE architecture, OLE for Process Control – Unified Architecture (OPC UA) is used to implement the communications backbone. OPC UA is backward compatible with distributed control system protocols such as IEC 61850. OPC UA provides authentication and authorization services at the application layer. Availability in a network is provided by two mechanisms. First, the isolation of the control network from external networks ensures that the control network communications can meet the low latency requirement and critical infrastructure components are not unavailable due to large latencies or disruptions caused by microgrid components being out of sync. Second, cryptographic protection of messages and the network, as well as network firewalls, ensure that attackers cannot compromise the network or launch denial-of-service attacks against network components. It is important to emphasize

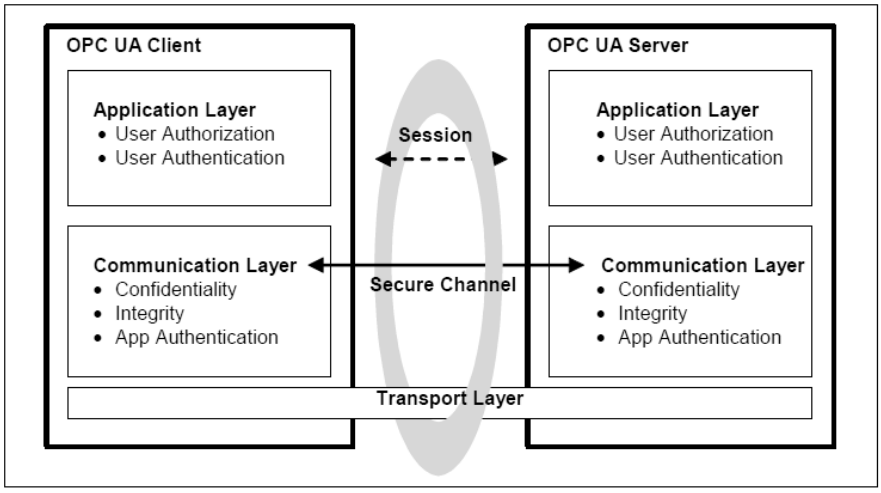

Figure 3. OPC UA security model [13].

that the closed loop control network is enclosed within the secure enclaves and the control network is physically isolated, hence it cannot be reached from the communications network. The communications network uses high-end cryptographic protection to enforce cyber security without adding additional latency to the control network due to its isolation.

Finally, important events, accesses and messages are logged to enable auditing and forensic analysis. This helps identify anomalous behavior and perform root cause analysis if an attack is suspected.

3.3 OPC UA Integration

This section describes how OPC UA is integrated with the SNAPE architecture to provide a secure communications backbone. Details of the OPC UA security model are provided to demonstrate that the SNAPE architecture has the security properties listed above.

The OPC UA standard was created by the OPC Foundation [13]. It improves on the earlier OPC Classic standard, which was restricted to the Windows operating system. OPC UA builds on OPC Classic with several significant updates, including an open platform architecture, a built-in security model and a feature-rich data model. It is also backward compatible with standards such as IEC 61850. This makes OPC UA an excellent choice for integration within the SNAPE architecture.

Figure 3 shows the OPC UA security model. The model has two layers, the communications layer and the application layer. In the communications layer, a secure channel provides confidentiality and integrity of the communications. Another feature that is supported is application authentication, which allows

only authenticated applications to participate in microgrid operations. In the application layer, user authentication and authorization are used to establish a secure session over a secure channel. An important point to note is that availability itself is not provided by the OPC UA security model. It relies on the minimal processing of messages prior to authentication and defers availability to the server implementation. The SNAPE architecture complements these mechanisms by providing strong availability properties via features such as network segmentation, cryptographic separation and network firewalls.

The OPC UA security model is comprehensive and offers multiple options for achieving security properties in the communications and application layers [13]. In the application layer, authentication may be achieved by three different means: username/password, an X.509v3 certificate or a WS-SecurityToken. An X.509v3 certificate involves multiple asymmetric cryptographic operations that are computationally intensive and are not well suited for authentication in resource-constrained environments. However, username/passwords and WS-security tokens provide comparatively efficient authentication. During system implementation, it would be necessary to compare the different mechanisms against the real-time system requirements and select the most efficient form of authentication for the SNAPE architecture. Authorization in the OPC UA security model is more open ended and can integrate already-deployed authorization solutions. Since the SNAPE architecture targets microgrids, existing authorization mechanisms in the form of access control lists are integrated to provide fine-grained authorization for microgrid resources.

In the communications layer, confidentiality is provided by encryption within a secure channel, message signatures for message integrity and digital signatures for application authentication. Like the application layer, the OPC UA stack provides multiple options to implement each security mechanism. The optimal combination of asymmetric and symmetric cryptographic algorithms was selected for the SNAPE architecture to meet microgrid performance requirements. OPC UA is flexible and allows any combination of the mechanisms to be selected to suit a specific deployment. For example, a combination of mechanisms such as transport layer security (TLS) for channel protection and symmetric algorithms for message integrity may suit a microgrid deployment environment. This would allow SNAPE to leverage the benefits of TLS for channel protection and the advantages of symmetric algorithms such as AES256 and HMAC(SHA1) for improved real-time performance with regard to message integrity protection.

4. SNAPE Threat Model Analysis

This section identifies the potential cyber threats that exist in the microgrid deployment scenarios presented in Figures 1 and 2, and demonstrates that the SNAPE architecture mitigates the threats.

Remote Sabotage:

- **Threat:** An adversary can remotely access the microgrid and launch a privilege elevation attack to gain higher rights. The adversary can then perform unauthorized operations to disrupt the microgrid system and potentially the power supply.
- **Mitigation:** The SNAPE architecture implements a number of security controls to mitigate this threat. Secure network communications protects against threats such as session hijacking. Identity management with strong account management protects against account spoofing attacks. The access control implementation in the microgrid system prevents unauthorized access to microgrid resources and operations.

Tampering with Power Enclave Synchronization:

- **Threat:** The adversary can disrupt power enclave synchronization by reporting incorrect power measurements to other entities. This could potentially destabilize the power enclaves and disrupt their operations.
- **Mitigation:** In the SNAPE architecture, the control network and the SCADA network are isolated from each other. This isolation drastically reduces the attack surface from the SCADA network to the energy network. Moreover, authentication and access control protection in the microgrid system prevent unauthorized access. As such, it is highly unlikely that an adversary could reach the control network and disrupt its operation.

Sensitive Information Disclosure:

- **Threat:** An attacker can view sensitive microgrid information that is at rest or in transit.
- **Mitigation:** The SNAPE architecture implements authentication and access control in the microgrid system, so that only authorized entities can view or operate on sensitive data. Additionally, information in transit is protected by strong network security involving encrypted communications channels using TLS. Thus, sensitive information at rest or in transit is protected from unauthorized disclosure.

Denial of Service:

- **Threat:** An attacker can launch a denial-of-service attack by flooding a network to disrupt microgrid operations and potentially the power supply.
- **Mitigation:** The SNAPE architecture uses secure network topologies derived from reports and standards such as NIST SP 800-53 and IEC 62443 to deploy firewalls and demilitarized zones to isolate the SCADA and control networks from the enterprise network. The firewalls protect

against network flooding attacks. Also, the SCADA and control networks are isolated, which further reduces the control network attack surface. Additionally, the OPC UA communications backbone performs minimal processing of unauthenticated messages to mitigate the denial-of-service threat.

Targeting Legacy Devices:

- **Threat:** Legacy devices in the microgrid system are unable to implement encryption for secure communications channels. An attacker can target these channels to view sensitive information or to inject or manipulate commands.

- **Mitigation:** The SNAPE architecture positions bump-in-the-wire hardware in front of legacy devices to implement secure communications. The bump-in-the-wire devices provide network security via TLS, which makes legacy devices compatible with other devices and provides uniform and strong network security. The bump-in-the-wire devices can be DIACAP- or DIARMF-certified to provide strong, standards-compliant network security regardless of end device capabilities.

Malware Installation:

- **Threat:** An attacker can install malware on microgrid devices.

- **Mitigation:** The SNAPE architecture provides two types of protection against malware installation. First, software or firmware installation on a device is a privileged action that can only be performed by an administrator; it would be very difficult for an attacker to compromise a highly-secure administrator account to install malware. Second, software and firmware integrity checks are performed by validating their digital signatures; only firmware and software that pass the validity checks can be installed. These security mechanisms protect against the installation of malware on the microgrid system.

5. Discussion

Whenever security considerations are included in an architecture, certain trade-offs have to be made to balance security versus performance, cost, development time and usability. The SNAPE architecture uses bump-in-the-wire devices to support the secure integration of legacy devices. This provides uniform security in a microgrid network by enabling legacy devices to communicate using strong encryption algorithms. The downside, however, is that these devices can be expensive, depending on their functionality and the desired level of security. However, this is an optional feature in the SNAPE architecture, although it may be mandatory for microgrids at sensitive locations such as military bases.

Another trade-off is that network separation using bump-in-the-wire devices may increase network complexity and latency. However, the separation offers the choice of cryptographic algorithms for network protection. The bump-in-the-wire devices are DIACAP-certified and perform cryptographic operations end-to-end. The added latency is very low and is only introduced in the communications network. The control network is part of the secure enclaves where there is no additional latency related to cryptographic operations.

The SNAPE architecture proposes the use of TLS for strong network protection. The architecture also provides end device authentication, which is especially useful in sensitive installations and helps achieve DIACAP or DIARMF compliance. The downside of using TLS is that public-key infrastructure certificates must be installed and managed by the network. Using symmetric encryption is possible with TLS, but this is a non-standard mode of operation that is not recommended for regular deployments.

The final trade-off is related to the integration of OPC UA in SNAPE. The integration increases complexity and the cost of system development. However, on the positive side, it provides standards-based communications security. Also, it inherits a versatile and feature-rich communications backbone from SNAPE.

Massie [9] has presented a proposal for microgrid cyber security based on a distributed control approach that uses IPv6 for communications. IPv6 provides some benefits such as making host scanning and identification more difficult from outside a network because of the large number of possible IP addresses, and supporting end-to-end encryption and secure name resolution that helps counter attacks such as ARP poisoning. The SNAPE architecture provides all the benefits of an IPv6-based network. Indeed, the SNAPE architecture was developed by performing threat modeling and risk analysis, and security controls and mechanisms were subsequently incorporated to address the identified threats. In the SNAPE architecture, a microgrid deployment uses a private network with strong perimeter protection. Secure firewalls disable network scanning and identification. End-to-end encryption is implemented using TLS. Also, TLS used for network-level authentication can be configured for the mutual authentication of clients and servers; this eliminates ARP attacks. Additionally, SNAPE uses bump-in-the-wire devices to provide end-to-end authentication of legacy devices.

Massie's approach [9] suffers from several security issues compared with the SNAPE architecture. First, a decentralized peer-to-peer control architecture means that every node is trusted equally and can even take over the functionality of other nodes, especially during automated recovery. In addition to introducing complexity, this approach potentially opens new attack vectors. The adversary needs to compromise just one node and then pivot to sabotage the system. In a centralized model, a server has much stronger security than a client node. Maintaining trust in an open decentralized peer-to-peer system is a hard problem [6, 10] and even controlled system deployments would inherit some of its threats if they are connected to the Internet. Second, since control and coordination are distributed to every node, it is not possible to segment

the network and isolate it for higher security and performance, something that is inherently supported and demonstrated in the SNAPE architecture. Third, Massie's approach assumes that all control devices are deployed with the peer-to-peer functionality and there are no legacy devices (actually, the approach is unable to integrate legacy devices). On the other hand, SNAPE has a method to integrate legacy devices; this is important because most network deployments are incremental in nature and it is exceedingly rare not to encounter legacy devices in a deployment.

Additionally, deploying IPv6-based networks potentially opens a number of security holes. If IPv6 and IPv4 are being run simultaneously, then IPv6 should be tunneled over IPv4 or run independently. In the tunneling mode, configuration problems can create security holes in the system [8]. If the two protocols are run in parallel, then firewalls have to be configured to filter the IPv6 traffic, which is not very common. A normal firewall does not filter IPv6 traffic; this insecure channel can be leveraged by an attacker to enter the system. Also, administrators must employ new (and better) ways to deploy, configure and monitor networks. Important tasks include troubleshooting networks, configuring firewalls, enforcing secure configurations, monitoring security logs, analyzing real-time behavior and performing network audits. Most intrusion detection/prevention systems are still not very effective at handling IPv6 traffic, which increases the potential of attacks.

6. Related Work

Strickland [16] has presented an approach for protecting military microgrids from cyber attacks. However, the approach relies primarily on security best practices and does not consider some key issues that are addressed in the SNAPE architecture such as the vulnerabilities originating from SCADA networks and legacy devices.

The CERTS MicroGrid is a novel approach for integrating distributed energy resources in a microgrid to seamlessly island it from and reconnect it to the power grid [7]. To the control center, all the distributed energy resources appear to be a single entity for coordination and control. The traditional method has been to integrate a small number of distributed energy resources and to shut down the microgrid when problems arise (according to the IEEE P1547 standard). However, unlike the SNAPE architecture, the CERTS model does not specifically focus on cyber security for microgrids.

The Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) Project is conducted jointly by the Department of Energy, Department of Defense and Department of Homeland Security [14, 15]. The project goal is to provide secure control of on-base generation at military bases by building secure and robust microgrids that incorporate renewable energy resources. Cyber security is provided by commercially-available technologies, so the technology itself is not novel. Unlike SNAPE, SPIDERS does not provide a comprehensive architecture to address all possible attack vectors.

Mueller [11] discusses research undertaken under the NSF ERC FREEDM Project [11]. The project investigates the challenges of the cyber-physical nature of microgrids and highlights novel opportunities for providing selective power delivery during power outages. Mueller recognizes the need to secure microgrids from cyber attacks. However, the FREEDM Project does not propose any security solutions. SNAPE stands out because it recognizes the need to secure microgrids and presents a comprehensive cyber security architecture that adheres to industry standards and satisfies actual microgrid requirements.

Massie [9] presents a distributed control framework for microgrids to enhance coordination, communications and security. The framework, which uses IPv6-based communications, attempts to leverage security from IPv6 and the peer-to-peer distributed model, but it also inherits their problems. SNAPE provides all the security features provided by the framework and introduces many additional security mechanisms.

7. Conclusions

Microgrids are being deployed at military bases and other mission-critical facilities to reduce the dependence on the power grid, to provide power during outages and to achieve the net-zero goal imposed by the U.S. Department of Defense. The SNAPE architecture is designed specifically for the secure deployment of military microgrids. It introduces several key concepts such as the physical or logical separation of microgrid control networks from SCADA networks, bump-in-the-wire devices that integrate legacy devices in a secure manner and standards-based security controls for microgrid network protection.

Current efforts are focused on realizing the SNAPE architecture in a microgrid facility under construction at a U.S. military base. The design divides the power network into several power enclaves, each served by a microgrid unit. These units will be connected using the SNAPE architecture to support common control and coordination. An OPC UA based communications backbone will be implemented along with the additional security mechanisms described in Section 3. An architectural risk analysis of the system has revealed that SNAPE effectively addresses all the identified risks. During the microgrid design phase, security threat use cases will be evaluated using the SNAPE architecture to verify that the threats are comprehensively addressed. During the deployment phase, strong efforts will be taken to ensure that all the architectural and design considerations will be implemented and tested.

References

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

[2] N. Hatziargyriou, H. Asano, R. Iravani and C. Marnay, Microgrids, *IEEE Power and Energy*, vol. 5(4), pp. 78–94, 2007.

[3] F. Hohlbaum, M. Braendle and F. Alvarez, Cyber security practical considerations for implementing IEC 62351, presented at the *PAC World Conference*, 2010.

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

[5] International Electrotechnical Commission, IEC 62443, Industrial Communications Networks – Network and System Security, Geneva, Switzerland, 2013.

[6] S. Kamvar, M. Schlosser and H. Garcia-Molina, The Eigentrust algorithm for reputation management in P2P networks, *Proceedings of the Twelfth International Conference on World Wide Web*, pp. 640–651, 2003.

[7] 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.

[8] J. Lyne, Why IPv6 matters for your security, Sophos, Oxford, United Kingdom (`www.sophos.com/en-us/security-news-trends/security-trends/why-switch-to-ipv6.aspx`), 2014.

[9] D. Massie, Implementation of a cyber secure microgrid control system, presented at the *SPIDERS JCTD Industry Day*, 2014.

[10] A. Mohan and D. Blough, AttributeTrust – A framework for evaluating trust in aggregated attributes via a reputation system, *Proceedings of the Sixth Annual Conference on Privacy, Security and Trust*, pp. 201–212, 2008.

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

[14] 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.

[15] J. Stamp, The SPIDERS Project – Smart power infrastructure demonstration for energy reliability and security at U.S. military facilities, *Proceedings of the IEEE PES Conference on Innovative Smart Grid Technologies*, 2012.

[16] T. Strickland, Microgrid security considerations in military base deployments, DNV KEMA, Arnhem, The Netherlands (`smartgridsherpa.com/blog/microgrid-security-considerations-in-military-base-deployments`), 2014.