EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Security Architecture Methodology for the Electric Sector, Version 2.0

3002007887

Security Architecture Methodology for the Electric Sector, Version 2.0

3002007887

Technical Update, December 2016

EPRI Project Manager

A. Lee

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE ELECTRIC POWER RESEARCH INSTITUTE (EPRI) PREPARED THIS REPORT

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report.

Electric Power Research Institute (EPRI)
3420 Hillview Avenu
Palo Alto, CA 94304

Principal Investigators
A. Lee
J. Stewart
G. Chason
R. King

This report describes research sponsored by EPRI.

EPRI acknowledges the collaboration of several organizations: National Rural Electric Cooperative Association (NRECA), American Public Power Association (APPA), Edison Electric Institute (EEI), and Utilities Technology Council (UTC) for their interest and involvement. The author also thanks the input from the utilities who have provided valuable information to guide this report.

This publication is a corporate document that should be cited in the literature in the following manner:

Security Architecture Methodology for the Electric Sector, Version 2.0. EPRI, Palo Alto, CA: 2016. 3002007887.

ABSTRACT

The nation's power system consists of both legacy and next generation technologies, with devices that may be 30–50 years old, have no cyber security controls, and implement proprietary communication protocols and applications. Many of these legacy devices have significant computing and performance constraints that limit the cyber security controls that may be implemented. By contrast, the new technology may include modern information technology (IT) devices with commercially available applications and communication protocols. The new operations technology (OT) devices may also include commercially available applications and communications.

With this shift in technology, utilities are exploring methods to better address cyber security requirements. This includes prioritizing the systems, performing a cyber security risk assessment, and determining the impacts of a cyber security compromise as part of a cyber security strategy.

Another component of the cyber security strategy is a cyber security architecture. Currently, utilities have enterprise architecture diagrams, but they have not typically developed a security architecture. This report includes a methodology for developing a cyber security architecture that leverages existing architecture methodologies. It focuses on identifying the attack surface and mitigation strategies for transmission and distribution substations. The report is an update to the first cyber security architecture methodology document, 3002005942, published in 2015, and is a companion document to EPRI's *Substation Security Architecture Reference Diagrams, Version 1.0* (3002009519).

Keywords

Cyber security
Cyber security architecture
Cyber security controls
Security use cases
Attack surface

Deliverable Number: 3002007887

Product Type: Technical Update

Security Architecture Methodology for the Electric Sector, Version 2.0

PRIMARY AUDIENCE: Power delivery system owners and operators

SECONDARY AUDIENCE: Research organizations and solution providers

KEY RESEARCH QUESTION

For grid modernization, increased interconnection in electric sector devices is required, resulting in a larger attack surface that may be exploited by potential adversaries such as nation-states, terrorist organizations, malicious contractors, and disgruntled employees. The focus of this document is to present a standardized security architecture methodology that has been applied to transmission and distribution substations in this new environment and that includes an approach for analyzing the attack surface and reference architecture diagrams. This second version of the methodology will be widely distributed upon completion; the goal is to receive feedback and then publish an updated version. The report is a companion document to EPRI's *Substation Security Architecture Reference Diagrams, Version 1.0* (3002009519).

RESEARCH OVERVIEW

Typically, an enterprise architecture does not address cyber security, in specific the overall attack surface, attack vectors, potential vulnerabilities, and applicable mitigation strategies. The challenge is to develop a security architecture methodology that augments, rather than replaces, current enterprise architecture methodologies and is at a level that is useful to utilities. This report includes the second version of a cyber security architecture methodology that may be used by utilities for existing and planned system architectures. The objective is to provide a common methodology applicable to utilities of all sizes—from large investor-owned utilities to smaller cooperatives and municipalities. EPRI is collaborating with other research efforts to ensure that the security architecture methodology does not conflict with ongoing work.

KEY FINDINGS

- At present, there is no common security architecture methodology used throughout the utility industry. Several architecture frameworks are available, and each includes unique terms and definitions. In general, these frameworks are intended for use in developing an enterprise architecture and not specifically a cyber security architecture.
- A reference cyber security architecture may be used in evaluating the current system configuration and defining transition and target configurations.
- A security architecture methodology is an important tool in a utility's cyber security risk management strategy.
- A reference cyber security architecture may be used to support utility situational awareness.

WHY THIS MATTERS

A cyber security architecture methodology is one of the tools that can be used to assess the constantly changing threat and technology environments.

HOW TO APPLY RESULTS

As utilities modernize the grid, they will need to assess the architecture to identify potential vulnerabilities that may be exploited by an attacker as well as appropriate attack mitigation strategies. This can be a difficult task without the use of a cyber security architecture methodology. Because the goal of this project is to develop a common methodology, participation in the project and provision of input will ensure that the product is useful to utilities.

LEARNING AND ENGAGEMENT OPPORTUNITIES

- Collaborators: Edison Electric Institute (EEI), National Rural Electric Cooperative Association (NRECA), American Public Power Association (APPA), and Utilities Technology Council (UTC)
- Presentation materials: EPRI 2016 Cyber Security Technology Transfer Workshop, held November 1–2, 2016, in Dallas, TX
- EPRI 2017 Winter Advisory Meeting, held February 13–15, 2017, in Huntington Beach, CA

EPRI CONTACT: Annabelle Lee, Principal Technical Executive, alee@epri.com

PROGRAM: Cyber Security, 183

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

CONTENTS

LIST OF FIGURES

LIST OF TABLES

TABLE OF SECURITY USE CASES

1
INTRODUCTION

Currently, the nation's power system consists of both legacy and next generation technologies. This includes devices that may be 30-50 years old that have no cyber security controls and implement proprietary communication protocols and applications. Many of these legacy devices have significant computing and performance constraints that limit the cyber security controls that may be implemented. In contrast, the new technology may include modern information technology (IT) devices with commercially available applications and communication protocols. The new operations technology (OT) devices may also include commercially available applications and communications. To utilize this new technology, increased interconnection is required with the applicable cyber security controls implemented to address this larger attack surface that may be exploited by potential adversaries such as nation-states, terrorist organizations, malicious contractors, and disgruntled employees. The challenge and complexity of addressing cyber security risks has increased in part because the technology landscape and threat environment are constantly changing.

Each utility should develop and implement an overall risk management strategy that includes a cyber security risk strategy. The cyber security strategy may need to be tailored to the OT environment because of the performance and computing constraints referenced above. Another difference between IT and OT is that the primary security objectives for OT systems are availability and integrity, with confidentiality third. The primary security objectives for IT systems are confidentiality and integrity and availability third. This difference impacts the risk assessment and the specific security requirements that are selected.

An enterprise architecture may be included as one component of a risk assessment package. The architecture identifies, for example, the hardware, software, applications, and data that are included in the system. The architecture may be represented in several forms, for example, as a diagram and/or a list of applicable standards. An architecture framework methodology should be defined at the enterprise level to ensure consistency of the architectures developed throughout the organization. If diagrams are developed, they may be used to document the current or *baseline* system and the *target* system. One of the difficulties is that these enterprise diagrams can take significant time to create and can be very complex. As a result, they may not be maintained, thus reducing their usefulness.

Typically, an enterprise architecture does not address cyber security, specifically, the overall attack surface, attack vectors, potential vulnerabilities, and applicable response strategies. Alternatively, cyber security is documented in policies and procedures that are defined at the organization level. At the system level, these policies and procedures should be tailored and specifications developed.

The challenge is to develop a security architecture methodology that augments, rather than replaces current enterprise architecture methodologies and is at a level that is useful to utilities. The resulting security architecture should be used to document the baseline architecture, the target architecture, and the transition approach. For this report, a security architecture includes:

- A diagram that displays the physical devices and communication links between the devices. The source could be the enterprise architecture diagram. Applicable standards should be included.
- Identification of the access points to various devices. The access points can be used by an attacker, including an insider, to initiate intrusion into the system.
- Identification of the potential vulnerabilities that may be exploited by an attacker.
- Specification of the response strategies to the potential system compromise. The response strategy may include the selection and implementation of cyber security technical controls. Applicable standards should be included.

A security architecture diagram may be one component of the cyber security risk assessment package that supports a cyber security risk strategy. A cyber security risk strategy is documented in *Risk Management in Practice, A Guide for the Electric Sector*, EPRI Technical Update 3002003333, December 2014. The cyber security risk strategy is divided into three categories based on methodology:

- **Maturity Model Methodology –** maturity models provide utilities with a method to assess the degree of an organization's alignment with the best practices in the structure and operation of the organization and its IT and OT systems.
- **Control-Based Methodology** – controls-based methodologies address the technical aspects related to the configuration of the IT and OT systems and protective hardware and software.
- **Compliance Methodology** – compliance methodologies focus on specific mandatory requirements. At this time, there are only regulations for the bulk electric system (BES).

A security architecture may be used with both the control-based methodology and the compliance methodology. For this report, the focus is on the control-based methodology. Figure 1-1 below illustrates the relationship between the Control-Based Methodology and the development of a security architecture.

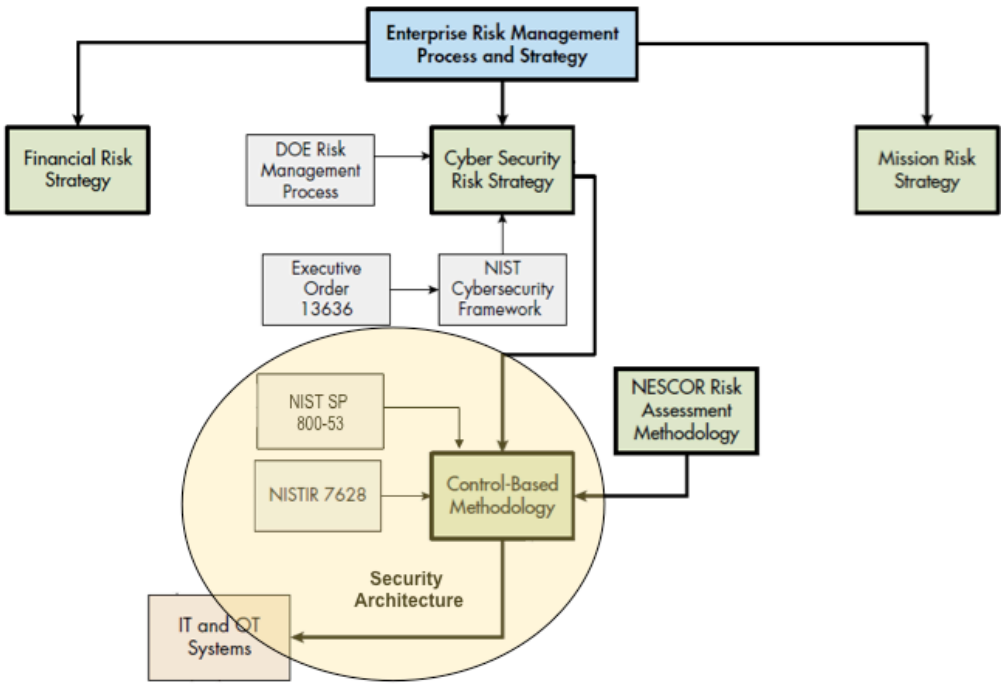


Figure 1-1
Control-Based Methodology and Security Architecture

The security architecture methodology described in this report builds on output from existing guidelines and processes that are elements of a cyber security risk management strategy. The objective is to build on these existing guidelines and processes that have been used by utilities rather than developing a new approach. Two of the documents included in Figure 1-1 above are the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations and NIST Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security. Both documents specify security requirements that may be applied to both IT and OT systems. In addition, NISTIR 7628 focuses on the smart grid and control systems. The selection of security requirements is based on a risk assessment that includes determining the priority of the system based on the impact levels for the security objectives of confidentiality, integrity, and availability.

1.1 Document Purpose

The purpose of this document is to define a security architecture methodology that may be implemented throughout the electric sector by utilities of all sizes - large investor-owned utilities (IOUs), municipalities, and cooperatives. There are several architecture frameworks that are currently available, and each includes unique terms and definitions. In general, these frameworks are intended to be used to develop the enterprise architecture, and not specifically a security architecture. The frameworks that focus on security architectures typically do not include an approach for analyzing the attack surface and identifying attack vectors and potential vulnerabilities that may be exploited. The focus of this document is to present a standardized security architecture methodology that has been applied to transmission and distribution substations that includes an approach for analyzing the attack surface and reference architecture

diagrams. This is the second version of this methodology and once it has been completed, it will be widely distributed. The goal is to receive feedback and then publish an updated version.

1.2 Document Content

This document contains the following sections:

- Section 1: Introduction
- Section 2: Security Architecture Context
- Section 3: Security Architecture Methodology
- Section 4: Substation Device Categories
- Section 5: Substation Reference Security Architectures
- Section 6: Use Case Examples
- Section 7: Next Steps

2
SECURITY ARCHITECTURE CONTEXT

Utilities are facing many challenges in addressing cyber security for the existing and planned grid. As described above, the current grid architecture includes both new and legacy technology and commercially-available and proprietary solutions. From a cyber security perspective, the goal is to manage rather than avoid risk. This report describes a security architecture methodology that takes as the base the existing enterprise architecture, risk management approach, and cyber security strategy.

2.1 Changing Grid Environment

The technology environment is constantly changing and this is impacting the electric sector and cyber security. In general, these changes are making the cyber security environment more complex and the attack surface larger. Some of these changes are listed below:

- With the deployment of distributed energy resources (DER), utilities are modifying the overall grid architecture – and this requires considering centralized versus distributed application of technology. With distributed applications, remote access to substations, control centers, and devices is increasing. In general, remote access to OT systems is through an enterprise IT system.
- Many utilities are considering consolidating their IT security operations, OT security operations, and physical security in an integrated security operations center (ISOC) to address the new cyber security environment.
- Deployment of cloud computing. Cloud computing provides for network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services).
- Grid modernization. With the increased deployment of digital technology and capabilities, insiders have increased functionality and access to data. With increased privileges, insiders have greater opportunity to compromise systems. Addressing the insider threat and determining how to represent them in the security architecture still needs to be determined.

All of these changes should be reflected in the security architecture that must be adaptable and resilient while ensuring reliability.

2.2 Terms

Section 1 of this report includes an overview of the terms enterprise architecture and security architecture. Included below are architecture terms and concepts from referenced documents. They are included as background and were used in developing the scope of this project. Note: this is not intended to be a comprehensive review of the literature.

There are several definitions related to an architecture. The definition of an architecture used in ANSI/IEEE Std. 1471-2000 is:

> "The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution."

The Open Group Architecture Framework (TOGAF) does not strictly adhere to the ANSI/IEEE Std. 1471-2000 terminology. In TOGAF, "architecture" has two meanings depending upon its contextual usage:

1. A formal description of a system, or a detailed plan of the system at component level to guide its implementation.
2. The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time.

There are two other concepts applicable to an architecture, as defined by TOGAF.

> An *architecture framework* is a tool that can be used for developing a broad range of different architectures. It should describe a method for designing an information system in terms of a set of building blocks, and for showing how the building blocks fit together. It should contain a set of tools and provide a common vocabulary. It should also include a list of recommended standards and compliant products that can be used to implement the building blocks.
>
> An *architecture description* is a formal description of an information system, organized in a way that supports reasoning about the structural properties of the system. It defines the components or building blocks that make up the overall information system, and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system.

According to the ISO/IEC/IEEE 42010-2011 standard:

> An architecture framework includes:
>
> > Conventions, principles and practices for the description of architectures established within a specific domain of application and/or community of stakeholders.
>
> An *architecture description* is a work product used to express an architecture.

This report does not include architecture frameworks or descriptions.

3
SECURITY ARCHITECTURE METHODOLOGY

Based on a risk assessment strategy, the systems should be prioritized and the security objectives of confidentiality, integrity, and availability specified for each system. A security architecture should address the requirements and potential risks for each system that is implemented in a specific operational environment. The security architecture should also identify where to apply security controls and applicable standards/guidelines. A security architecture should be overlaid on an existing system/enterprise architecture that may include, for example, the various devices, communications links, communications protocols, operating systems, applications, and data. The security architecture should augment the existing architecture and include the attack vectors, potential vulnerabilities, and mitigation strategies. Output from a cyber kill chain analysis can be used in developing the target security architecture.

As described previously, the development of a security architecture should be one component of an overall cyber security risk management strategy and should facilitate the objectives to manage exposure to business risk. The security architecture may be used as input to evaluating the likelihood and impacts of security threats and vulnerabilities. A security architecture can be developed for the current system and for the target system. These security architectures can then be used to:

- Identify cyber security gaps and mitigation strategies to address these gaps,
- Perform a cyber kill chain analysis,
- Assess the operational implementation,
- Ensure that the overall cyber security risk management strategy is mirrored in the mitigation strategies,
- Assist in the analysis of new threats, technologies, and vulnerabilities.

3.1 Reference Security Architecture

The development of security architectures for all systems within a utility is a significant task. Initially, the scope of this project was to develop a high level security architecture methodology that could be applied to all IT and OT systems within a utility. However, this methodology would require extensive time to develop, review, and revise prior to use within an organization. Alternatively, the security architecture methodology included in this report focuses on one domain of the grid – substations for distribution and transmission. The goal is to provide a practical approach that is timely. The substation security architectures are developed as *reference architectures*.

A reference architecture provides a template solution for a particular domain and is not intended to represent a specific implementation. It is a specification that defines the overall structure (components and relationships among them) in a systematic, consistent manner. The architecture also includes a common vocabulary and rules. Any reference architecture should be tailored by each utility to represent the current system implementations and the future configurations. Included in this report are three substation reference architectures: legacy, transition, and future.

Including the three reference architectures was based on feedback, with the goal of addressing the current architecture and associated vulnerabilities and planning for the transition and target (future) architectures. By looking forward, a utility can be more proactive in identifying potential vulnerabilities and attack vectors and determining a mitigation strategy based on an acceptable level of risk.

In the first version of this report, the reference architecture diagram included three overlay layers: information, communications, and component/technology. Upon further analysis, this overlay layer approach was not used because concentrating on layers focuses on individual elements, such as servers, gateways, and substation buses, rather than on their functionality in the operational environment. Identifying the attack surface and attack vectors depends on device functionality in the operational environment. Rather than focusing on layers, the revised methodology includes system and device categories and their functionality/roles. These categories are used in determining the attack vectors and mitigation strategies.

3.2 Cyber Kill Chain

One of the major challenges for the electric sector is addressing the constantly changing threat environment. Many of the OT devices have life cycles of 30 to 40 years, and utilities will be required to upgrade/modify the embedded software and firmware. In addition, commercially available communication protocols, applications, and operating systems need to be patched for new vulnerabilities. Finally, zero day vulnerabilities may be exploited by attackers prior to the deployment of patches. Utilities need to understand the attack process to develop and implement mitigation strategies.

In 2011, Lockheed Martin created the Cyber Kill Chain™ to help the decision-making process for better detecting and responding to adversary intrusions[1]. This model was adapted from the concept of military kill chains. The ICS kill chain[2] was developed by individuals from the SANS Institute and augments the original kill chain and tailors it for control systems. The original cyber kill chain and the associated ICS Cyber Kill Chain are displayed in Figure 3-1 and Figure 3-2 below.

[1] Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin, Ph.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains".
www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

[2] *The Industrial Control System Cyber Kill Chain,* Michael J. Assante and Robert M. Lee, October 2015, The SANS Institute InfoSec Reading Room.

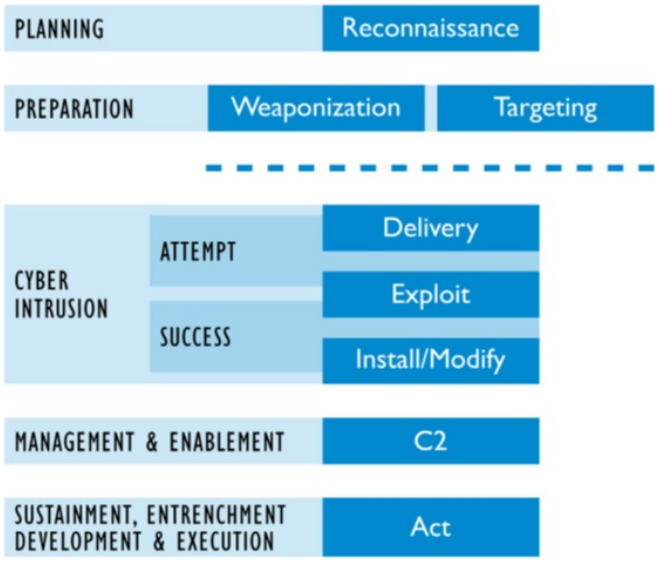


Figure 3-1
Cyber Kill Chain – Stage 1: Cyber Intrusion Preparation and Execution

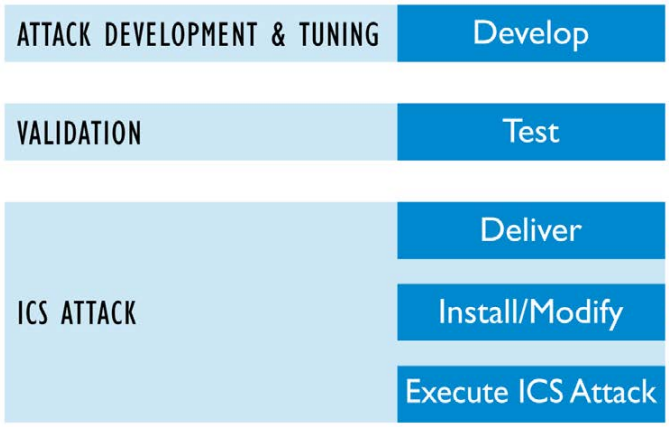


Figure 3-2
ICS Cyber Kill Chain – Stage 2: ICS Attack Development and Execution

The steps in the Lockheed Martin chain are as follows:

- *Reconnaissance*: the attacker finds a gap in security of the social network
- *Weaponization*: builds a malicious attachment
- *Delivery*: and delivers it using social media or email targeting an employee
- *Exploitation*: the employee opens the file and the vulnerability is exposed
- *Installation*: malware immediately installs on the client
- *Command & Control*: the attacker takes control of the system
- *Actions on Objectives*: and is able to pinpoint and access critical data

The tailored ICS cyber kill chain includes the following steps and descriptions that are extracted from the ICS Kill Chain document[3]. This is an overview and additional details are included in the SANS document.

Stage 1: Cyber Intrusion Preparation and Execution

- *Planning and Reconnaissance*: *Reconnaissance* is an activity to gain information about something through observation or other detection methods. The objective of the Planning step is to reveal weaknesses and identify information that support attackers in their efforts to target, deliver and exploit elements of a system.
- *Preparation:* Preparation can include weaponization or targeting. *Weaponization* includes modifying an otherwise harmless file, such as a document, for the purpose of enabling the adversary's next step. Targeting occurs when the adversary or its agent (such as a script or tool) identifies potential victim(s) for exploitation.
- *Cyber Intrusion*: An *intrusion* is any attempt by the adversary, successful or not, to gain access to the defender's network or system. This includes the *Delivery* step, in which the adversary uses a method to interact with the defender's network. The next step, the *Exploit step*, is the means the adversary uses to perform malicious actions. When the exploitation is successful, the adversary will *install* a capability and may also, or instead, *modify* existing capabilities.
- *Management and Enablement:* Here the actor will establish *command and control* (C2). With managed and enabled access to the environment, the adversary can now begin to achieve his or her goal.
- *Sustainment*, *Entrenchment*, *Development*, and *Execution:* In this step, the adversary *acts*. This can be a critical phase for the planning and execution of Stage 2 of the ICS Cyber Kill Chain.

Stage 2: ICS Attack Development and Execution

- *Attack Development and Tuning phase*. The aggressor develops a new capability tailored to affect a specific ICS implementation and for the desired impact. This development will most likely take place through exfiltrated data.
- *Validation*: Here, the attacker must *Test* his or her capability on similar or identically configured systems if the capability is to have any meaningful and reliable impact.

ICS Attack: the adversary will *deliver* the capability, *install* it or *modify* existing system functionality, and then *execute* the attack. The security use cases vulnerabilities and descriptions may be allocated to the applicable ICS Kill Chain steps. This is useful in determining when the mitigation strategies should be implemented.

[3] *The Industrial Control System Cyber Kill Chain,* Michael J. Assante and Robert M. Lee, October 2015, The SANS Institute InfoSec Reading Room.

4
SUBSTATION DEVICE CATEGORIES

There are a wide range of intelligent devices and systems in use at substations across the power grid. This document divides these devices and systems into a number of categories by role. Within each category, a number of example devices are listed to clarify the scope of the category. These lists are not intended to be comprehensive.

4.1 Automated Protection Systems

These systems have direct control or influence on the station switchgear and are designed to operate without requiring any manual actions. Typical equipment in this category is tasked with the protection of power system equipment or automated controls that help correct power system issues. The following list contains examples of protection systems.

1. Relays
2. Programmable Logic Controllers (PLC)
3. Substation Automation Controller

4.2 Manually Initiated Systems

These systems also have direct control or influence on the station switchgear but are designed to be operated manually. They are typically controlled by operators either locally or at one or more centralized control centers. The capability to access equipment remotely is important when evaluating cyber security for a substation architecture. The following list contains examples of devices that are manually initiated.

1. SCADA Remote Terminal Unit (RTU)
2. SCADA Gateway/Protocol Converter
3. Dedicated Human Machine Interface (HMI)

4.3 Monitoring and Measurement Systems

When operating an unmanned substation, many states and conditions must be monitored and recorded for a number of operational and maintenance reasons. The devices within this category are responsible for the collection of that data. From a hardware perspective, many of the devices in this category may be similar to those in both the automated and manual control categories. The key difference for these devices is the lack of direct control over, or operation of, the high voltage equipment.

Even though they do not have direct control, these devices play a critical role in the operations and maintenance of the power grid. Information from these systems may cause an operator to make a manual control decision. Additionally, measurements or conditions observed by these systems may be used as input to an automated protection scheme. The following list contains examples of monitoring and measurement systems. Included in this category are two subcategories based on the function that a given device is designed to support. System monitors are used to report the state of the power system while asset health monitors are deployed to provide insight into the health of a key asset.

System Monitors

1. Power Quality Monitor
2. Phasor Measurement Unit (PMU)
3. Meters
4. Intelligent Transducer

Asset Health Monitors

1. Transformer Monitor
2. Circuit Breaker Monitor

4.4 Communications Systems

Communications are used to facilitate the exchange of information among devices in the other categories and systems external to the substation. This exchange of information may occur within the substation, between the substation and remote locations, and between the substation and a control center. This category includes serial based devices, packet based devices, and devices used to translate between serial and packet systems. In addition to an array of devices, the infrastructure used for communications between the devices is multi-faceted. These facets can be broken down into two primary groups, range and ownership. Communications ranges from short to medium and long distances. Ownership can be any combination of Utility, third party, or a combination of the two. The following list contains some examples of communication devices.

1. Ethernet switches
2. Routers
3. Modems
4. Digital Protection Units (Pilot Protection Channels)
5. Terminal Servers
6. Channel Banks
7. Phone Line Switches
8. Fiber Optic Terminals
9. Microwave Terminals

4.5 Support Systems

The support system category contains the substation devices and systems that do not play a direct role in the operation of the grid, but can be critical to the proper operation of devices listed in the other categories. These devices provide primary and backup power along with providing a time reference where required. The following list contains examples of support systems.

1. GPS Clocks
2. 48V-125VDC Battery Chargers
3. 48V-125VDC Power Distribution
4. 120VAC Station Service Distribution

4.6 Primary Power Equipment Systems

In the categories listed above, all systems and devices share the characteristic of being electronic and programmable. These systems and devices may also be called “cyber” assets. In addition to these systems and devices, a typical substation also includes primary power equipment systems and devices. This equipment is responsible for carrying power and interrupting or reconfiguring the flow of power through the substation.

Many of the primary power equipment systems and devices may evolve over time into processor-based assets. One such example is the instrument transformer. In its current form it uses electromagnetic induction to convert voltage and current down to a more convenient level for use by protection or measurement systems. This conversion is controlled by mechanical connections and the transformer does not contain any programmable components. In the future, some instrument transformers may be replaced with a programmable device that samples the current or voltage values using a high sample rate. The devices then publish the sampled values for use. Examples of primary power equipment substation devices are listed below:

1. Instrument Transformer
2. Power Transformer
3. Circuit Breaker
4. Capacitance Coupled Voltage Transformer (CCVT)

4.7 Security Mitigation Strategies

While the categories included above contain systems that enable or support the delivery of power, security mitigation strategies contain categories focused on the protection of the substation devices and systems. The example systems listed below have been divided into two categories. The first category is focused on the cyber security of the substation while the second category is focused on physical security.

4.7.1 Cyber Security Systems

Cyber security systems protect intelligent substation devices and data from any potential compromise of availability, integrity, and confidentiality. The following list contains examples of cyber security systems.

1. Firewall
2. Intrusion Detection System (IDS)
3. Intrusion Prevention System (IPS)
4. Security Gateway
5. Log Collector
6. Security Proxy Server

Physical security systems are deployed at substations to control and monitor physical access to the site. For this report, the focus is on data received from these devices and its correlation with data from cyber security systems. Therefore, these devices are included under Cyber Security Systems. The following list contains examples of physical security systems.

1. Card Access Readers
2. Card Access Controller
3. Video Camera
4. Digital Video Recorder (DVR)

5
SUBSTATION REFERENCE SECURITY ARCHITECTURES

Included below are the substation reference security architecture diagrams with devices that are common to a substation. The diagrams are not intended to include all the various devices that may be located at a substation, rather they include devices that are representative of each device category listed above. These diagrams should be revised to replicate the specific planned and proposed substation configurations. There may be variations depending on the size of the substations and/or whether they are for transmission or distribution.

Included are three diagrams: legacy, transition, and future with the device categories highlighted in different colors. The device categories and color coding include:

Automated Protection Systems

Manually Initiated Systems

Monitoring and Measurement Systems

Communications Systems

Support Systems

Primary Power Systems

Cyber Security Systems

The differences between the three architectures are:

- Legacy substations typically consist of electromechanical control systems and a small number of single purpose programmable devices with limited resources and capabilities. Coordination among devices is typically done by wiring inputs and outputs between terminal blocks. All communication interfaces and protocols are relatively simple and often proprietary.

- Transition substations begin to leverage microprocessor based devices that may perform the functions of multiple electromechanical devices. Serial communications protocols have increased in complexity and evolved toward more use of open standards.
- Future substations rely on high speed sampling to convert inputs and outputs into logic states and values that can be exchanged among different multipurpose devices. As the function each device performs becomes abstracted from the hardware, complexity in device software and configuration increases. Newer protocols leverage techniques like self-description to deal with the new complexity.

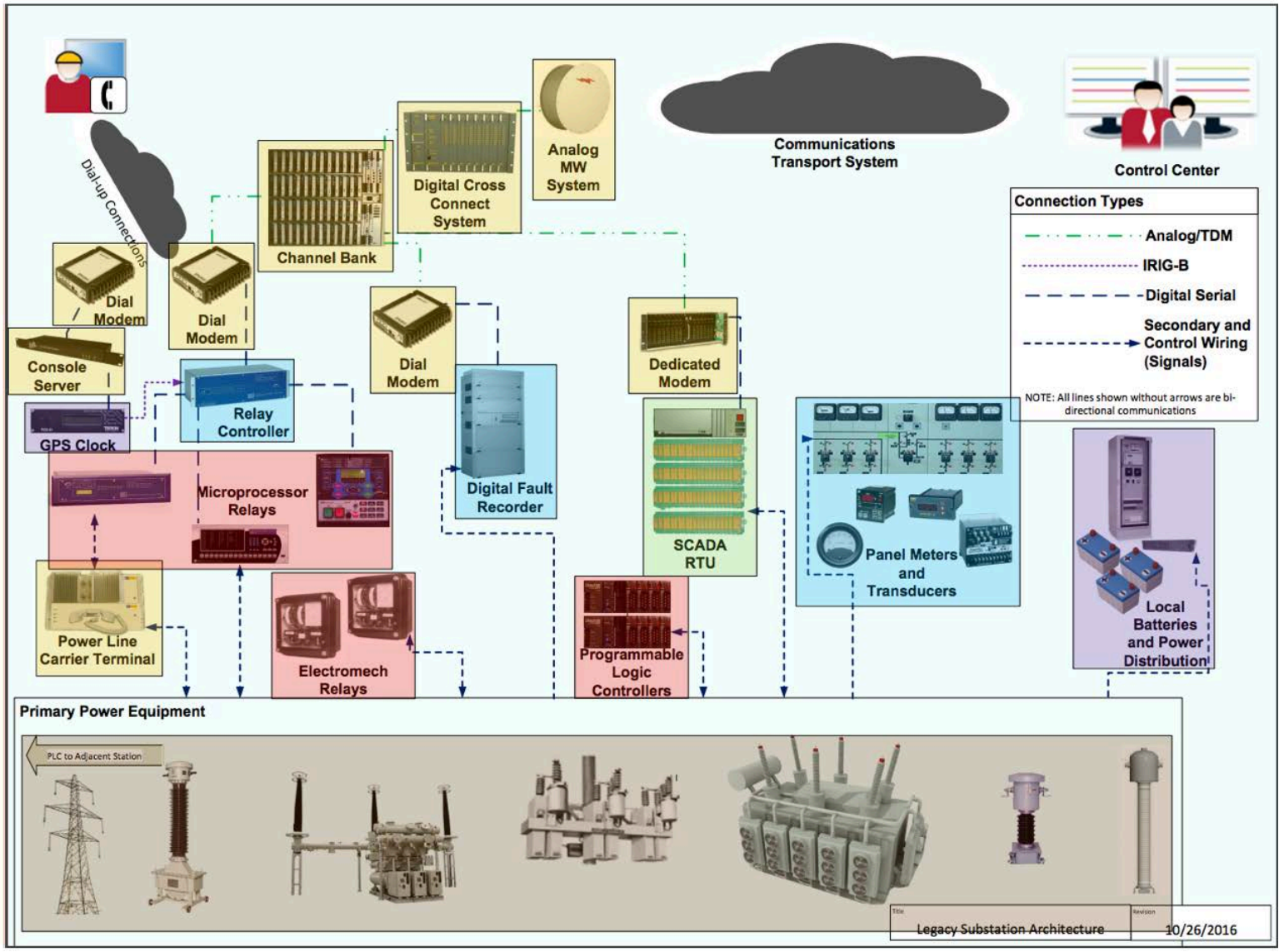


Figure 5-1
Legacy Substation Security Architecture

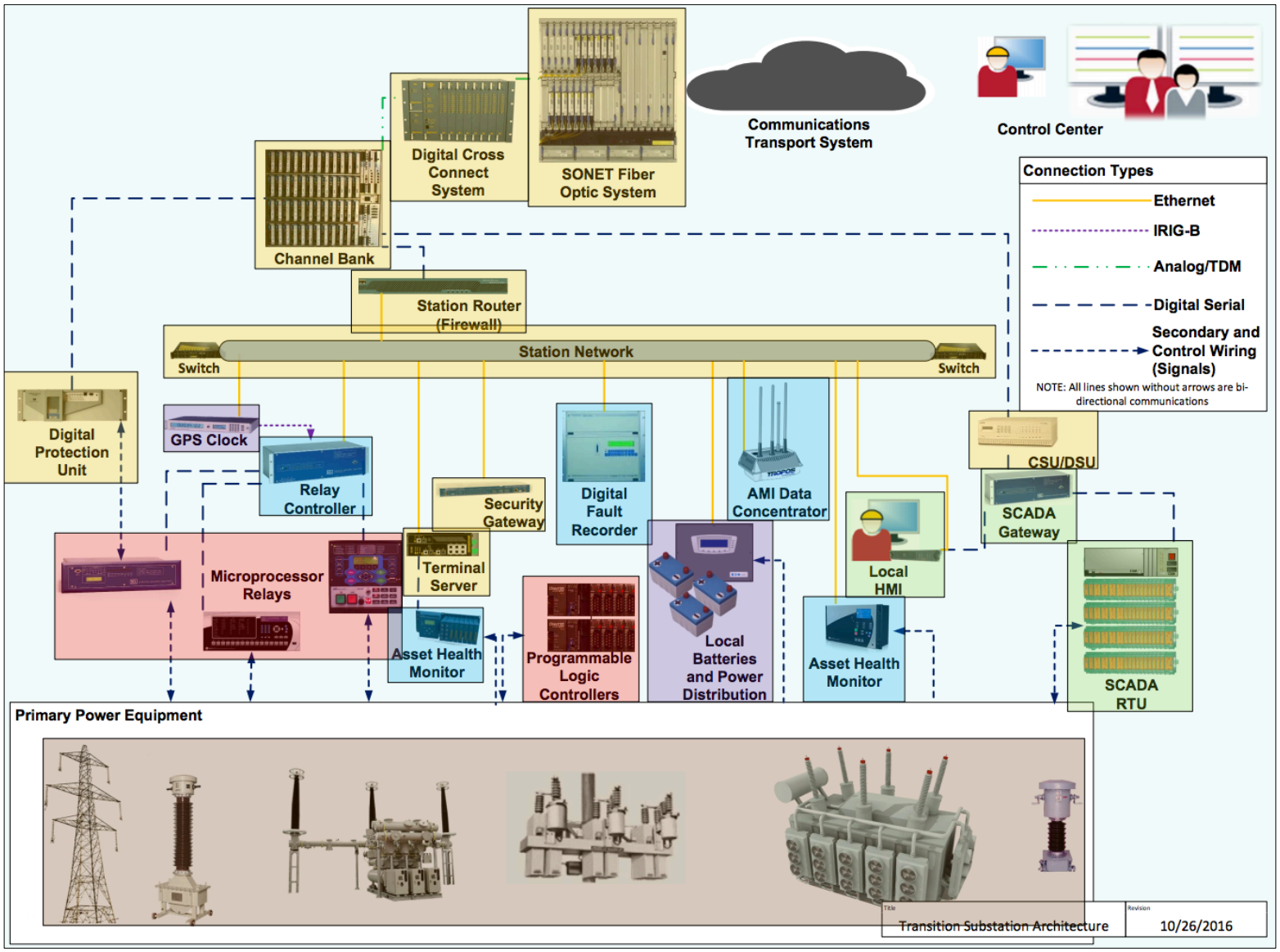


Figure 5-2
Transition Substation Security Architecture – All Device Categories

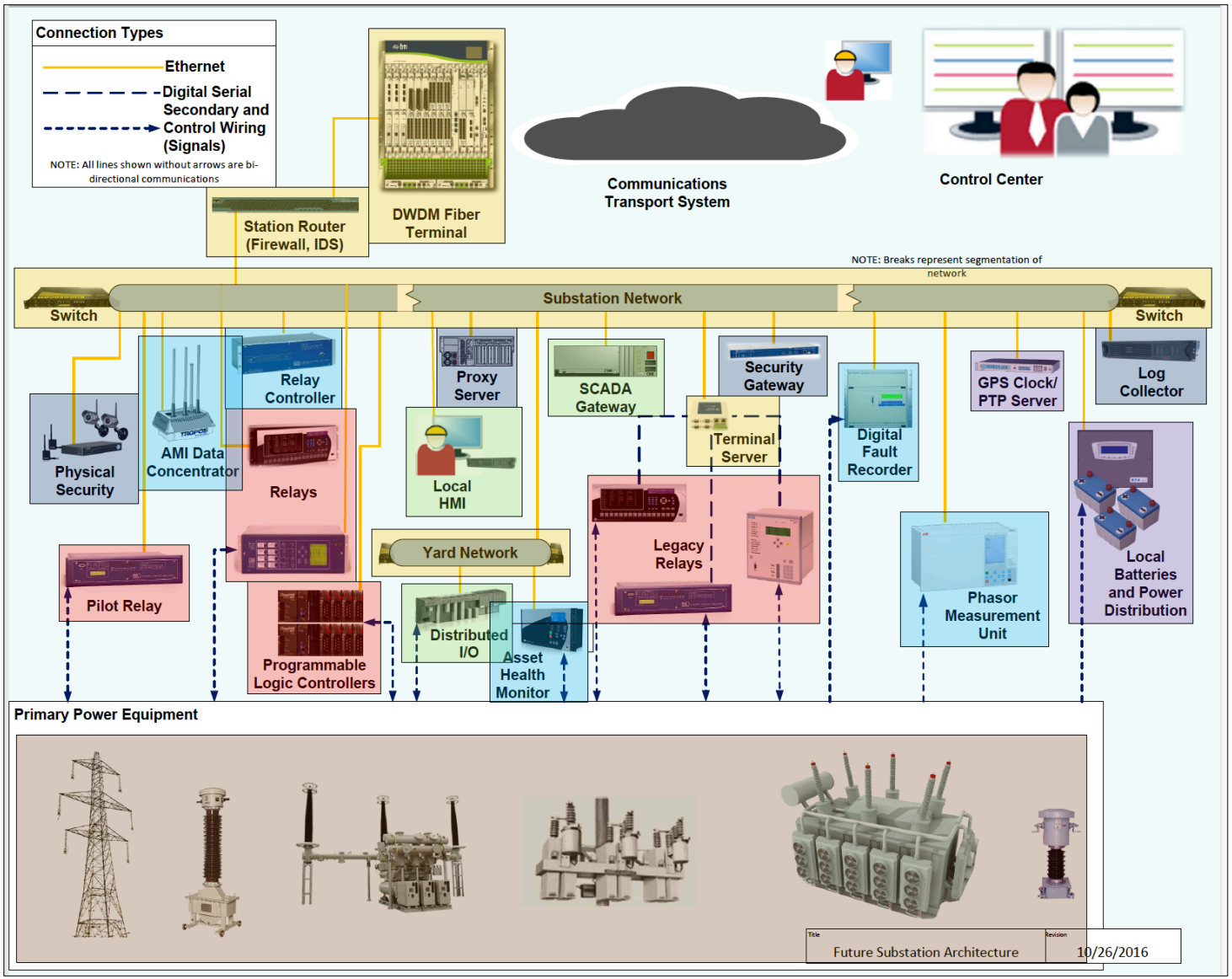


Figure 5-3
Future Substation Security Architecture

A security architecture should be developed as part of the overall security assessment methodology, as illustrated in Figure 5-4. Included below are descriptions of the various steps in the security architecture methodology and the associated risk assessment methodology phase. Each phase is underlined in the descriptions below.

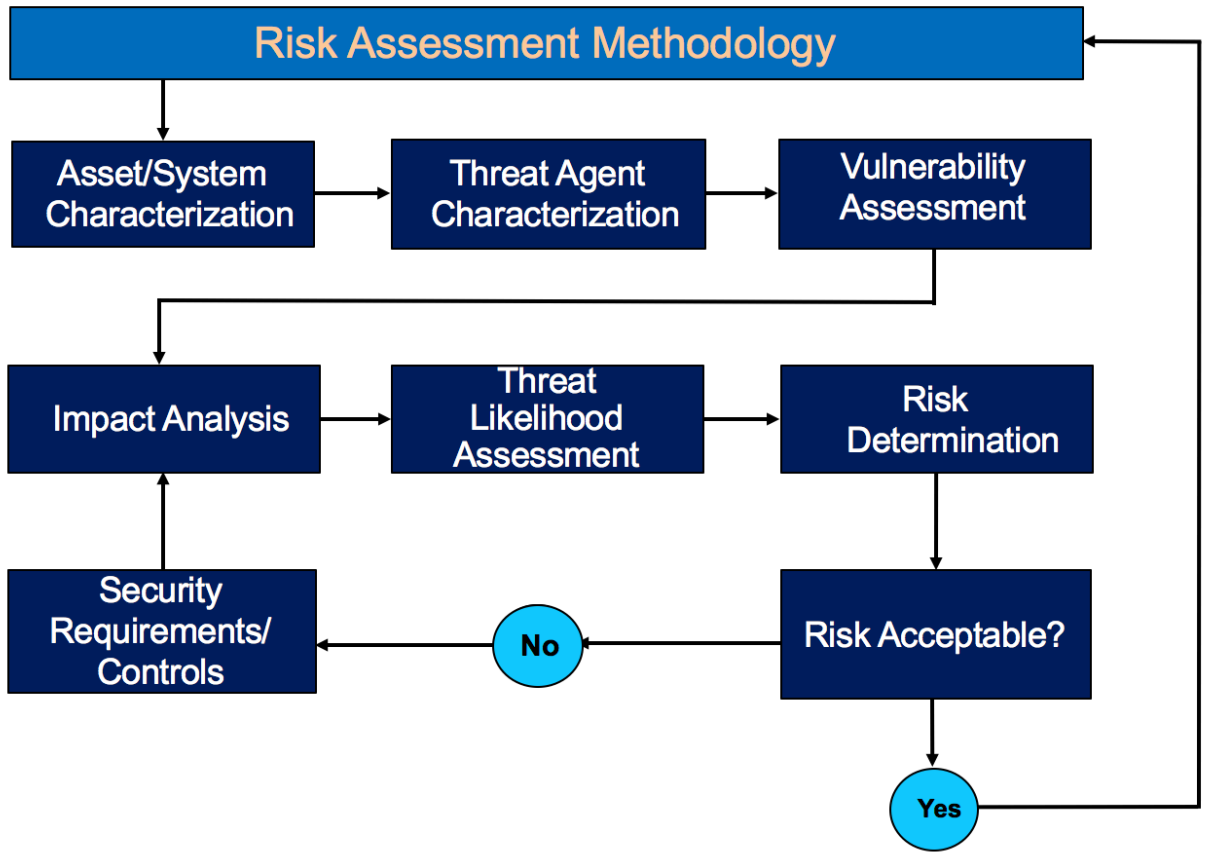


Figure 5-4
Security Risk Assessment Methodology

5.1 Step 1: Identify the Substations

The first step is to identify the substations (*Asset/System Characterization*) that will be included in the security architecture. The utility may select the substations based on their criticality or whether they are scheduled to be upgraded. In the risk assessment process used to prioritize the various systems, the set of threat agents should be reviewed and the applicable threat agents identified (*Threat Agent Characterization*). Included in the NESCOR Electric Sector Failure Scenarios and Impact Analyses document is a list of threat agents. It is included in Appendix B of this report for reference.

5.2 Step 2: Revise the Reference Architecture Diagrams

The reference architecture diagrams need to be revised to reflect the implemented and planned implementation configurations at the utility. A utility may decide to only develop legacy and future security architectures, or develop all three. When the reference architectures have been developed, the devices should be allocated to the various device categories. The device lists in

each category in this document are intended to be representative and not comprehensive. Therefore, a utility may identify a specific device that is not included in the lists in this document. The utility should add the device to the applicable category.

5.3 Step 3: Select the Security Use Cases

After the diagrams are created, the security use cases should be selected from the set included in this report. These use cases are at a high level, and should be tailored to the specific implementation. A utility may need to develop additional use cases using the template illustrated in the use cases in this report.

5.4 Step 4: Specify the Attack Surface and Attack Vectors

The next step is to identify the attack surface and attack vectors (*Vulnerability Assessment*). Included in this report are the security use cases based on the National Electric Sector Cybersecurity Organization Resource (NESCOR) failure scenarios. These security use cases, included in Appendix C of this report, were initially selected based on their applicability to substations. Each use case includes the original content of the failure scenarios:

- Description
- Relevant Vulnerabilities
- Impact
- Potential Mitigations

In addition, the following is added to each security use case:

- Device categories
- Applicability to legacy, transition, or future diagram
- Vulnerabilities allocated to the device categories
- Mitigations allocated to device categories

The attack surface and attack vectors can be developed from several sources, including the vulnerabilities and vulnerability classes included in the *NESCOR Failure Scenarios and Impact Analyses document*.

Included in each security use case is a description of the impact (*Impact Analysis*) of the security event.

Note: The *Threat Likelihood Assessment* should be determined by a utility when tailoring the security use case to a specific substation(s) implementation.

5.5 Step 5: Select Mitigation Strategies

The final step is to determine the risk level (*Risk Determination*) and select the mitigation strategies (*Security Requirements/Controls*) to address the various attacks based on the level of acceptable risk to the organization. The mitigation strategies include risk acceptance, risk mitigation, and remediation. In the risk acceptance strategy, the risk may be transferred. In the risk mitigation strategy, the risk is reduced and in remediation, the risk is fixed. This report lists potential risk mitigation and risk remediation strategies.

6
SECURITY USE CASES EXAMPLES

Included in this chapter are two security use cases: Wide Area Monitoring, Protection, and Control (WAMPAC) and Generic and the associated reference architecture diagrams. The substation categories that are applicable to the different sections of the use case are highlighted in red. The substation categories are assigned to all three architectures: legacy, transition, and future, as applicable. There is one additional category that is included in the mitigations section: Design, policies, and procedures. This category includes the non-technical mitigation strategies. As shown in the two examples, the applicable substation categories may be different for the relevant vulnerabilities, impact, and potential mitigations sections of the use case.

6.1 WAMPAC.1 Denial of Service Attack Impairs PTP Service

Description: A set of Phasor Measurement Units (PMUs) receive their time via network communication from a Precision Time Protocol (PTP) server. A threat agent is able to perform a denial of service attack against PTP either by leveraging vulnerabilities in the PTP service itself or by flooding it with high volume of traffic or malformed packets targeting open ports that are not required by PTP. This leads to delays or lack of functionality of the PTP service, translating into the inability of the PMUs to correctly timestamp their measurements.

Substation Categories:

- Communications Systems – Future
- Support Systems – Future

Relevant Vulnerabilities:

- *Network interfaces permit unnecessary traffic flows* for the network hosting the PTP server, (Communications Systems)
- *Unnecessary system services are configured to run* on the PTP server, (Support Systems)
- *Unnecessary access is permitted to critical functions* in the PTP service. (Support Systems)

Included in Figure 6-1 below are the various devices included in the Communications Systems and Support Systems categories that may include the listed relevant vulnerabilities.

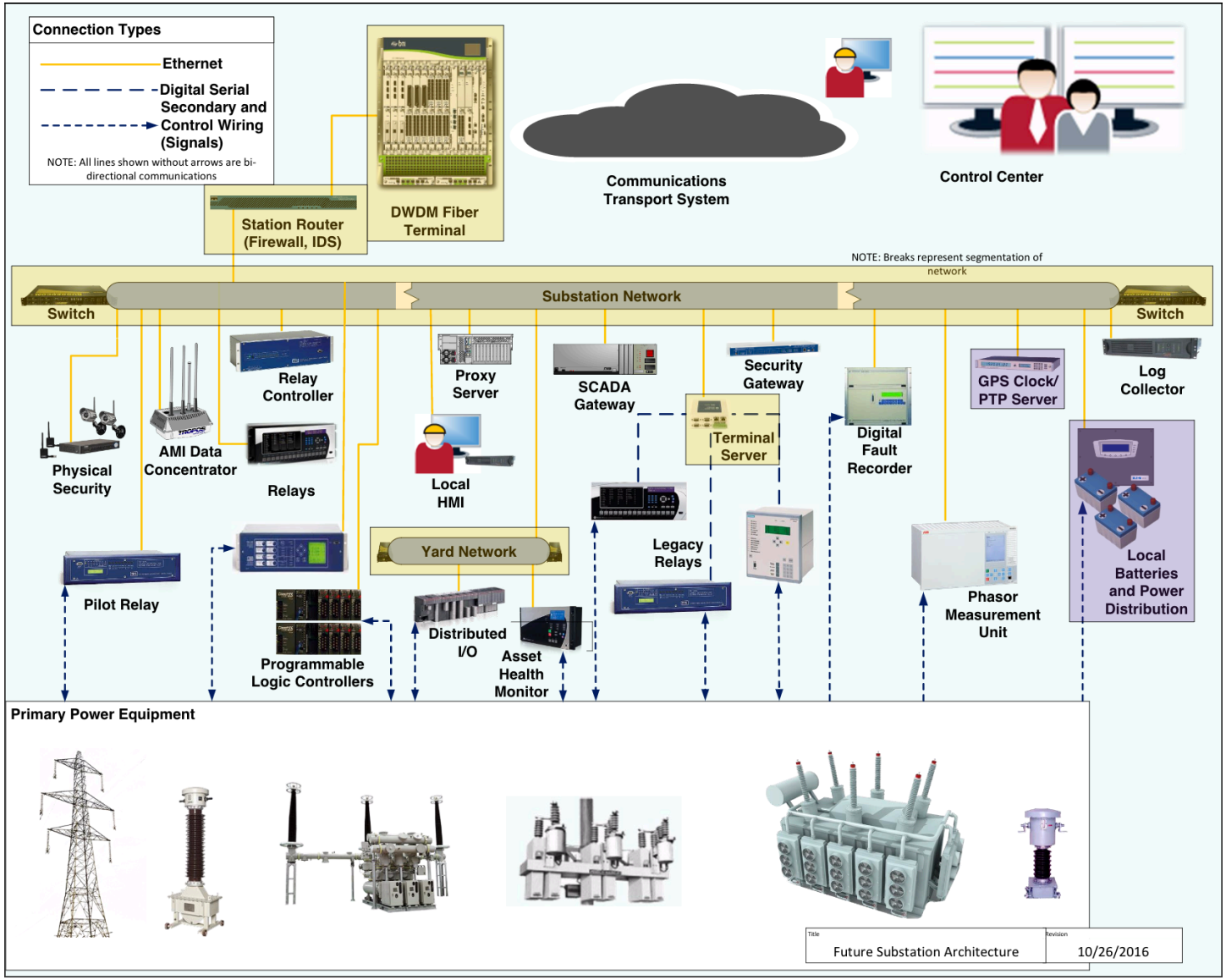


Figure 6-1
WAMPAC.1 Future Security Architecture Relevant Vulnerabilities

Impact:

- All impacts presented in Table 6-1, are potentially caused by loss of measurements due to lack of time synchronization.

Table 6-1
Impact Examples by Type of WAMPAC Application

		Alert/Emergency
Monitoring	*Data loss*	• Delay in taking actions (e.g., load shedding) • Delay in grid reconfiguration • Unnecessary power generation, overload of lines, or creation of fault conditions, if timely or appropriate corrective actions are not taken
	Altered data	• Incorrect actions to be taken
Local Protection	*Data loss*	• Failure in taking action, if no alternative data source is available
	Altered data	• Line trip, which can lead to cascading failures if lines are overloaded and other protection takes place • Improper synchronous closing, leading to equipment damage
Special Protection	*Data loss*	• Delay in triggering protection elements • Overload of lines, or creation of fault conditions, if timely or appropriate corrective actions are not taken
	Altered data	• Line trip, which can lead to cascading failures if lines are overloaded and other protection takes place • Improper synchronous closing, leading to equipment damage
Control	*Data loss*	• Delay in taking actions (e.g., load shedding) • Delay in grid reconfiguration • Unnecessary power generation, overload of lines, or creation of fault conditions, if timely or appropriate corrective actions are not taken
	Altered data	• Failure to take action, when needed, leading to voltage or frequency conditions that could have been prevented • Cascading failures

As illustrated in Figure 6-2 below, the impact is applicable to a different set of substation categories than the categories listed for relevant vulnerabilities. The Communications Systems category is not included and the Monitoring and Measurements Systems (PMU) and the Primary Power Equipment Systems (Primary Power Equipment) has been included.

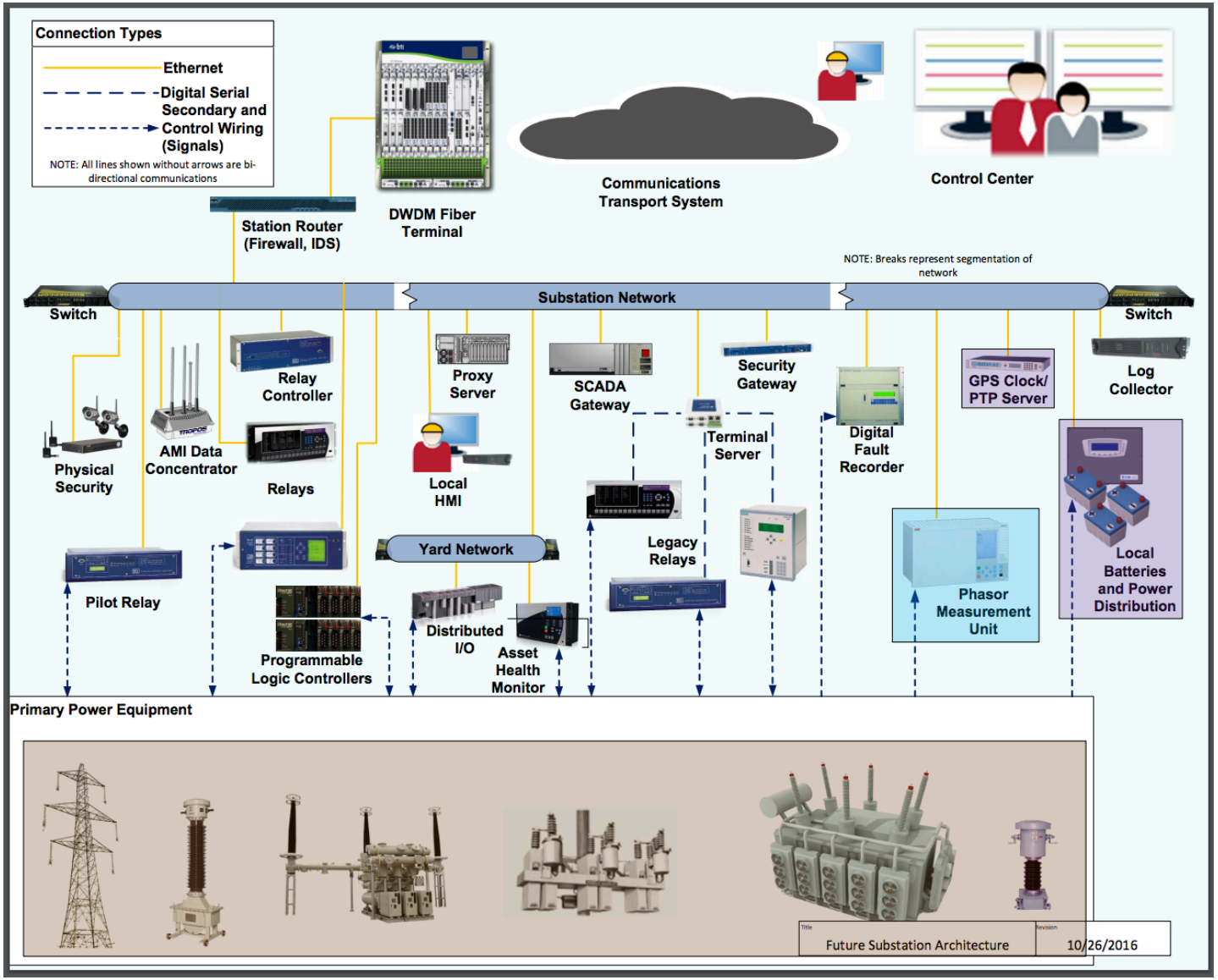


Figure 6-2
WAMPAC.1 Future Security Architecture Impact

Potential Mitigations:

- *Restrict network service access* to the PTP service, (Support Systems)
- *Isolate functions* between the PTP service and the auxiliary services running on the same server (for example, resource prioritization), (Design, policies, and procedures)
- *Configure for least functionality* the PTP server, (Support Systems)
- *Verify correct operation* of the PTP server in order to remain operational when subjected to erroneous traffic and large amounts of traffic in the network stack, PTP and required auxiliary services, (Design, policies, and procedures)
- *Require intrusion detection and prevention*, (Cyber Security Systems)
- *Restrict network access* to the network hosting the PTP server, (Communications Systems)
- *Restrict access* to the GPS clock (locally or via the network). (Support Systems)

Included in Figure 6-3 below are the substation categories used for the potential mitigation strategies. The two categories listed in Relevant Vulnerabilities are included with the addition of Cyber Security Systems and Design, policies, and procedures.

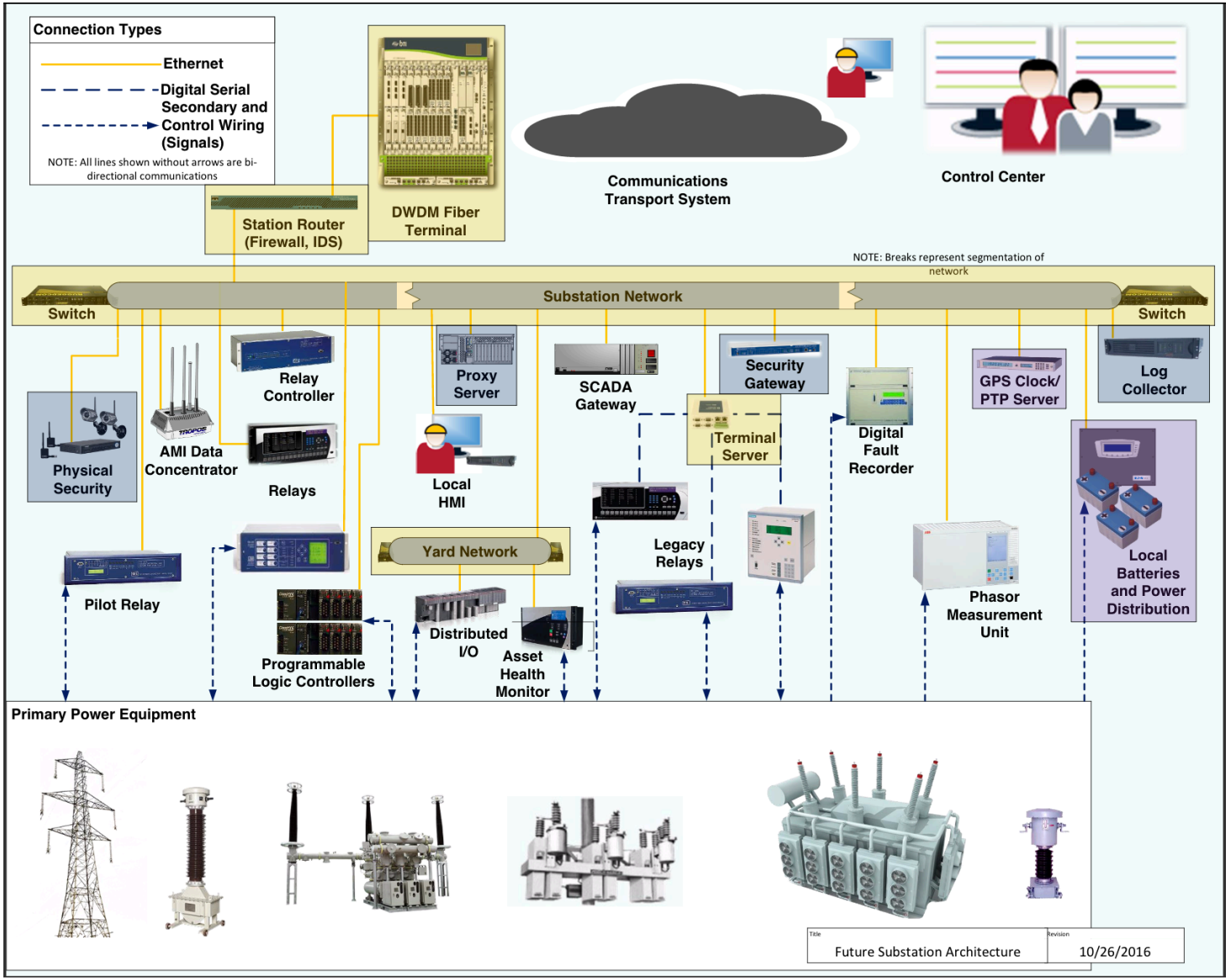


Figure 6-3
WAMPAC.1 Future Security Architecture Mitigation Strategies

6.2 Generic.2 Inadequate Network Segregation Enables Access for Threat Agents

Description: A threat agent compromises an asset that has access to the Internet via the "business" network. The asset on the business network also has access to a control system asset or network. The compromise of the business network asset provides a pivot point for the threat agent to gain control of a control system asset or network.

Substation Categories:

- Automated Protection Systems – Transition, Future
- Manually Initiated Systems – Transition, Future
- Monitoring and Measurement Systems – Transition, Future
- Communications Systems –Transition, Future
- Support Systems – Transition, Future
- Cyber Security Systems – Transition, Future

Relevant Vulnerabilities:

- *Network interconnections provide users and hardware/software entities with access unnecessary for their roles* such as using virtual local area networks (VLANs) for security or using the same networks for business operations and control systems, (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)
- *Remote access may be obtained by unauthorized individuals* (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)
- *Network is connected to untrusted networks* that are viewed as trusted, specifically the control systems network is connected to the business network and views the business network as trusted. (Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)

Included in Figure 6-4 below are the various device categories that may include the listed relevant vulnerabilities. Because this use case is broad, most of the device categories are included. Although this use case is applicable to the transition and future architectures, only the transition architecture diagrams are included for illustration.

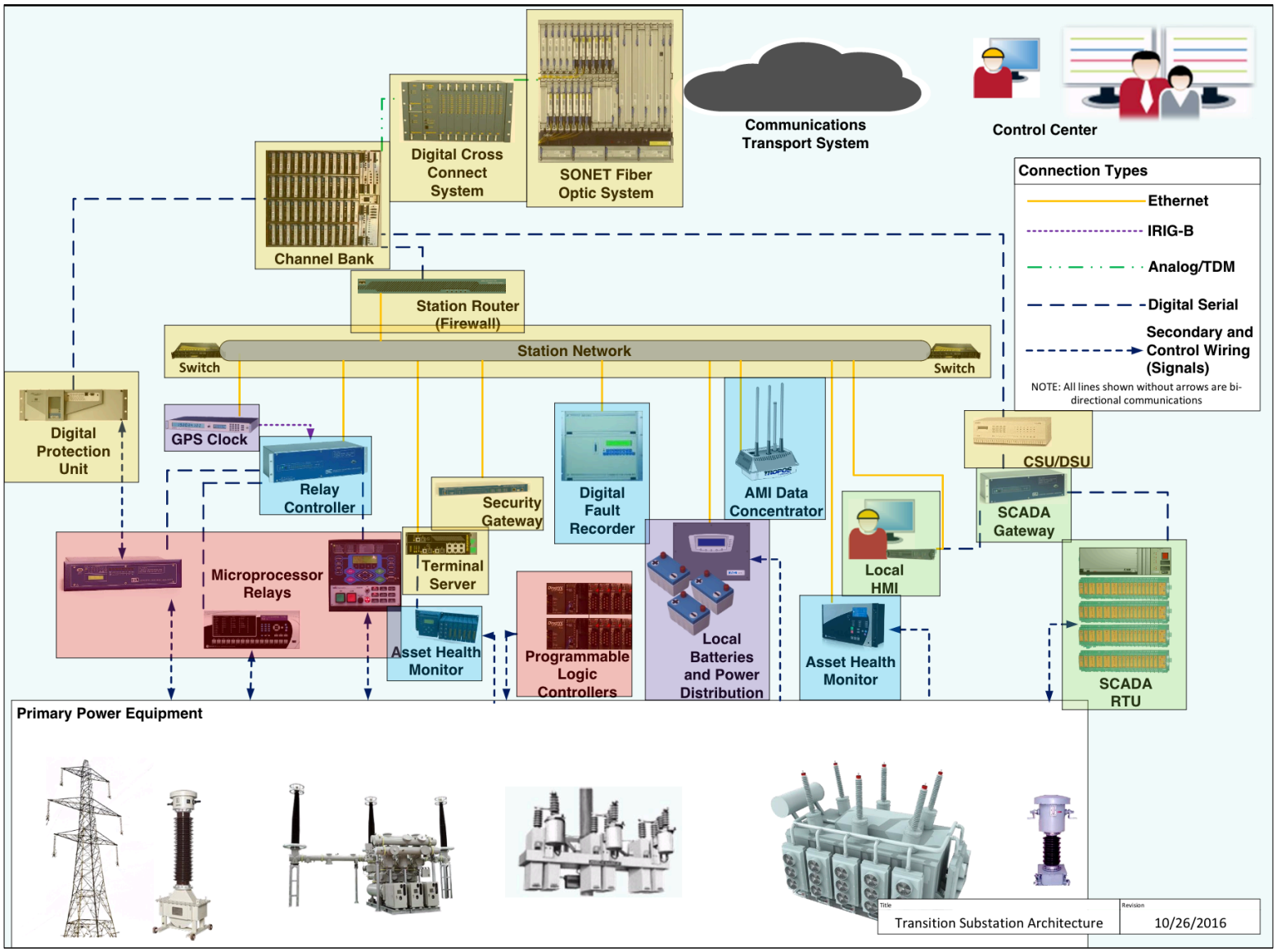


Figure 6-4
Generic.2 Transition Security Architecture Relevant Vulnerabilities

Impact:

- The impact for this scenario could range from a minor system being offline to a widespread outage of unknown duration.

As illustrated in Figure 6-5 below, all device categories are included as potential impacts.

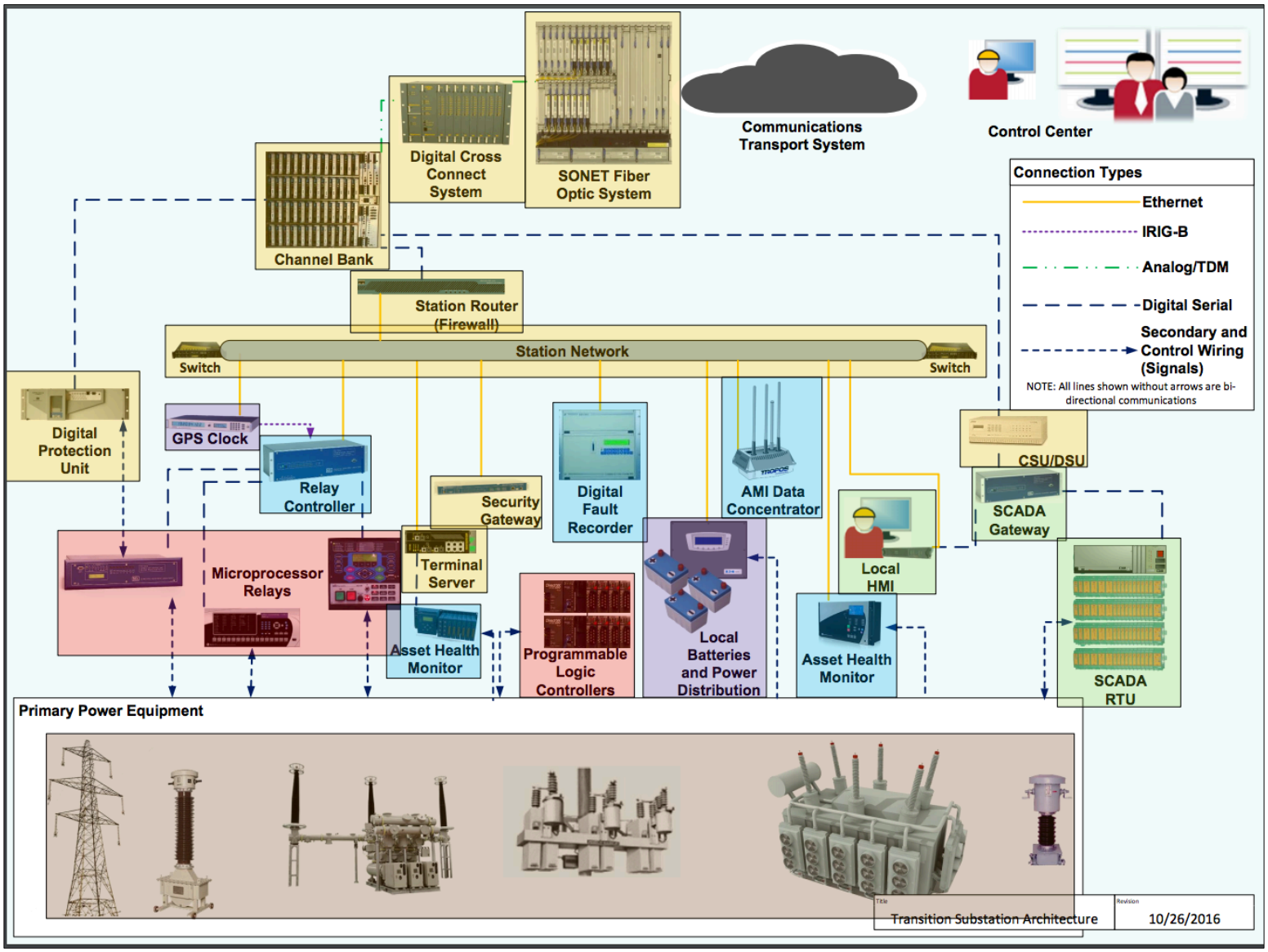


Figure 6-5
Generic.2 Transition Security Architecture Impact

Potential Mitigations:

- *Isolate networks* that host business systems from those that host control systems, (Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)
- *Generate alerts* using a Security Information and Event Monitoring (SIEM) solution and monitor alerts according to the associated risks. This includes alerts generated by firewalls, anti-virus, and specific systems, (Cyber Security Systems)
- *Isolate networks* with a defensible, defense in depth, network architecture which includes a demilitarized zone (DMZ), (Design, policies, and procedures)
- *Enforce restrictive firewall rules* to achieve network isolation, (Cyber Security Systems)
- Require intrusion detection and prevention, (Cyber Security Systems)
- *Train personnel* to monitor traffic to and from the Internet and to recognize when an incident is occurring, (Design, policies, and procedures)
- *Define incident response plan* to reduce response time when incidents do occur, (Design, policies, and procedures)
- *Define contingency plan* as part of the incident response plan, to maintain adequate resiliency in high-priority control systems. (Design, policies, and procedures)

All the device categories (except for the primary power equipment substation system and devices) and the Design, policies and procedures category are included.

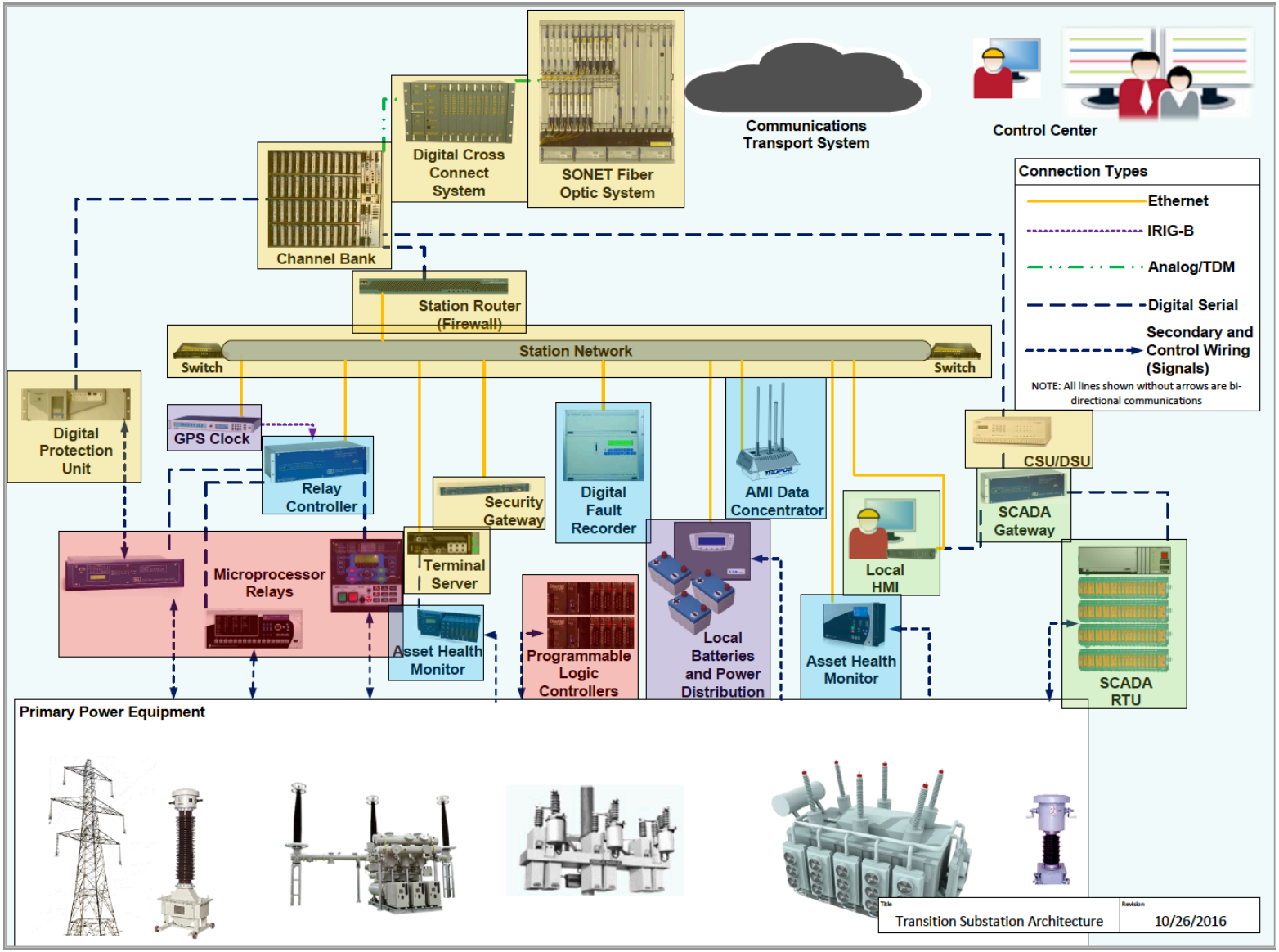


Figure 6-6
Generic.2 Transition Security Architecture Potential Mitigations

7
NEXT STEPS

A security architecture is one tool that utilities may use to define the current and target architectures including the attack surface and response strategies. In 2015, the focus was on a review of existing architecture methodologies and frameworks and how they can be used for security architectures. In 2016, the focus is on tailoring and applying the methodology to transmission and distribution substations. This report includes substation reference architecture diagrams and security use cases. The reference architecture diagrams were developed in collaboration with utilities who participated in the EPRI Cyber Security Program. The security use cases are input to testing projects being executed in the EPRI Cyber Security Research Laboratory (CSRL). This testing will continue in 2017. Once the substation security use cases are finalized, analysis will be performed to identify the most common attack methods, vulnerabilities, and mitigation strategies.

To ensure that the security architecture methodology is standardized across the electric sector, this report will be released publicly and feedback requested. The goal is to ensure that the methodology and associated terms and concepts are practical for utilities of all sizes and varying levels of sophistication in addressing cyber security. Future work will be coordinated with such organizations as NRECA, APPA, and EEI.

7.1 Future Research Topics

Some of the areas that will need future research to determine how they should be included in the security architecture are:

- Identification of the common vulnerabilities and mitigations for the various use cases in the device categories
- Specific technologies such as cloud computing and virtualization
- Insider threat
- Application to other electric sector domains, such as field devices.

8
REFERENCES

1. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, February 12, 2014 [report].
2. National Electric Sector Cybersecurity Organization Resource, *Electric Sector Failure Scenarios and Impact Analyses, Version 3.0*, December 2015. [report].
3. National Institution of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, Rev. 1, June 2014. [report].

A
ACRONYMS

ANSI	American National Standards Institute
APPA	American Public Power Association
CCTV	Capacitance Coupled Voltage Transformer
DER	Distributed Energy Resources
DOE	Department of Energy
DVR	Digital Video Recorder
EEI	Edison Electric Institute
EPRI	Electric Power Research Institute
GPS	Global Positioning System
HMI	Human Machine Interface
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IOU	Investor Owned Utility
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ISOC	Integrated Security Operations Center
IT	Information Technology
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NRECA	National Rural Electric Cooperative Association
OT	Operations Technology

PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
RTU	Remote Terminal Unit
SP	Special Publication
TC	Technical Committee
UTC	Utilities Technology Council

B
THREAT AGENT

Table B-1
Threat Agent List

Threat Agent	Subcategory	Example Members
Economic Criminals		
	Transnational or national criminal Organization	Former Soviet Union Mafia, extortion groups
	Insiders (financial, espionage)	Employees, contractors
	Customers	Residential, commercial, schools
	External individual	
Malicious Criminals		Disgruntled employees or contractors, deranged persons, cyber gangs
Recreational Criminals		Hackers
Activist Groups		
	Eco and cause driven	Earth First, Green Peace
	US national separatists	US militias and hate groups (known to steal power)
Terrorists		
	Religious radical extremists	Al Qaeda, Taliban, ISIS
	Lone extremists	Anti-society individual
	Strategic political	Nation State: China, North Korea, Cuba
	Tactical political	Lashkar-e-Taiba, Hamas
Hazards		
	Natural hazards	Tornados, pandemics, floods, earthquakes
	Human errors and other accidents	- Poor human-system design - Configuration or data entry errors - Inadequate or non-existent policies, processes, procedures, and/or training - Non-compliance (not following policies and procedures) - Inadequate auditing, maintenance and testing - Poor plant system design - Legacy and aging systems
	Other hazards to required resources	- Employees that monitor cyber security are absent due to terror threat - Loss of processing/communication facilities due to nearby physical attack

C
ELECTRIC SECTOR USE CASES

The security use cases included in this appendix are based on the failure scenarios developed for the National Electric Sector Cybersecurity Organization Resource (NESCOR) project. Failure scenarios that are applicable to transmission and distribution substations were selected and tailored, as applicable. This included revisions to the description, deletion/addition of some vulnerabilities and mitigations, and allocation of the substation device categories to the impacts, vulnerabilities, and mitigations.

The use cases are organized in the following domains:

1. Advanced Metering Infrastructure (AMI)
2. Distributed Energy Resources (DER)
3. Wide Area Monitoring, Protection, and Control (WAMPAC)
4. Demand Response (DR)
5. Distribution Grid Management (DGM)
6. Generic

Generic is a cross-cutting category that includes failure scenarios that may impact many of these domains.

Vulnerabilities are described using a common schema defined by a *common vulnerability* followed by a *context*. Likewise, mitigations are described using a common schema defined by a *common mitigation* followed by an *action application* that provides context for the *common action*. The substation categories are highlighted in red throughout this section, for ease of reference.

C.1 Advanced Metering Infrastructure (AMI)

This section presents a set of use cases for the Advanced Metering Infrastructure (AMI) domain. AMI is intended to implement residential demand response and to serve as the chief mechanism for implementing dynamic pricing. It consists of the communications hardware and software and associated system and data management software that creates a two-way network between advanced meters and utility business systems, enabling collection and distribution of information to customers and other parties, such as the competitive retail supplier or the utility itself. AMI provides customers real-time (or near real-time) pricing of electricity and it can help utilities achieve necessary load reductions.

AMI.1 Authorized Employee Issues Unauthorized Mass Remote Disconnect

Description: An employee within the utility having valid authorization, issues a “remote disconnect” command to a large number of meters. The employee may be bribed, disgruntled, or socially engineered.

Substation Categories:

- Monitoring and Measurement Systems – Future

Relevant Vulnerabilities:

- *System permits potentially harmful command sequences* such as a sufficiently large number of disconnects that may threaten system balance. (Monitoring and Measurement Systems)

Impact:

- An instantaneous mass disconnect/reconnect over multiple feeders, if permitted by the system, could cause temporary blackouts due to circuit breaker trips until power on the grid can be rebalanced,
- A small number of disconnects could subvert the smart grid deployment and make the utility lose consumer confidence.

Potential Mitigations:

- *Validate data* to ensure reasonableness of changes, (Monitoring and Measurement Systems)
- *Generate alarms* for changes to sensitive data, (Monitoring and Measurement Systems)
- *Create audit logs* to track who has made system configuration, software, or database additions or modifications, (Monitoring and Measurement Systems)
- *Require two-person rule* for single transactions that initiate mass disconnects (e.g., substation feeder, all meters listening to a given aggregation point, geographic region, etc.), (Cyber Security Systems)
- *Limit events* to no more than (n) number of disconnects (using any number of transactions) within a specified time period, (Design, policies, and procedures)
- *Require two-person rule* for greater than (n) number of disconnects within a specified time. (Cyber Security Systems)

AMI.2 Out of Scope

AMI.3 Out of Scope

AMI.4 Out of Scope

AMI.5 Out of Scope

AMI.6 Out of Scope

AMI.7 Out of Scope

AMI.8 Out of Scope

AMI.9 Out of Scope

AMI.10 Out of Scope

AMI.11 Out of Scope

AMI.12 Out of Scope

AMI.13 Out of Scope

AMI.14 Out of Scope

AMI.15 Out of Scope

AMI.16 Out of Scope

AMI.17 Out of Scope

AMI.18 Out of Scope

AMI.19 Out of Scope

AMI.20 Out of Scope

AMI.21 Out of Scope

AMI.22 Out of Scope

AMI.23 Out of Scope

AMI.24 Out of Scope

AMI.25 Out of Scope

AMI.26 Out of Scope

AMI.27 Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control

Description: A threat agent is able to reverse engineer AMI equipment (meters and concentrators) to determine how to remotely control them. This allows the threat agent to control many devices simultaneously, and, for example, to perform a simultaneous mass disconnect, send DR messages that cause consumption of electricity to go up dramatically, or cause devices to send out last gasp or self-test failed messages.

Substation Categories:

- Monitoring and Measurement Systems – Transition, Future

Relevant Vulnerabilities:

- *Design permits unnecessary privileges*, such as unprotected interfaces used for development, testing, monitoring, or maintenance purposes that remain in production equipment, (Monitoring and Measurement Systems)
- *Back doors for access are left in place* for AMI equipment. (Monitoring and Measurement Systems)

Impact:

- When demand can be manipulated quickly by a threat agent, there is the potential for outages while operators adjust generation to demand,
- Faked failure messages cause the utility to assume the cost of investigation and deploying technicians to resolve issues, as well as cost of their inability to address real problem meters due to the false event "noise."

Potential Mitigations:

- *Design for security* to identify and remove unsecure development features and "nonstandard" interfaces from "production devices," (Design, policies, and procedures)
- *Design for security* in equipment such that knowledge of the design alone should not allow a threat agent to access a device without knowledge of keys and other credentials in equipment devices, (Design, policies, and procedures)
- *Configure for least functionality* by removing unnecessary interfaces and labeling from production devices. (Monitoring and Measurement Systems)

AMI.28 Out of Scope

AMI.29 Out of Scope

AMI.30 Out of Scope

AMI.31 Out of Scope

AMI.32 Out of Scope

C.2 Distributed Energy Resources (DER)

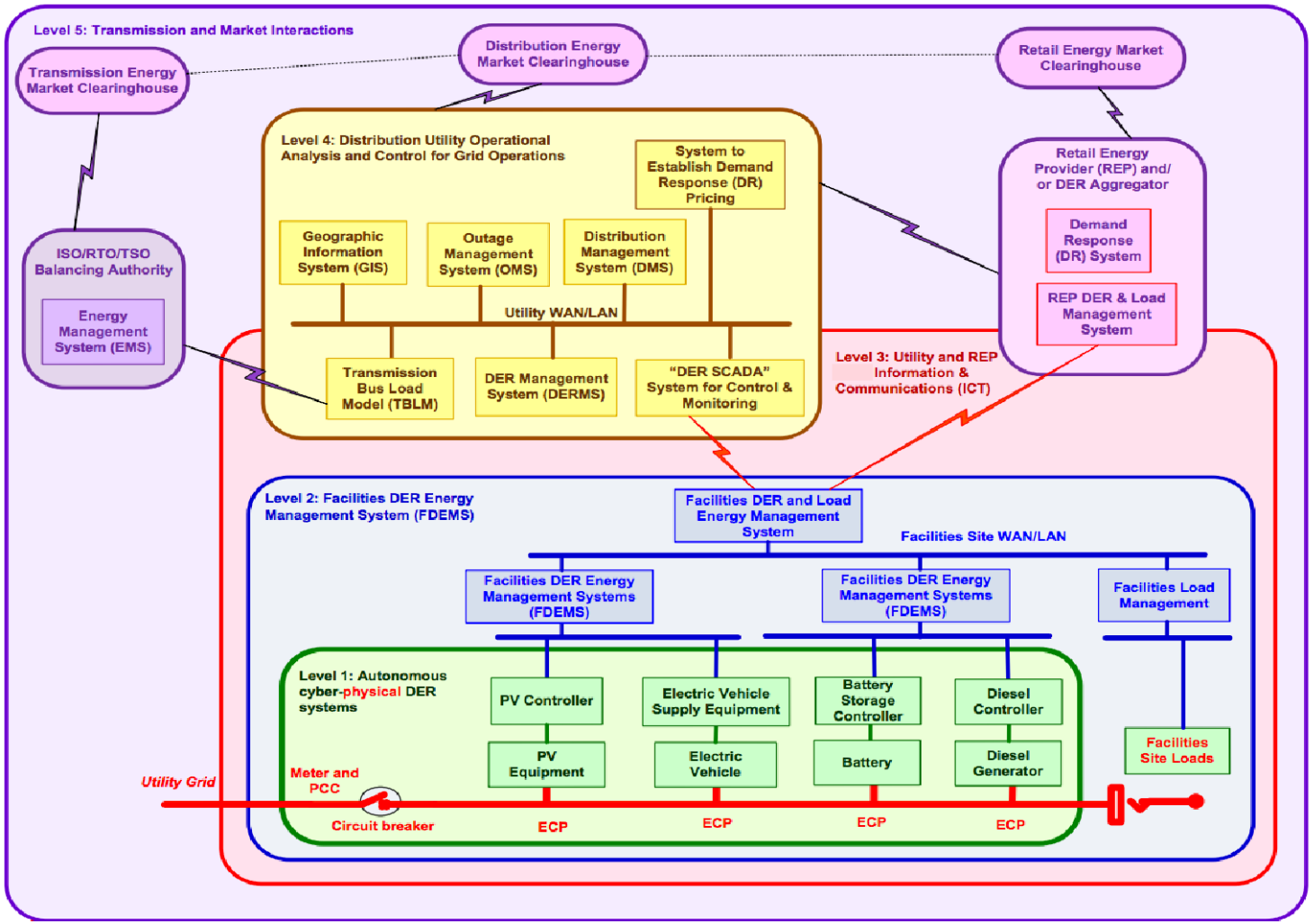
This section presents a set of use cases for the Distributed Energy Resources (DER) domain. DER systems are "cyber-physical systems that provide energy and ancillary services to the power grid, typically through the distribution system. DER systems can be generators, storage devices, and even electric vehicles if their chargers are capable of managing the charging and discharging processes. Generally, DER systems are small", but they are becoming prevalent in the distribution system (potentially there will be thousands if not millions of DER systems interconnected with the distribution system).[4] The following concepts are used throughout the DER scenarios:

- *Distributed Energy Resource Management System (DERMS): Utility system that manages the requests and commands to the DER systems*. It is also responsible for the database of interconnection permits and registrations of DER systems.
- *Facilities DER Energy Management System (FDEMS)*: System that manages combinations of DER generation, DER storage, and customer loads at a residential, commercial, or industrial customer site.

Included below is a diagram that illustrates a generic five-level DER hierarchical architecture. The five levels are:

- Level 1: Autonomous cyber-physical DER systems
- Level 2: Facilities DER Energy Management Systems (FDEMS)
- Level 3: Utility and REP Information and Communications (ICT)
- Level 4: Distribution Utility Operational Analysis and Control for Grid Operations
- Level 5: Transmission and Market Interactions

[4] NESCOR Guide to Penetration Testing for Electric Utilities, http://www.smartgrid.epri.com/doc/NESCORGuidetoPenetrationTestingforElectricUtilities-v3-Final.pdf



ECP: Electrical Connection Point

(Figure Developed by Xanthus Consulting)

Figure C-1
DER Five-Level Hierarchical Architecture

DER.1 Inadequate Access Control of DER Systems Causes Electrocution

Description: The DER owner fails to change the default password or not set a password for the DER system user interface. A threat agent (inept installer, hacker, or industrial spy) gets access through the user interface and changes the DER settings so that it does not trip off upon low voltage (anti-islanding protection), but continues to provide power during a power system fault.

Substation Categories:

- Automated Protection Systems – Transition, Future
- Monitoring and Measurement Systems – Transition, Future

Relevant Vulnerabilities:

- *Default password is not changed* for the DER system, (Automated Protection Systems, Monitoring and Measurement Systems)
- *System permits unauthorized changes* to anti-islanding protection in the DER system due to poor configuration design. (Automated Protection Systems, Monitoring and Measurement Systems)

Impacts:

- DER system suffers physical damage due to feeding into a fault,
- A utility field crew member may be electrocuted,
- The utility experiences damage to its reputation due to smart grid anomalies.

Potential Mitigations:

- *Authenticate users* for all user interface interactions, (Automated Protection Systems, Monitoring and Measurement Systems)
- *Change default access credentials* after installation, (Automated Protection Systems, Monitoring and Measurement Systems)
- *Train personnel* on secure networking requirements so that DER owners will understand the impact of bypassing security settings, (Design, policies, and procedures)
- *Require approval* of next level of management for critical security settings. (Design, policies, and procedures)

DER.2 DER's Rogue Wireless Connection Exposes the DER System to Threat Agents via the Internet

Description: An industrial or large commercial DER system is configured for local operational access through a wireless network, but is erroneously connected to the company's wireless corporate network, thus exposing the DER system to the Internet. Through the incorrect connection to the Internet, a threat agent gains control of the DER system and alters the operation of the DER functions to make them ignore utility commands and to turn off the "acknowledge command" interaction with the utility. The DER system may no longer limit power output during critical situations.

Substation Categories:

- Manually Initiated Systems – Transition, Future
- Monitoring and Measurement Systems – Transition, Future
- Communications Systems – Transition, Future

Relevant Vulnerabilities:

- *Network is connected to untrusted networks,* specifically the DER operational network is connected to the company's wireless corporate network, (Communications Systems)
- *System relies on credentials that are easy to obtain for access* to the wireless network allowing an unauthorized entity to gain control of DER system through the Internet, (Communications Systems)
- *System permits wireless access by unauthorized parties* to the wireless network in the DER system, (Communications Systems)
- *Unnecessary access is permitted to system functions* in the DER system, (Monitoring and Measurement Systems)
- *Users lack visibility to the failure of the system to respond to commands* by the utility for the DER system. (Manually Initiated Systems, Monitoring and Measurement Systems)

Impact:

- Utility power equipment is damaged, causing financial impacts and outages of customers,
- The utility experiences damage to its reputation due to smart grid anomalies,
- The utility's networked grid in a city may experience damaging reverse power flows, or overloads to substation transformers.

Potential Mitigations:

- *Verify network changes* including connections available between networks, (Communications Systems)
- *Authenticate devices* so that any new connections support only authorized equipment, (Monitoring and Measurement Systems)
- *Detect unauthorized configuration changes* to the DER system, (Monitoring and Measurement Systems)
- *Configure for least functionality* by limiting the types of traffic, shutting down certain ports, etc., (Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems)
- *Authenticate messages*, including their source and destinations, in communication protocols used between DER system components, (Communications Systems)
- *Require acknowledgements* in communication protocols used for critical commands from the utility to DER systems, (Communications Systems)
- *Require failure messages* in communication protocols used for critical commands from the utility to DER systems, (Communications Systems)

- *Train personnel* (DER system installers) to ensure that the recommended access control security settings are enabled, (Design, policies, and procedures)
- *Require secure factory settings* for configuration and network parameters by default, (Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems)
- *Authenticate users* who make modifications to secure configuration and network parameters. (Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems)
- *Use Role-Based Access Control* to limit privileges to safety critical functions, (Manually Initiated Systems)
- *Limit remote modification* of functional and security settings for the DER system. (Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems)

DER.3 Out of Scope

DER.4 Out of Scope

DER.5 Out of Scope

DER.6 Compromised DER Sequence of Commands Causes Power Outage

Description: A utility-owned DER storage system is located in a substation to balance large feeder generation and load variations. A threat agent causes a sequence of commands, although valid individually, to arrive at the DER system in the wrong order (possibly through a replay attack), causing the DER system to create a greater imbalance and tripping off all customers served from that substation.

Substation Categories:

- Automated Protection Systems – Future
- Manually Initiated Systems – Future

Relevant Vulnerabilities:

- *System permits potentially harmful command sequences* in the application-to-application messaging scheme of the DER storage system, (Automated Protection Systems, Manually Initiated Systems)
- *A copy of a prior message or command is difficult or infeasible to distinguish from a new legitimate message or command* in the communication protocol of the DER storage system. (Automated Protection Systems, Manually Initiated Systems)

Impact:

- Outages for all customers served by the substation,
- Continued threat of outages until the cause of the improper DER system operation is determined and corrected,
- Utilities need to curtail customer generation and/or loads until the problem is corrected.

Potential Mitigations:

- *Check message integrity* in communication protocols used to manage DER systems, (Communications Systems, Cyber Security Systems)
- *Protect against replay* in communication protocols used to manage DER systems, (Communications Systems, Cyber Security Systems)
- *Create audit log* of out-of-sequence data, (Communications Systems, Cyber Security Systems)
- *Generate alarms* for system owners when out-of-sequence data is detected. (Communications Systems, Cyber Security Systems)

DER.7 Incorrect Clock Causes Substation DER System Shut Down During Critical Peak

Description: A utility-owned DER system is located in a substation with the primary purpose of providing additional power during a critical peak. A threat agent changes the time clock in the DER system through a false time-synchronization message, so that either the DER system believes that the critical peak event is over or that all time-stamped messages to it are invalid, so it goes into default shut-down mode.

Substation Categories:

- Support Systems – Transition, Future

Relevant Vulnerabilities:

- *System permits messages to be modified by unauthorized individuals* in the time synchronization communication protocol, (Support Systems)
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the time synchronization communication protocol, (Support Systems)
- *System permits unauthorized changes* to time references source (Support Systems)

Impact:

- The DER system performs an immediate shut down and causes damage to a transformer,
- Customer outages occur during the critical peak,
- Utilities need to curtail customer generation and/or loads until a new transformer is installed.

Potential Mitigations:

- *Authenticate messages* in the time synchronization communication protocol[5], (Cyber Security Systems)
- *Check message integrity* in the time synchronization communication protocol[6]. (Cyber Security Systems)

---

[5] Is it realistic to implement between time reference and time clock?

[6] Is it realistic to implement between time reference and time clock?

DER.8 Out of Scope

DER.9 Loss of DER Control Occurs due to Invalid or Missing Messages

Description: A malicious or non-malicious individual causes the loss of DER control due to invalid or missing messages. Since the DER system either tries to act on invalid messages or no longer has messages constraining its output, it causes a distribution transformer to overload, thus causing an outage for the site and for neighboring sites. The DER system also sustains damage due to invalid settings.

Substation Categories:

- Automated Protection Systems – Transition, Future
- Communications Systems – Transition, Future

Relevant Vulnerabilities:

- *System permits messages to be modified by unauthorized individuals*, (Automated Protection Systems, Communications Systems)
- *System permits message interruption by unauthorized individuals*, (Communications Systems)
- commands or other messages may be inserted on the network by unauthorized individuals (Automated Protection Systems, Communications Systems)

Impact:

- A distribution transformer is damaged,
- A local outage occurs that requires field crews to replace the damaged transformer,
- The DER system may sustain damage due to trying to act on invalid messages or not being constrained by expected messages that did not arrive.

Potential Mitigations:

- *Authenticate messages* in all communication protocols, (Communications Systems, Cyber Security Systems)
- *Generate alarms* for messages that fail message authentication, (Communications Systems, Cyber Security Systems)
- *Create audit log* of messages that fail message authentication. (Communications Systems, Cyber Security Systems)

DER.10 Out of Scope

DER.11 Out of Scope

DER.12 Modified Management Settings for Substation FDEMS Impact Power Quality

Description: A malicious individual accesses a utility FDEMS that manages DER generation and storage systems within a substation, and modifies the energy output, the volt-var curves, or other DER management settings. When the utility requests the FDEMS to control the DER

systems to provide more vars, the FDEMS causes the DER systems to behave erratically and causes the substation to have power quality problems, including tripping of the transmission line breaker.

Substation Categories:

- Automated Protection Systems – Transition, Future
- Monitoring and Management Systems – Transition, Future

Relevant Vulnerabilities:

- *Unauthorized network access is permitted* for the FDEMS network, (Automated Protection Systems, Monitoring and Management Systems)
- *System relies on credentials that are easy to obtain for access* that allows modification of the FDEMS settings. (Automated Protection Systems, Monitoring and Management Systems)

Impact:

- Power system power quality problems, including erratic supply of vars to the transmission system,
- An outage of all feeders in the substation.

Potential Mitigations:

- *Restrict application access* for all FDEMS user interface interactions, (Automated Protection Systems, Monitoring and Management Systems)
- *Authenticate users* for all FDEMS user interface interactions, (Automated Protection Systems, Monitoring and Management Systems)
- *Enforce changing default credentials* as a system enforced step during installation, (Automated Protection Systems, Monitoring and Management Systems)
- *Use RBAC* in the FDEMS system, (Automated Protection Systems, Monitoring and Management Systems)
- *Enforce restrictive firewall rules* for access to the FDEMS network, (Cyber Security Systems)
- *Protect credentials* that allow access to the FDEMS network, (Cyber Security Systems)
- *Protect credentials* for the FDEMS application that permit access to modify the FDEMS settings, (Cyber Security Systems)

DER.13 Out of Scope

DER.14 Out of Scope

DER.15 Out of Scope

DER.16 DER SCADA System Issues Invalid Commands

Description: A threat agent breaches a DER SCADA system and causes the DER SCADA system to issue an invalid command to all DER systems. Since DER systems may react differently to invalid commands, the power system experiences immediate and rapid fluctuations as some DER systems shut down, while others go into default mode with no volt-var support,

still others revert to full output, and a few become islanded microgrids. The distribution equipment tries to compensate automatically, but causes more problems as the voltage experiences severe surges and sags.

Substation Categories:

- Manually Initiated Systems – Transition, Future

Relevant Vulnerabilities:

- *System permits potentially harmful command sequences,* in particular issuance of commands with unknown impact on the DER systems, (Manually Initiated Systems)
- *System permits unauthorized changes* to SCADA application data or software that allows the DER SCADA system to send invalid commands to DER systems, (Manually Initiated Systems)
- *System relies on credentials that are easy to obtain for access* to the SCADA DER system. (Manually Initiated Systems)

Impact:

- Power system rapid fluctuations that cause power quality problems for customers, including outages,
- Equipment damage (that can lead to loss of life) due to power system surges and sags,
- Transmission power quality problem.

Potential Mitigations:

- *Authenticate users* accessing the DER SCADA system, (Manually Initiated Systems)
- *Authenticate messages* communicated in the DER SCADA network, (Communications Systems)
- *Use RBAC* in the utility's DER SCADA system, (Manually Initiated Systems)
- *Validate inputs* that the DER system receives from the DER SCADA system, (Manually Initiated Systems)
- *Protect credentials* that allow access to the DER SCADA network, (Cyber Security Systems)
- *Protect credentials* for DER SCADA application and operating system. (Cyber Security Systems)

DER.17 Out of Scope

DER.18 Microgrid Disconnect Process Compromised via DERMS

Description: A threat agent gains access to the utility DERMS system and alters the conditions that determine when a utility has permission to disconnect a pre-established microgrid from the grid. This modification causes the microgrid either to disconnect at some random time in the future, or to prevent it from disconnecting even when it is supposed to disconnect (e.g., in the case of an outage).

Substation Categories:

- Automated Protection Systems – Transition, Future

Relevant Vulnerabilities:

- *Unnecessary access is permitted to system functions* in the DERMS system, (Automated Protection Systems)
- *System permits unauthorized changes* to utility permissions for microgrid disconnect, (Automated Protection Systems)
- *System permits messages to be modified by unauthorized individuals* to convey a command to modify utility permission for microgrid disconnect, (Automated Protection Systems)
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message*. (Automated Protection Systems)

Impact:

- Since the microgrid may not be prepared to disconnect from the grid or may be brought down during the grid outage, it will experience a complete outage,
- Legal costs for litigation with the adversely affected customers.

Potential Mitigations:

- *Use RBAC* to limit those users authorized to change microgrid establishment permissions in the utility's DERMS system, (Automated Protection Systems)
- *Require intrusion detection*, as part of DERMS network and system management capabilities, (Cyber Security Systems)
- *Authenticate messages* for administrative messages received by the utility DERMS, (Automated Protection Systems)
- *Check message integrity* for administrative messages received by the utility DERMS. (Cyber Security Systems)

DER.19 Threat Agent Gains Access to Utility DERMS via FDEMS

Description: A threat agent uses a FDEMS to which they have full access, to access the utility's DERMS system. The threat agent is able to modify the DER commands, schedules, and requests sent to other DER systems, making these settings beneficial to their own DER systems, and consequently less beneficial to other DER systems.

Substation Categories:

- Manually Initiated Systems – Transition, Future

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to modify the DERMS settings, when communicating using the FDEMS to DERMS protocol, (Manually Initiated Systems)

- *Unnecessary access is permitted to system functions* in the DERMS system that modify settings that impact individual DER systems, (Manually Initiated Systems)
- *System permits messages to be modified by unauthorized individuals* so that a message to the DERMS using the FDEMS communications channel appears to come from an entity authorized to change DERMS settings, and contains a request for such changes, (Manually Initiated Systems)
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message,* in this case a change to the apparent source of the message as well as its contents, (Manually Initiated Systems)
- *Users lack visibility that unauthorized changes were made* to DERMS functions. (Manually Initiated Systems)

Impact:

- Inefficient or cost-ineffective power system operated by the utility,
- Utility legal costs related to DER owner litigation for unfair practices.

Potential Mitigations:

- *Use RBAC* in the utility's DERMS system to limit privilege to modify DERMS settings, (Manually Initiated Systems)
- *Validate inputs* in the DERMS control commands, (Manually Initiated Systems)
- *Authenticate messages* received by the DERMS from FDEMS systems, (Manually Initiated Systems)
- *Check message integrity* for messages received by the DERMS from an FDEMS. (Manually Initiated Systems)

DER.20 Out of Scope

DER.21 Out of Scope

DER.22 DELETED

DER.23 Out of Scope

DER.24 Out of Scope

DER.25 Out of Scope

DER.26 Spoofed Microgrid Status Messages Cause Disconnect from Grid

Description: A threat agent spoofs messages that appear to come from a microgrid to the utility. The messages indicate that the pre-established conditions have been met for the utility to disconnect from the microgrid. The utility disconnects from the microgrid, even though these conditions are not actually met.

Substation Categories:

- Automated Protection Systems – Transition, Future
- Manually Initiated Systems – Transition, Future

Relevant Vulnerabilities:

- *System permits messages to be modified by unauthorized individuals* (e.g., status messages from the microgrid), (Automated Protection Systems, Manually Initiated Systems)
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* (e.g., status messages from the microgrid). (Automated Protection Systems, Manually Initiated Systems)

Impact:

- Since the microgrid may not be prepared to disconnect from the grid or may be brought down during the grid outage, it will experience a complete outage,
- Legal costs for litigation with the adversely affected customers.

Potential Mitigations:

- *Authenticate messages* that communicate microgrid status to the utility, where that status communicates whether or not pre-established disconnect conditions have been met, (Automated Protection Systems, Manually Initiated Systems, Cyber Security Systems)
- *Confirm action* to disconnect microgrid with the microgrid operator, if microgrid status indicates that pre-established disconnect conditions have been met. (Design, policies, and procedures)

C.3 Wide Area Monitoring, Protection, and Control (WAMPAC)

This section presents a set of use cases for the Wide Area Monitoring, Protection, and Control (WAMPAC) domain. "WAMPAC systems constitute a suite of different system solutions aimed at meeting various wide-area application requirements." [7] "WAMPAC systems often center around synchrophasor technology and the devices that generate, receive, and utilize this synchrophasor data. WAMPAC systems should be setup to include all components from the Phasor Measurement Unit (PMU) to the WAMPAC applications leveraging that data, including other intermediate devices such as the servers that manage the PMUs, devices that provide alignment services like Phasor Data Concentrators (PDCs), phasor gateways, phasor data stores, and other such components."[6]

The impact of a failure scenario for WAMPAC is fully dependent upon the use of the WAMPAC data. For example, a failure in a WAMPAC application that offers control capabilities has a higher impact than a failure in a monitoring application. Currently, most utilities consider WAMPAC as a supplementary source of data; hence its failure impact is considered less significant. It is anticipated that WAMPAC will become a primary trusted data source in the near future.

[7]NESCOR Wide Area Monitoring, Protection, and Control Systems (WAMPAC) – Standards for Cyber Security Requirements, http://www.smartgrid.epri.com/doc/ESRFSD.pdf

NOTE: In Table C-1, presented are the possible impact of the WAMPAC use cases, which takes into consideration the state in which the system is in and also the nature of the application that the WAMPAC executes. Impacts that relate to "Loss of data for each application" are distinguished from impacts that relate to "Altered data or timestamps for each application". Each WAMPAC failure scenario refers to the impact presented in Table C-1 that is applicable to it.

Table C-1
Impact Examples by Type of WAMPAC Application

		Alert/Emergency
Monitoring	*Data loss*	• Delay in taking actions (e.g., load shedding) • Delay in grid reconfiguration • Unnecessary power generation, overload of lines, or creation of fault conditions, if timely or appropriate corrective actions are not taken
	Altered data	• Incorrect actions to be taken
Local Protection	*Data loss*	• Failure in taking action, if no alternative data source is available
	Altered data	• Line trip, which can lead to cascading failures if lines are overloaded and other protection takes place • Improper synchronous closing, leading to equipment damage
Special Protection	*Data loss*	• Delay in triggering protection elements • Overload of lines, or creation of fault conditions, if timely or appropriate corrective actions are not taken
	Altered data	• Line trip, which can lead to cascading failures if lines are overloaded and other protection takes place • Improper synchronous closing, leading to equipment damage
Control	*Data loss*	• Delay in taking actions (e.g., load shedding) • Delay in grid reconfiguration • Unnecessary power generation, overload of lines, or creation of fault conditions, if timely or appropriate corrective actions are not taken
	Altered data	• Failure to take action, when needed, leading to voltage or frequency conditions that could have been prevented • Cascading failures

WAMPAC.1 Denial of Service Attack Impairs PTP Service

Description: A set of Phasor Measurement Units (PMUs) receive their time via network communication from a Precision Time Protocol (PTP) server. A threat agent is able to perform a denial of service attack against PTP either by leveraging vulnerabilities in the PTP service itself or by flooding it with high volume of traffic or malformed packets targeting open ports that are not required by PTP. This leads to delays or lack of functionality of the PTP service, translating into the inability of the PMUs to correctly timestamp their measurements.

Substation Categories:

- Communications Systems – Future
- Support Systems – Future

Relevant Vulnerabilities:

- *Network interfaces permit unnecessary traffic flows* for the network hosting the PTP server, (Communications Systems)
- *Unnecessary system services are configured to run* on the PTP server, (Support Systems)
- *Unnecessary access is permitted to critical functions* in the PTP service. (Support Systems)

Impact:

- All impacts presented in Table C-1, as potentially caused by loss of measurements due to lack of time synchronization.

Potential Mitigations:

- *Restrict network service access* to the PTP service, (Support Systems)
- *Isolate functions* between the PTP service and the auxiliary services running on the same server (e.g., resource prioritization), (Design, policies, and procedures)
- *Configure for least functionality* the PTP server, (Support Systems)
- *Verify correct operation* of the PTP server in order to remain operational when subjected to erroneous traffic and large amounts of traffic in the network stack, PTP and required auxiliary services, (Design, policies, and procedures)
- *Require intrusion detection and prevention*, (Cyber Security Systems)
- *Restrict network access* to the network hosting the PTP server, (Communications Systems)
- *Restrict access* to the GPS clock (locally or via the network). (Support Systems)

WAMPAC.2 Network Equipment used to Spoof WAMPAC Messages

Description: A threat agent leverages vulnerabilities to perform a spoofing attack and inject messages in WAMPAC network equipment (router, switch, etc.). The altered messages might be either measurements used as input to the WAMPAC algorithms, or commands to phasor measurement units (PMUs) or phasor data concentrators (PDCs).

Substation Categories:

- Communications Systems – Transition, Future

Relevant Vulnerabilities:

- *Unnecessary access is permitted to networking components* for WAMPAC networking devices, (Communications Systems)
- *System permits messages to be modified by unauthorized individuals* in the standard industry-wide WAMPAC protocols (such as IEEE C37.118 which has no built-in security capabilities), (Communications Systems)
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the standard industry-wide WAMPAC protocols (such as IEEE C37.118 which has no built-in security capabilities), (Communications Systems)
- *System permits networking components to be accessed by unauthorized individuals* (e.g., routers, switches, etc.), (Communications Systems)

Impact:

- All impacts presented in Table C-1, as potentially caused by altered measurements or loss of measurements.

Potential Mitigations:

- *Encrypt link layer* on the WAMPAC network, (Communications Systems)
- *Encrypt application layer* across the WAMPAC network, (Communications Systems)
- *Check message integrity* (e.g., digital signatures) of commands and data received by the WAMPAC components, (Monitoring and Measurement Systems)
- *Restrict network access* to the WAMPAC network, (Cyber Security Systems)
- *Use Role-Based Access Control* to limit privileges to access WAMPAC networking components, (Communications Systems, Cyber Security Systems)
- *Authenticate users* of WAMPAC networking components, (Cyber Security Systems)
- *Detect unusual patterns* in WAMPAC components traffic communications. (Cyber Security Systems)

WAMPAC.3 Improper PDC Configuration Interferes with Transmission of Measurement Data

Description: An insider is able to gain access to the network to which a PDC is connected and to the PDC's credentials, assuming credentials are in place. This individual compromises (malicious intent) or misconfigures (accidentally) the PDC. Consequently, the PDC does not recognize certain PDCs/PMUs and sends incomplete measurement data up in the WAMPAC hierarchy.

Substation Categories:

- Monitoring and Measurement Systems – Transition, Future
- Communications Systems – Transition, Future

Relevant Vulnerabilities:

- *Network interfaces permit unnecessary traffic flows* to the PDC, (Communications Systems)

- *Users lack visibility that unauthorized changes were made* to the PDC configuration, (Monitoring and Measurement Systems)

Impact:

- All impacts presented in Table C-1, as potentially caused by loss of measurements.

Potential Mitigations:

- *Restrict network service access* at multiple layers to prevent unauthorized individuals from gaining access to the PDC, (Communications Systems, Cyber Security Systems)
- *Detect unauthorized connections* captured in the communication patterns to and from the PDC, (Cyber Security Systems)
- *Enforce restrictive firewall* rules for access to the PDC host network, (Cyber Security Systems)
- *Require multi-factor authentication* for remote access to PDC configuration functions, (Cyber Security Systems)
- *Use Role-Based Access Control* to limit privilege to modify the PDC configuration, (Cyber Security Systems; Design, policies, and procedures)

WAMPAC.4 Measurement Data Compromised due to PDC Authentication Compromise

Description: Although access control and connection authentication from a PMU into a PDC are in place, these are compromised. This may be due to a backdoor not subject to the usual controls, social engineering, network sniffing to gain credentials or an attack on the authentication database to modify or steal credential information. This allows inadvertent or malicious introduction of false measurement data.

Substation Categories:

- Monitoring and Measurement Systems – Transition, Future

Relevant Vulnerabilities:

- *Credentials are accessible in the clear* while in transit or at rest, (Monitoring and Measurement Systems)
- *System permits bypass of access control mechanisms*, (Monitoring and Measurement Systems)
- *System permits unauthorized changes* to the PDC/PMU configuration, which may include connection information. (Monitoring and Measurement Systems)

Impact:

- All impacts presented in Table C-1, as potentially caused by altered measurements.

Potential Mitigations:

- *Protect credentials* used to authenticate the PMU to the PDC, (Cyber Security Systems)
- *Change default credentials*, (Design, policies, and procedures)

- *Encrypt data at rest*, specifically credentials, (Cyber Security Systems)
- *Restrict remote access* to the network hosting authentication database, (Cyber Security Systems)
- *Require intrusion detection and prevention* for the network hosting authentication database, (Cyber Security Systems)
- *Authenticate users* to the network hosting authentication database, (Cyber Security Systems)
- *Protect security configuration* that lists the systems permitted to connect to the PDC. (Cyber Security Systems)

WAMPAC.5 Out of Scope

WAMPAC.6 Out of Scope

WAMPAC.7 Out of Scope

WAMPAC.8 Malware in PMU/PDC Firmware Compromises Data Collection

Description: A threat agent inserts firmware into PMU/PDC that alters measurements while they are collected. The altering mechanism can be triggered at all times, randomly or by certain events (e.g., time of day, certain date, etc.) that are assumed to inflict significant damage.

Substation Categories:

- Monitoring and Measurement Systems – Transition, Future

Relevant Vulnerabilities:

- Users lack visibility that unauthorized firmware has been installed before running it, (Monitoring and Measurement Systems)
- System permits unauthorized installation of software or firmware. (Monitoring and Measurement Systems)

Impact:

- All impacts presented in Table C-1, as potentially caused by altered measurements,
- Significant effort/cost invested in troubleshooting the systems given the lack of measurement consistency, followed by equipment replacement.

Potential Mitigations:

- *Implement configuration management* for controlling modifications to firmware to ensure that a PMU/PDC is protected against inadequate or improper modifications before, during, and after firmware manufacturing, (Design, policies, and procedures)
- *Check software execution integrity* for the firmware, since software may be compromised when loaded for execution, (Monitoring and Measurement Systems; Design, policies, and procedures)
- *Restrict system access* for firmware install/updates. (Cyber Security Systems; Design, policies, and procedures)

WAMPAC.9 DELETED

WAMPAC.10 Out of Scope

WAMPAC.11 Compromised Communications between Substations

Description: An insider delays local measurement data exchange between substations by compromising the integrity of the WAMPAC communication link between substations. This might be done by attacking network components such as routers, or gaining access to the network and employing a flooding attack.

NOTE: The impact of the use case presented below is assessed under the assumption that WAMPAC is used as part of a special protection scheme (SPS).

Substation Categories:

- Communications Systems – Transition, Future

Relevant Vulnerabilities:

- *Unnecessary network access is permitted* to network components. (Communications Systems)

Impact:

- All impacts presented in Table C-1, as potentially caused by altered measurements or loss of data, for Special Protection and Control applications.

Potential Mitigations:

- *Restrict network access* to administrative functions of network components, (Communications Systems, Cyber Security Systems)
- *Detect unauthorized access* on the substation communication links, (Communications Systems)
- *Restrict network access* on the substation communication links, (Communications Systems, Cyber Security Systems)
- *Restrict network access* to limit network traffic, using solutions such as router access control lists (ACLs) and firewalls, (Communications Systems, Cyber Security Systems)
- *Require intrusion detection and prevention*, (Cyber Security Systems)
- *Test before installation* of an IDS/IPS solution to verify that it does not compromise normal operation of the system. (Design, policies, and procedures)

WAMPAC.12 GPS Time Signal Compromise

Description: An attacker blocks or alters the GPS time signal that is associated with the synchrophasor measurements. The attacker can perform either a GPS spoofing or GPS jamming attack, where the GPS receiver is deceived by a more powerful signal resulting in the GPS signal being intentionally blocked or altered.

Substation Categories:

- Support Systems - Transition, Future

Relevant Vulnerabilities:

- *Spoofed signal is either difficult or infeasible to distinguish from a legitimate signal* that provides GPS-based time synchronization. (Support Systems)

Impact:

- All impacts presented in Table C-1, as potentially caused by altered measurements (in the case of GPS spoofing) or loss of measurements (in the case of GPS jamming),
- Significant effort/cost invested in troubleshooting the systems given the lack of time signal consistency.

Potential Mitigations:

- *Design for trust* the synchronization mechanism for the synchrophasor signals (e.g., use internal clocks rather than GPS for the time signal), (Design, policies, and procedures)
- *Validate signal* by using a redundant GPS signal transmitted through a communication network to detect the time signal drift in the GPS time signal (e.g., use NTP or PTP), (Design, policies, and procedures)
- *Require fail-over* for the local GPS signal to either a GPS signal brought from another part of the grid through a communication network or internal clocks for when an intrusion is detected. (Design, policies, and procedures)

C.4 Demand Response (DR)

This section presents a set of use cases for the Demand Response (DR) domain. "Demand Response (DR) communications cover interactions between wholesale markets and retail utilities and aggregators, as well as between these entities and the end-load customers who reduce demand in response to grid reliability or price signals. […] Price (often with the time that the price is effective), grid integrity signals (e.g., event levels of low, medium, high), and possibly environmental signals (e.g., air quality) are components of DR communications."

DR.1 Out of Scope

DR.2 Out of Scope

DR.3 Out of Scope

DR.4 Out of Scope

DR.5 Out of Scope

DR.6 Custom Malware Compromises DRAS

Description: A threat agent injects purpose-built malware into the DRAS. This malware places the server under remote command of this agent. The agent might use this capability to send out DR messages appropriate for non-peak times at peak times, and vice versa.

Substation Categories

- Manually Initiated Systems – Transition, Future

Relevant Vulnerabilities:

- *System permits unauthorized changes* to software in the DRAS, (Manually Initiated Systems)
- *Users lack visibility that unauthorized changes were made* to the DRAS software, (Manually Initiated Systems)
- *Unnecessary system services are configured to run* on un-blocked or unnecessary open ports, (Manually Initiated Systems)

Impact:

- Addition of extra load at peak times and reduction of load at non-peak times could result in power outages and physical power system damage,
- Loss of public confidence in the utility and DR program.

Potential Mitigations:

- *Restrict remote access* to the DRAS systems, (Manually Initiated Systems)
- *Use RBAC* to limit access to the DRAS software files, (Manually Initiated Systems, Cyber Security Systems)
- *Require application whitelisting* on the DRAS, (Cyber Security Systems)
- *Configure for least functionality* by making unavailable any unnecessary functions and ports on the DRAS systems. (Manually Initiated Systems)

C.5 Distribution Grid Management (DGM)

This section presents a set of use cases for the Distribution Grid Management (DGM) domain. DGM "focuses on maximizing performance of feeders, transformers, and other components of networked distribution systems and integrating with transmission systems and customer operations. As smart grid capabilities, such as AMI and demand response, are developed, and as large numbers of distributed energy resources and plug-in electric vehicles (PEVs) are deployed, the automation of distribution systems becomes increasingly more important to the efficient and reliable operation of the overall power system. The anticipated benefits of distribution grid management include increased reliability, reductions in peak loads, and improved capabilities for managing distributed sources of renewable energy"[4].

DGM.1 Wireless Signals are Jammed to Disrupt Monitoring and Control

Description: A threat agent uses a wireless signal jammer to disrupt wireless communications channels used to monitor and control distribution systems and substations. Examples are wireless local area network (LAN) communications for inter-substation differential protection, wireless communications between a distribution management system (DMS) and static VAR compensators (SVC), and communications to wireless monitoring equipment.

Substation Categories:

- Communications Systems – Legacy, Transition, Future

Relevant Vulnerabilities:

- *System relies on communications that are easy to jam* in physical radio frequency (RF) communications. Physical radio frequency (RF) communications are subject to deliberate jamming since few radio systems outside of the military have anti-jamming capability. Sustained jamming is less effective than intermittent jamming with the latter potentially causing the system to execute inappropriate or out of order commands, (Communications Systems)
- System makes messages accessible to unauthorized individuals in wireless radio signals. (Communications Systems)

Impact:

- Reduced situational awareness and impaired ability to react to fluctuations in load and apply controlled remedies such as switching capacitor banks and triggering voltage regulators. This could cause voltage adjustment inefficiencies resulting in voltage sags and swells that can trigger unwanted over and under voltage trips on feeders or in substations,
- The uncoordinated capacitor banks due to loss of communications could conflict with substation load tap changer (LTC) actions, causing "hunting" or other inefficient actions that increase utility power losses and premature transformer failures,
- Extreme or long-duration voltage and frequency instability can damage customer or utility equipment,
- Disruption in wireless communications between pilot protection relays can impede differential protection schemes, possibly leading to equipment damage in substations or feeders during fault conditions.

Potential Mitigations:

- *Require redundancy* in communications channels when the wireless channel is no longer available, (Communications Systems)
- *Require safe mode* in feeder devices such as capacitor banks and voltage regulators to have default states that rely on local electrical conditions if communications are lost, (Monitoring and Measurement Systems)

DGM.2 Shared Communications Leveraged to Disrupt DMS Communications

Description: Some utilities depend upon communication providers for long-haul and wide area network (WAN) communications for monitoring and control of their distribution system. Furthermore, utilities that provide their own communication network for critical functions often resell unused bandwidth to offset costs while others have spun off their communication network as a separate communications company. There is also a general trend toward economizing communications costs by sharing them. A threat agent could take advantage of these paradigms by compromising computer systems using the same network as the Distribution Management System (DMS) to facilitate a distributed denial of service attack through the infected computer system by means of a botnet centered on IP spoofing and Internet Control Message Protocol (ICMP) flooding. With the network overburdened, monitoring and control functions could become unavailable for optimization or protection.

Substation Categories:

- Communications Systems – Legacy, Transition, Future

Relevant Vulnerabilities:

- *Communication channels are shared between different system owners* that may reduce availability and reliability of entities or functions that rely on those channels. Attackers have demonstrated flooding attacks against communications paths up to optical carrier (OC) 48. These optical fiber connections carry 2400+ megabits per second and are typically used in regional Internet Service Provider networks, (Communications Systems)
- *Network services are shared between different system owners* that increase the attack surface for the systems sharing the service. This requires a utility to put a certain level of trust in the systems sharing the communications channel and the entity that manages it. (Communications Systems)

Impact:

- Reduced situational awareness and impaired ability to react to fluctuations in load and apply controlled remedies such as switching capacitor banks and triggering voltage regulators. This could cause voltage adjustment inefficiencies resulting in voltage sags and swells that can trigger unwanted over and under voltage trips on feeders or in substations,
- The uncoordinated capacitor banks due to loss of communications could conflict with substation load tap changer (LTC) actions, causing "hunting" or other inefficient actions that increase utility power losses and premature transformer failures,
- Extreme or long-duration voltage and frequency instability can damage customer or utility equipment,
- Disruption in wireless communications between pilot protection relays can impede differential protection schemes, possibly leading to equipment damage in substations or feeders during fault conditions.

Potential Mitigations:

- *Verify personnel* (service providers) to ensure their services are secure and reliable, (Design, policies, and procedures)
- *Verify personnel* (customers) sharing the network are reputable, security conscious and using network resources appropriately, (Communications Systems)
- *Require safe mode* in feeder devices such as capacitor banks and voltage regulators to have default states that rely on local electrical conditions if communications are lost, (Monitoring and Measurement Systems)

DGM.3 Moved to Generic.5

DGM.4 Malicious Code Injected into Substation Equipment via Remote Access

Description: A threat agent uploads malicious code into substation equipment via remote engineering access, either through an IP network WAN or dialup to a line-sharing switch (LSS). Examples of target equipment include communication concentrators, RTUs, and protection relays. Connections with peers are another avenue of attack. Some distribution substations,

particularly in urban environments, use Bluetooth or ZigBee for access to reduce the need for crews to install underground cables. Malicious code could change device settings for purposes of rendering equipment inoperable, data gathering, denial of service, or misconfiguration.

Substation Categories:

- Automated Protection Systems – Legacy, Transition, Future
- Manually Initiated Systems – Legacy, Transition, Future
- Monitoring and Measurement Systems - Transition, Future
- Communications Systems – Legacy, Transition, Future
- Support Systems – Legacy, Transition, Future
- Primary Power Equipment Systems – Transition, Future

Relevant Vulnerabilities:

- *Unnecessary access is permitted to the communications channel* for remote substation WAN communications, (Communications Systems)
- *Software patches are not checked regularly to ensure that they are current*. (Design, policies, and procedures)

Impact:

- Substation components could be modified to fail detection and clearing of bus and feeder faults (although these can be managed by reclosers which are not necessarily in the substation). These faults could lead to destruction of electrical grid equipment,
- Substation components could be reprogrammed to disallow feeder sectionalizing or service restoration via SCADA. However, these are frequently done manually,
- Equipment firmware changes may create the need for equipment servicing that can be costly and time consuming,
- Possible lack of monitoring capabilities reduces situational awareness, inhibits a utility's ability to react proactively, and could increase the number and duration of failures.

Potential Mitigations:

- *Restrict remote access* to protective relays and other critical devices, (Cyber Security Systems)
- *Create audit log* of substation actions, (Cyber Security Systems)
- *Generate alarms* for any serious anomalies, such as connection changes and device configuration changes, (Cyber Security Systems)
- *Maintain patches* for all substation communication equipment, (Design, policies, and procedures)
- *Maintain anti-virus* on substation equipment, (Design, policies, and procedures)
- *Require application whitelisting* on substation equipment, (Design, policies, and procedures)
- *Authenticate users* in the substation network (possibly two factor authentication), (Cyber Security Systems)

- *Require VPNs* in the substation network. (Communications Systems, Cyber Security Systems)

DGM.5 Out of Scope

DGM.6 Spoofed Substation Field Devices Influence Automated Responses

Description: Threat agent spoofs data inputs from field devices at substations and below to cause the DMS to report a false system state. This could cause operator or automated responses that are inappropriate.

Substation Categories:

- Monitoring and Measurement Systems – Transition, Future

Relevant Vulnerabilities:

- *System permits messages to be modified by unauthorized individuals* in the communications between field devices and the DMS, (Monitoring and Measurement Systems)
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the communications between field devices and the DMS, (Monitoring and Measurement Systems)
- *System makes messages accessible to unauthorized individuals*. (Monitoring and Measurement Systems)

Impact:

- Inappropriate fault-clearing actions, feeder sectionalization, and overuse of remedial capabilities leading to loss of power to customers,
- Volt/VAR controls are wrongly applied or adjusted based on erroneous data, possibly triggering over/under voltage trips,
- Collected meter data is incorrect or inaccurate, leading to possible loss in revenue.

Potential Mitigations:

- *Authenticate messages* in communication from field devices to control centers, (Monitoring and Measurement Systems)
- *Detect unusual patterns* of inputs that could indicate they are not trustworthy, by comparing inputs to each other and previous inputs, (Monitoring and Measurement Systems)

DGM.7 QoS Spoofed to Create Denial of Service for DGM Communications

Description: Assuming the same communications system serves DGM, DR, AMI, and many other services at the distribution level, a Quality of Service (QoS) allocation of bandwidth is necessary. QoS can be spoofed and if end device classifications are trusted, a threat agent can escalate the priority of malevolent data streams. If denial of service is the goal, the threat agent could spoof the QoS of flooded ICMP packets to prevent the transmission and reception of monitoring and control packets.

Substation Categories:

- **Communications Systems – Transition, Future**

Relevant Vulnerabilities:

- *Network interfaces permit unnecessary traffic flows* to communication networks. (Communications Systems)

Impact:

- An end device could cause a denial of service to critical applications such as control of feeder sectionalizers and capacitor banks. In combination with a volatile electrical grid situation, this could lead to power failures,
- Reduced situational awareness and impaired ability to react to fluctuations in load and apply controlled remedies such as switching capacitor banks and triggering voltage regulators. This could cause voltage adjustment inefficiencies resulting in voltage sags and swells that can trigger unwanted over and under voltage trips on feeders or in substations,
- Extreme or long-duration voltage and frequency instability can damage customer or utility equipment,
- Denial of service in wireless communications between pilot protection relays can impede differential protection schemes, possibly leading to equipment damage in substations or feeders during fault conditions.

Potential Mitigations:

- *Profile equipment* (end devices) based on their association with ports and traffic, (Design, policies, and procedures)
- *Design for trust* by analysis of equipment profiles, (Design, policies, and procedures)
- *Restrict network access* to the control system network, (Communications Systems, Cyber Security Systems)
- *Encrypt communication paths* to prevent spoofing, (Cyber Security Systems)
- *Authenticate users* to prevent spoofing. (Communications Systems, Cyber Security Systems)

DGM.8 Supply Chain Vulnerabilities Used to Compromise DGM Equipment

Description: Lifecycle attacks against equipment during development, production, shipping, and maintenance can introduce deliberate errors that will result in failure under special conditions. For example, a threat agent might upload modified firmware in a relay during production that introduces a back door for changing relay settings and set points. This could render the relay inoperable or cause it to operate unexpectedly.

Substation Categories:

- Monitoring and Measurement Systems – Legacy, Transition, Future
- Automated Protection Systems – Legacy, Transition, Future
- Manually Initiated Systems – Legacy, Transition, Future
- Communications Systems – Legacy, Transition, Future

- Support Systems – Legacy, Transition, Future

Relevant Vulnerabilities:

- *System permits unauthorized changes* during software/firmware development, (Monitoring and Measurement Systems, Automated Protection Systems, Manually Initiated Systems, Communications, Support Systems)
- *System permits unauthorized changes* to software/firmware at suppliers of equipment, maintenance, and transportation, (Monitoring and Measurement Systems, Automated Protection Systems, Manually Initiated Systems, Communications, Support Systems)
- *System permits unauthorized changes* to software/firmware by utility employees with access to modify field equipment. (Monitoring and Measurement Systems, Automated Protection Systems, Manually Initiated Systems, Communications, Support Systems)

Impact:

- Any ill effect, including the most severe, is possible using this mechanism.

Potential Mitigations:

- *Require spares* for critical components, (Design, policies, and procedures)
- *Implement configuration management* for developers of equipment, (Design, policies, and procedures)
- *Verify personnel*, including developers of equipment, utility employees, and contract maintenance personnel through thorough employee background checks, (Design, policies, and procedures)
- *Conduct code reviews* on DMS systems, (Design, policies, and procedures)
- *Vulnerability scan before installation* of the code base, (Design, policies, and procedures)
- *Create audit log* of all code changes, (Monitoring and Measurement Systems, Automated Protection Systems (excluding Legacy), Manually Initiated Systems, Communications, Support Systems (excluding Legacy))
- *Restrict access* to software/firmware during development, (Design, policies, and procedures)
- *Confirm action* taken by contract maintenance personnel that modifies equipment, (Design, policies, and procedures)
- *Enforce least privilege* for utility employees for access to modify field equipment, (Monitoring and Measurement Systems, Automated Protection Systems (excluding Legacy), Manually Initiated Systems, Communications, Support Systems (excluding Legacy))
- *Design for trust* by introducing the concept of devices of varying degrees of trust along with associated certifications for their associated supply chains. (Design, policies, and procedures)

DGM.9 Out of Scope

DGM.10 Switched Capacitor Banks are Manipulated to Degrade Power Quality

Description: Switched capacitor banks can create large switching transients when connected to a utility feeder, generating voltage spikes up to twice the rated voltage and can be exacerbated when two are switched on back-to-back. A threat agent social engineers DMS Human Machine

Interface (HMI) passwords to gain control of switched capacitor bank relays to repeatedly switch capacitor banks on and off, generating cascading voltage spikes and instability to trip protection devices.

Substation Categories:

- Monitoring and Measurement Systems – Transition, Future

Relevant Vulnerabilities:

- *Users and hardware/software entities are given access unnecessary for their roles to* critical DMS functions, (Monitoring and Measurement Systems)
- *Insiders with high potential for criminal or malicious behavior have access to critical functions or sensitive data* in the DMS system. (Monitoring and Measurement Systems)

Impact:

- Repeated voltage spikes may damage customer or utility equipment,
- Possible loss of customer power due to false operation of protective devices.

Potential Mitigations:

- *Train personnel* on the threat of social engineering attacks and perform social engineering exercises (such as company generated phishing emails or rogue USB drives) to engage employees, (Design, policies, and procedures)
- *Require synchronous functions* for closing control, surge arrestors, or pre-insertion resistors to minimize capacitor bank switching transients, (Design, policies, and procedures)
- *Enforce least privilege* for access to critical DMS functions, (Monitoring and Measurement Systems)
- *Verify personnel* that have access to critical DMS functions, (Design, policies, and procedures)

DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System

Description: A threat agent performs reconnaissance of utility communications, electrical infrastructure, and ancillary systems to identify critical feeders and electrical equipment. Threat agent gains access to selected elements of the utility DMS system - which includes all distribution automation systems and equipment in substations, via remote connections. After gaining the required access, the threat agent manufactures an artificial cascade through sequential tripping of select critical feeders and components, causing automated tripping of generation sources due to power and voltage fluctuations. A blackout of varying degree and potential equipment damage ensues. The remote connections might be established using a variety of methods or combination of methods. These include, but are not limited to, using a lost, stolen, or acquired utility linemen's laptop to access the DMS directly; compromising an active remote maintenance connection used for vendor DMS application maintenance; taking advantage of an accidental bridged connection to the internet due to DMS misconfiguration; or subverting distribution control communications directly.

Substation Categories:

- Automated Protection Systems – Legacy, Transition, Future
- Manually Initiated Systems – Legacy, Transition, Future

Relevant Vulnerabilities:

- *Physical access to mobile devices may enable logical access to business functions by unauthorized individuals,* specifically linemen and maintenance personnel company laptops used for remote connections, (Transient Systems[8])
- *System relies on credentials that are easy to obtain for access* to company computers, (Automated Protection Systems, Manually Initiated Systems)
- *Physical access may be obtained by unauthorized individuals* to proprietary utility documents and information, (Automated Protection Systems, Manually Initiated Systems)
- *System permits unauthorized changes* by allowing remote access for vendors to do application maintenance and troubleshooting, (Automated Protection Systems, Manually Initiated Systems)
- *System makes messages accessible to unauthorized individuals* in the distribution control communication channel. (Automated Protection Systems, Manually Initiated Systems)

Impact:

- Loss of customer power,
- Disclosure of proprietary utility documents or information,
- Possible customer and utility equipment damage.

Potential Mitigations:

- *Require strong passwords* with complexity requirements for company devices and systems, (Automated Protection Systems, Manually Initiated Systems, Cyber Security Systems)
- *Train personnel* to protect company information and documents from unauthorized disclosure, (Design, policies, and procedures)
- *Define policy* on handling sensitive information. This includes substation one-line diagrams, equipment information, communication architectures, protection schemes, load profiles, etc., (Automated Protection Systems, Manually Initiated Systems)
- *Train personnel* (operations and maintenance employees) to handle and protect company computing devices securely, incorporating two-factor authentication, requirements on storing devices, and reporting instructions in cases of loss or theft, (Automated Protection Systems, Manually Initiated Systems)
- *Create audit log* of all changes in HMI control actions, (Manually Initiated Systems)
- *Generate alerts* for all changes for all changes in HMI control actions, (Manually Initiated Systems)

---

[8] This is a new device category that will be added in 2017 to the diagrams.)

- *Restrict remote access* of vendor connections (e.g., physically disconnect remote connections when not in use), (Automated Protection Systems, Manually Initiated Systems)
- *Require two-person rule* for to verify correct DMS configuration, (Design, policies, and procedures)
- *Implement configuration management* for configuration documents. (Design, policies, and procedures)

DGM.12 Hijacked Substation Wireless Damages Substation Equipment

Description: A threat agent carries out a man in the middle attack, hijacking the wireless communications channel to a substation transformer. The threat agent uses this capability to disable transformer cooling fans and overheat the device. Depending on the transformer and its controller, this could be done through a direct command or by drastically increasing oil temperature setpoints. Many transformers are also custom built and have long lead times for replacement or repair.

Substation Categories:

- Manually Initiated Systems – Transition, Future
- Communications Systems –Transition, Future

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* between the substation controller and the transformer, (Manually Initiated Systems, Communications Systems)
- *System makes messages accessible to unauthorized individuals* in the wireless communication channel. (Communications Systems)

Impact:

- Loss of customer power,
- Damage to critical substation equipment,
- Monetary loss.

Potential Mitigations:

- *Authenticate users* of wireless communications, (Communications Systems, Cyber Security Systems)
- *Design for trust* by replacing wireless communications with wired ones, (Design, policies, and procedures)
- *Create audit log* of all changes in control functions and set points, (Manually Initiated Systems)
- *Generate alerts* for unusual changes in control functions and set points. (Manually Initiated Systems)

DGM.13 Out of Scope

DGM.14 Power loss due to lack of serial communication authentication

Description: Serial communications to substations over phone lines often lack authentication of field devices, such as RTUs. This might allow a threat agent to directly dial into modems attached to RTU equipment by war dialing city phone numbers or company phone extensions. Such techniques could allow a threat agent to send breaker trip commands to substation relays and disconnect feeders.

Substation Categories:

- Manually Initiated Systems – Legacy, Transition
- Communications Systems - Legacy

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to substation relays and RTU (e.g., no passwords or default passwords), (Manually Initiated Systems)
- Publicly accessible and/or third party controlled links used, (Communications Systems)
- *System makes messages accessible to unauthorized individuals* using public communications channels without encryption. (Communications Systems)

Impact:

- Loss of customer power,
- Monetary loss,
- Negative publicity.

Potential Mitigations:

- *Authenticate users* of serial communications using strong passwords, (Cyber Security Systems)
- *Design for trust* and migrate serial communications to field devices from public phone lines to private communication channels. (Design, policies, and procedures)

DGM.15 Out of Scope

DGM.16 Threat agent compromises serial control link to substation

Description: The Telco/Commercial Service Provider (CSP) provides communications capability between the utility's substation and headend/control center. Both wired and wireless based interfaces may be involved depending on the particular utility standards and site-specific constraints. Wired-based communication links can be analog or digital leased lines, while wireless interfaces are typically radio, cellular or even satellite based. To establish the Telco/CSP end-to-end communications, a point of demarcation (Demarc) is provided where the local utility owned communications infrastructure interfaces the telco owned network infrastructure (see Figure C-2 below). A knowledgeable threat agent can compromise the serial communications at the Demarc by intercepting and selectively modifying communicated data to masquerade as a user (man-in-the-middle) or replay attack, in which the threat agent captures control messages and subsequent retransmission with the intent of producing an unauthorized effect. This can

potentially compromise both real-time (sometimes referred to as operational) traffic as well as non-real-time (sometimes referred to as non-operational) traffic. In the context of real-time data exchanges, the substation gateway or RTU in the substation be affected by manipulating command and control messages in the direction of the substation. In the case of non-operational data exchanges, IED settings can be potentially manipulated.

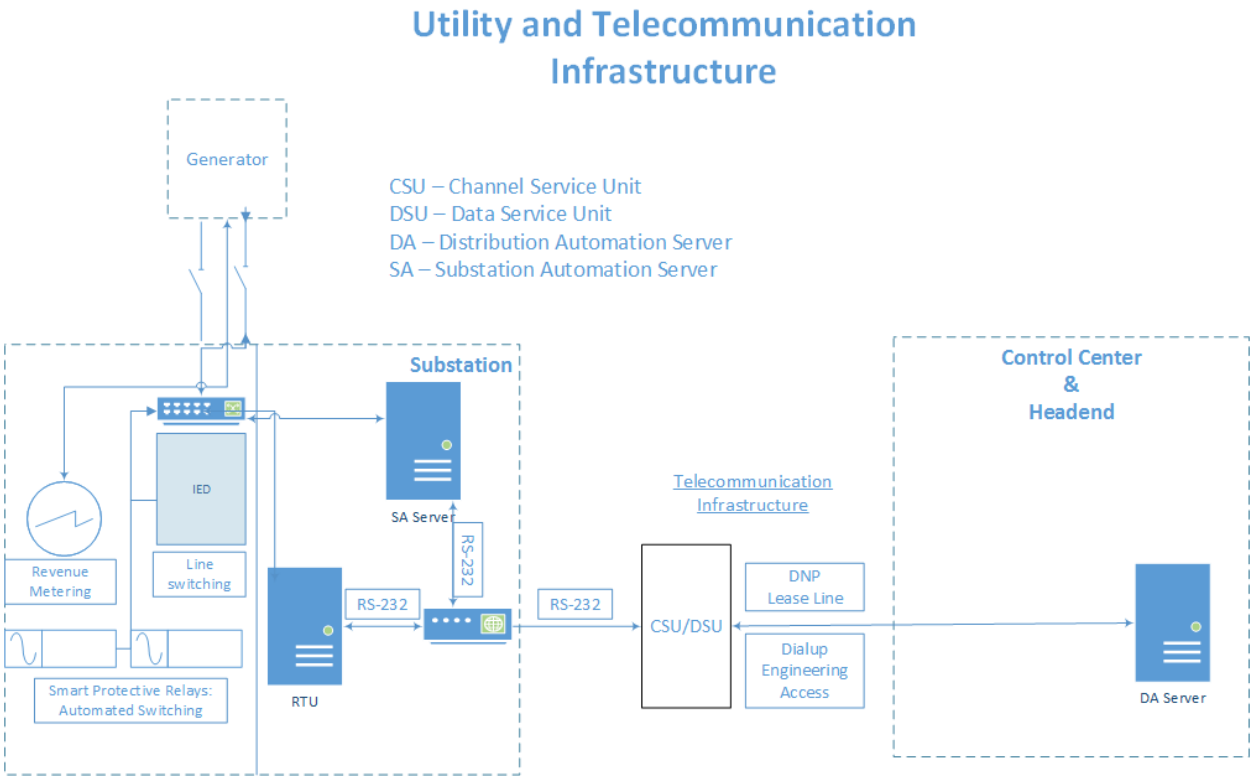


Figure C-2
Threat Agent Compromises Serial Control Link to Substation

Substation Categories:

- Manually Initiated Systems – Legacy, Transition
- Communications Systems – Legacy, Transition

Relevant vulnerabilities:

- *Unnecessary network access is permitted* allowing access of threat agent to the demarc or within the service providers network CSU/DSU, (Communications Systems)
- *System relies on credentials that are easy to obtain for access* to substation gateway/RTU or SCADA FEP, (Manually Initiated Systems, Communications Systems)
- *Users lack visibility of unapproved access to the demarc,* (Communications Systems)
- *Commands or other messages may be inserted on the network by unauthorized individuals* in the communication protocol, (Communications Systems)
- *System makes messages accessible to unauthorized individuals* over the serial link, (Communications Systems)

- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the communication protocol, (Manually Initiated Systems)
- *A copy of a prior message or command is difficult or infeasible to distinguish from a new legitimate message or command* over the serial link. (Manually Initiated Systems)

Impact:

- Loss of customer power, possibly to critical customers (e.g., hospital),
- Potential customer and utility equipment damage,
- Financial loss associated with any equipment damage or restoration to normal operations,
- Increase in public safety concerns (e.g., loss of heating or cooling on extremely cold or hot days),
- Negative impact on customer service due to increase in calls and complaints,
- Damage to goodwill toward utility.

Potential Mitigations:

- *Implement approved cryptographic algorithms* to protect the integrity of communications, (Cyber Security Systems)
- *Require authentication* on all data exchanges, (Manually Initiated Systems, Communication Systems)
- *Require multi-factor authentication* by Telco/CSP to the device containing CSU/DSU units through service level agreement (SLA), (Design, policies, and procedures)

C.6 Generic

This section presents a set of use cases which are generic. Particular cases of these generic use cases can be found among the use cases listed for specific domains in the previous sections. They are discussed in their generic form here to enable the reader to recognize additional instances of these types of use cases**.**

Generic.1 Malicious and Non-malicious Insiders Pose Range of Threats

Description: Authorized personnel - who may be operators, engineering staff or administrators, become active threat agents with legitimate access to IT, field systems, and/or control networks.

Substation Categories:

- Automated Protection Systems – Legacy, Transition, Future
- Manually Initiated Systems – Legacy, Transition, Future
- Monitoring and Measurement Systems – Legacy, Transition, Future
- Communications Systems – Legacy, Transition, Future
- Support Systems – Legacy, Transition, Future
- Cyber Security Systems – Legacy, Transition, Future

Relevant Vulnerabilities:

- *Users and hardware/software entities are given access unnecessary for their roles* to perform duties that should be separated, (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)
- *System permits unauthorized changes,* (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)
- *Users lack visibility of unapproved access* when privileges are elevated for access to security-relevant or operationally critical functions, (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)

Impact:

- Authorized personnel with legitimate access can inflict significant damage on a system either intentionally or by mistake. The impact for this scenario could range from a minor system being offline to a widespread outage of unknown duration.

Potential Mitigations:

- *Require separation of duties*, (Design, policies, and procedures)
- *Use RBAC* to limit access, (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)
- *Detect abnormal behavior* including out-of-policy behavior by authorized users in control networks through protection mechanisms and situational awareness (SIEM, IDS, firewalls, logging, and monitoring), (Cyber Security Systems)
- *Define procedures* for processing suspected or confirmed security incidents involving an insider, (Design, policies, and procedures)
- *Define procedures* concerning access to security-relevant and operationally critical functionality. (Design, policies, and procedures)

Generic.2 Inadequate Network Segregation Enables Access for Threat Agents

Description: A threat agent compromises an asset that has access to the Internet via the "business" network. The asset on the business network also has access to a control system asset or network. The compromise of the business network asset provides a pivot point for the threat agent to gain control of a control system asset or network.

Substation Categories:

- Automated Protection Systems – Transition, Future
- Manually Initiated Systems – Transition, Future
- Monitoring and Measurement Systems – Transition, Future
- Communications Systems –Transition, Future
- Support Systems – Transition, Future

- Cyber Security Systems – Transition, Future

Relevant Vulnerabilities:

- *Network interconnections provide users and hardware/software entities with access unnecessary for their roles* such as using virtual local area networks (VLANs) for security or using the same networks for business operations and control systems, (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)
- *Remote access may be obtained by unauthorized individuals* (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)
- *Network is connected to untrusted networks* that are viewed as trusted, specifically the control systems network is connected to the business network and views the business network as trusted. (Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)

Impact:

- The impact for this scenario could range from a minor system being offline to a widespread outage of unknown duration.

Potential Mitigations:

- *Isolate networks* that host business systems from those that host control systems, (Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)
- *Generate alerts* using a SIEM and monitor alerts according to the associated risks. This includes alerts generated by firewalls, anti-virus, and specific systems, (Cyber Security Systems)
- *Isolate networks* with a defensible, defense in depth, network architecture which includes a demilitarized zone (DMZ), (Design, policies, and procedures)
- *Enforce restrictive firewall rules* to achieve network isolation, (Cyber Security Systems)
- *Require intrusion detection and prevention*, (Cyber Security Systems)
- *Train personnel* to monitor traffic to and from the Internet and to recognize when an incident is occurring, (Design, policies, and procedures)
- *Define incident response plan* to reduce response time when incidents do occur, (Design, policies, and procedures)
- *Define contingency plan* as part of the incident response plan, to maintain adequate resiliency in high-priority control systems. (Design, policies, and procedures)

Generic.3 Portable Media Enables Access Despite Network Controls

Description: A threat agent introduces counterfeit firmware or software, a virus, or malware via removable media to obtain partial or total control of a device or networked system.

Substation Categories:

- Automated Protection Systems – Legacy, Transition, Future
- Manually Initiated Systems – Legacy, Transition, Future
- Monitoring and Measurement Systems – Legacy, Transition, Future
- Communications Systems – Legacy, Transition, Future
- Support Systems – Legacy, Transition, Future
- Cyber Security Systems – Legacy, Transition, Future

Relevant Vulnerabilities:

- *Physical access may be obtained by unauthorized individuals* to interfaces such as USB, Firewire, or serial ports that allows the unrestricted ability to load software or firmware to devices. (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)

Impact:

- The impact for this scenario could range from a minor system being offline to a widespread outage of unknown duration.

Potential Mitigations:

- *Configure for least functionality* by using software controls or other non-physical methods to disable unnecessary interfaces on equipment, (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)
- *Verify settings* on equipment before the equipment is installed in the field, (Design, policies, and procedures)
- *Test before installation* of equipment in the field, (Design, policies, and procedures)
- *Vulnerability scan before installation* of equipment in the field, (Design, policies, and procedures)
- *Require periodic walk-downs* of equipment to help ensure there are not any new unauthorized devices connected, (Design, policies, and procedures)
- *Define policy* outlining acceptable and unacceptable use of portable computing devices in a business/corporate local area network (LAN) environment and a control LAN environment, (Design, policies, and procedures)
- *Train personnel* under a user awareness training program that includes portable media guidelines. (Design, policies, and procedures)

Generic.4 Supply Chain Attacks Weaken Trust in Equipment

Description: An adversary replaces a legitimate device with a maliciously altered device and introduces the device into the supply chain without directly compromising a manufacturing entity. This can be done by buying a legitimate device, buying or creating a malicious device and

returning the malicious device in place of the legitimate device as an exchange. Alteration may be a modification or deletion of existing functions or addition of unexpected functions.

Substation Categories:

- Automated Protection Systems – Legacy, Transition, Future
- Manually Initiated Systems – Legacy, Transition, Future
- Monitoring and Measurement Systems – Legacy, Transition, Future
- Communications Systems – Legacy, Transition, Future
- Support Systems – Legacy, Transition, Future
- Cyber Security Systems – Legacy, Transition, Future

Relevant Vulnerabilities:

- *Sensitive data remains on disposed equipment* and allows a threat agent to acquire and reverse engineer equipment, (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems)
- *System permits unauthorized changes* in the supply chain. (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems; Design, policies, and procedures)

Impact:

- Depending on the level of sophistication of the threat agent, this scenario can result in the complete loss of confidentiality, integrity, and availability of systems using equipment from an infiltrated supply chain.

Potential Mitigations:

- *Develop SLA* for procurement which verifies the manufacture and origin of equipment from a known good and reputable source, (Design, policies, and procedures)
- *Define policy* addressing disposal which prevents the acquisition of sensitive parts from excessed or disposed devices, (Design, policies, and procedures)
- *Perform audit* of the supply chain periodically, to ensure adequate quality control, (Design, policies, and procedures)
- *Detect abnormal behavior* that may indicate supply chain issues, such as unauthorized communications or behavior by deployed devices in the system network, (Cyber Security Systems; Design, policies, and procedures)
- *Test before installation*, to detect unwanted functionality before putting devices into production. The objective is to validate functionality and usability. (Design, policies, and procedures)

Generic.5 Malicious Code Injected via Physical Access

Description: A threat agent injects malicious code through physical access of engineering serial ports or by memory update devices such as USB memory sticks, Secure Digital (SD) cards or Compact Flash (CF) cards. Examples of target equipment include communications concentrators,

remote terminal units (RTUs), and protection relays. Malicious code could change device settings for purposes of rendering equipment inoperable, data gathering, denial of service, or misconfiguration.

Substation Categories:

- Automated Protection Systems – Legacy, Transition, Future
- Manually Initiated Systems – Legacy, Transition, Future
- Monitoring and Measurement Systems – Legacy, Transition, Future
- Communications Systems – Legacy, Transition, Future
- Support Systems – Legacy, Transition, Future
- Primary Power Equipment Systems – Transition, Future

Relevant Vulnerabilities:

- *Unnecessary access is permitted to system functions* via engineering and console ports of substation equipment, (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Primary Power Equipment Systems)
- *System permits unauthorized changes* to software and information, (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Primary Power Equipment Systems)
- *Physical access may be obtained by unauthorized individuals,* (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Primary Power Equipment Systems)
- *Enabled but unused ports* (unused engineering and console ports). (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Primary Power Equipment Systems)

Impact:

- Substation components could be modified to fail detection and clearing of bus and feeder faults (although these can be managed by reclosers which are not necessarily in the substation). These faults could lead to destruction of electrical grid equipment,
- Substation components could be reprogrammed to disallow feeder sectionalizing or service restoration via SCADA. However, these are frequently done manually,
- Modification of devices controlling VOLT/VAR equipment, including load tap changers, SVCs, automatic voltage regulators, and synchronous condensers, could prevent direct voltage control leading to potential customer equipment damage, over/under voltage trips, or additional power losses,
- Equipment firmware changes may create the need for equipment servicing that can be costly and time consuming,
- Possible lack of monitoring capabilities reduces situational awareness, inhibits a utility's ability to react proactively, and could increase the number and duration of failures.

Potential Mitigations:

- *Restrict device access* (both physical and logical) to protective relays and other critical devices, (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems, Primary Power Equipment Systems)
- *Check software execution integrity* of software in substation equipment, since software may be compromised when loaded for execution, (Design, policies, and procedures)
- *Configure for least functionality* by disabling unused console and engineering ports on intelligent electronic devices (IEDs), (Design, policies, and procedures)
- *Create audit log* of substation actions, (Cyber Security Systems)
- *Generate alarms* for any serious anomalies, such as connection changes and device configuration changes in substations, (Cyber Security Systems)
- *Restrict physical access* to substation using, for example, card swipes, pin codes, etc., (Cyber Security Systems; Design, policies, and procedures)
- *Require video surveillance* of the human interfaces to the DGM equipment, (Cyber Security Systems; Design, policies, and procedures)
- *Restrict access* to engineering functions, (Design, policies, and procedures)
- *Maintain latest firmware* for substation equipment, (Design, policies, and procedures)
- *Maintain patches* for substation equipment, (Design, policies, and procedures)
- *Use Role-Based Access Control* to limit privileges for functions using engineering and console ports of substation equipment, (Automated Protection Systems, Manually Initiated Systems, Monitoring and Measurement Systems, Communications Systems, Support Systems, Cyber Security Systems, Primary Power Equipment Systems; Design, policies, and procedures)
- *Authenticate users* for access to engineering and console ports where feasible. (Cyber Security Systems)

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI members represent 90% of the electric utility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002007887

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com