Electric Sector Failure Scenarios and Impact Analyses – Version 3.0

National Electric Sector Cybersecurity Organization Resource (NESCOR)

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE FOLLOWING ORGANIZATION PREPARED THIS REPORT:

Electric Power Research Institute (EPRI)

Revision History

Version	Date	Changes
0.1	2012.01.30	Initial draft posted to EPRI site
0.5	2012.07.03	Fill in DER failure scenarios, technical and editorial improvements to failure scenario in other domains, names for scenarios, further detail in full scenario template and example write up in Appendix B, refine scenario ranking criteria and method, version for internal NESCOR review
0.6	2012.08.20	Removal of out of scope scenarios, clarifications and editorial improvements based on EPRI comments, version for use in 2012 NESCOR workshop
0.7	2012.08.24	Complete clarifications requested by EPRI, second draft for public release
0.8	2012.11.09	Input from the NESCOR workshop included. The following changes were included: - Executive summary was updated - Section 2 is new - Sections 5.1, 5.2, 5.3 and 5.5 were updated - AMI.1 was generalized - WAMPAC.9 – 12 are new - ET.16 is new - DR.7 is new - DGM.11 was updated - DGM.14 and 15 are new - Appendixes E and F are new
0.9	2013.01.18	The following changes were made: - AMI.1 was restructured and two new scenarios were created AMI.30 and AMI.31 - More input from Argonne National Laboratory was included
0.9a	2013.04.11	The following changes were made: - New section and appendix describing common mitigations analysis. - All failure scenarios have updated mitigations using the mapping presented in the common mitigation appendix.
0.9b	2013.07.26	The following changes were made: - Updated executive summary and introduction - All failure scenarios have been updated with the finalized mitigations mapping and to include feedback from the Team. - The long failure scenario has been removed from the current document, given that they have a dedicated document (both section 4 and the appendix). - WAMPAC.9 was removed - AMI.29 has a minor update: PII => private information - AMI.32 was added (not included in the mitigation analysis) - DGM.9 was updated to include verification for mitigations - DER.2 was updated with a clearer title - New serial control link scenario DGM.16 (impact to be reviewed before the August 2013 Workshop)
1.0	2013.09.06	The following changes were made: - Updated the WAMPAC section, introduced a new impact table that takes into consideration the state and application of the system - Addressed the feedback from EPRI - Updated the NISTIR mapping table - DER.26 was added (as a new scenario spanned from DER.18) - DER.22 was removed - Added a brief description of each domain in their respective sections

Version	Date	Changes
2.0	2014.06.15	The following changes were made: - common vulnerability analysis - all vulnerabilities listed for the scenarios were modified to use common vulnerability terminology and avoid vulnerabilities stated as lack of a mitigation, and mitigations augmented if needed capture information previously in the vulnerability section - common vulnerability list and supplementary information are new appendices - the full mapping of original mitigations to common mitigations is removed as an appendix (moved to separate document) - failure scenario scoring for criteria that influence likelihood and opportunity is reversed to have high scores mean more likely, introduce risk quadrants, retain prior risk calculation method of dividing impact by cost to adversary only as background to scenario rankings done by TWG1
3.0	2015.12.01	The following changes were made: - added generation failure scenarios - updated the common mitigations and common vulnerabilities list to include the generation failure scenarios and V2.0 revision

ACKNOWLEDGMENTS

The research was paid for by the Department of Energy (DOE) under the NESCOR grant.

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, California 94304-1338

Principal Investigator

A. Lee

This report was produced as a collaborative effort between attendees of the National Electric Sector Cybersecurity Organization Resource (NESCOR) workshops in Washington D.C., and industry experts, asset owners, and academia who participate in NESCOR technical working group (TWG) 1. This version was developed by utilities and EPRI.

In addition, the following individuals contributed their technical expertise and time in reviewing, revising, and augmenting the material produced throughout time: Chris Blask, Matthew Carpenter, Stephen Chasko, Glen Chason, Gabriela F. Ciocarlie, Frances Cleveland, Brian Davison, Dick DeBlasio, Dona Dickinson, Michael David, Pat Duggan, Mark Ellison, Shrinath Eswarahally, Irene Gassko, Efrain Gonzales, Slade Griffin, Virgil Hammond, Jordan Henry, Brian Isle, Mladen Kezunovic, Annabelle Lee, E. K. Lee, Ulf Lindqvist, Clifford Maraschino, Catherine Martinez, Carol Muehrcke, Russ Neal, Ray Parks, Charles Payne, Tomo Popovic, Alan Rivaldo, Justin Searle, John Simmins, Elizabeth Sisley, Shabbir Shamsuddin, Rebecca Slayton, Scott D. Sternfeld, Zachary Tudor, Ersin Uzun, Ron Vader, Russel C. Van Tuyl, Louis Wilder, Erica Wingad, Justin Thibault, Jason Christopher, Revis James, Joyce Sanders, and Scott Rosenberger.

Executive Summary

The National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1 (TWG1) developed previous versions of this document on the topic of cyber security failure scenarios and impact analyses for the electric sector. This version includes the addition of generation failure scenarios and updates to the common mitigations and vulnerabilities analyses. The information about potential cyber security failure scenarios is intended to be useful to utilities for risk assessment, planning, procurement, training, tabletop exercises and security testing. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power.

The present document includes the following:

- How a utility may use this document (Section 2),
- A threat model (Section 3),
- Criteria, method and results of prioritization of the failure scenarios (Section 4),
- A list of failure scenarios using consistent terminology for vulnerabilities and mitigations (Section 5),
- An analysis of vulnerabilities by frequency of appearance in the failure scenarios (Section 6),
- An analysis of mitigations by frequency of appearance in the failure scenarios (Section 7).

The guidance on how to use this document includes a discussion of its use in conjunction with the National Institute of Standards and Technology Interagency Report (NISTIR 7628) Revision 1, *Guidelines for Smart Grid Cybersecurity*, September 2014 and the Department of Energy (DoE) Electricity Sub-Sector Cybersecurity Capability Maturity Model (ES-C2M2). Appendix C includes mapping of failure scenarios to NISTIR 7628 controls.

The failure scenarios are organized in six categories, corresponding to the domains identified in the National Institute of Standards and Technology (NIST) Special Publication 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0,* Office of the National Coordinator for Smart Grid Interoperability.

1. Advanced Metering Infrastructure (AMI)
2. Distributed Energy Resources (DER)
3. WAMPAC (Wide Area Monitoring, Protection, and Control)
4. Electric Transportation (ET)

5. Demand Response (DR)
6. Distribution Grid Management (DGM)

In addition, there are failure scenarios in two additional categories: Generation (GEN) and Generic. Generic includes failure scenarios that may impact many of these functional domains.

Failure scenarios include malicious and non-malicious cyber security events such as:

- Failures due to compromising equipment functionality,
- Failures due to data integrity attacks,
- Communications failures,
- Human error,
- Interference with the equipment lifecycle, and
- Natural disasters that impact cyber security posture.

Impacts identified in the failure scenarios include loss of power, equipment damage, human casualties, revenue loss, violations of customer privacy, and loss of public confidence. Listed below are some potential impacts.

- A number of attack vectors may result in interference with delivery of or compliance with demand response messages. Any of these have the potential to unbalance power generation and load in a system that has been fine-tuned to anticipate power usage in accordance with demand response.

- Unintentional or intentional modification of time-of-use (TOU) pricing could result in generation/load imbalance leading to power loss.

- Repair of inadequately implemented distributed cryptographic functions for meter communication could be costly. There may be additional costs if actual violations of customer privacy have occurred.

- Interference with the time synchronization of Wide Area Monitoring, Protection and Control (WAMPAC) messages could limit the capability to respond to an imbalance of generation and load that has occurred for any reason.

In this version of the document, vulnerabilities use a common naming schema across all scenarios. The common form for a vulnerability consists of a *common vulnerability* and a *context*. Vulnerabilities identified in the failure scenarios are categorized into 23 vulnerability classes from NISTIR 7628 Volume 3. The mitigations for all scenarios also use a common naming schema, introduced in the prior version of this document. The common form for mitigations consists of a *common action* along with an *action*

application. There are 22 groups of common actions across all scenarios. Analysis of mitigations across all scenarios showed that automatic and manual mitigations are nearly evenly applied.

The failure scenarios, impacts, and mitigations were developed from a “bottom-up,” rather than a top-down assessment of potential cyber security events. Their focus is on cyber security events; hence, they do not consider requirements that are outside this scope (e.g., redundancy that supports reliability, general cyber-physical requirements such as range checking for values, etc.). The failure scenarios included in this document are not intended to be a complete list of all possible failure scenarios, and their mitigations are a suggested list of recommendations intended to provide a variety of options. The scenario write-ups are brief, and commonly include specific details to aid understanding. This is in contrast to a single more general failure scenario that includes significant details to address all elements.

Table of Contents

Table of Figures

Table of Tables

List of Failure Scenarios

1
INTRODUCTION AND SCOPE

The National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1 (TWG1) developed previous versions of this document on the topic of cyber security failure scenarios and impact analyses for the electric sector. This version includes the addition of generation failure scenarios and updates to the common mitigations and vulnerabilities analyses. The information about potential cyber security failure scenarios is intended to be useful to utilities for risk assessment, planning, procurement, training, tabletop exercises and security testing. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. Some of the scenario descriptions include activities that typically are not allowed by policies, procedures, or technical controls. These scenarios may be used to ensure that the applicable mitigation strategies are specified and implemented.

The present document includes the following:

- How a utility may use this document (Section 2),
- A threat model (Section 3),
- Criteria, method and results of prioritization of the failure scenarios (Section 4),
- A list of failure scenarios using consistent terminology for vulnerabilities and mitigations (Section 5),
- An analysis of vulnerabilities by frequency of appearance in the failure scenarios (Section 6),
- An analysis of mitigations by frequency of appearance in the failure scenarios (Section 7).

The guidance on how to use this document includes a discussion of its use in conjunction with the National Institute of Standards and Technology Interagency Report (NISTIR 7628) Revision 1, *Guidelines for Smart Grid Cybersecurity*, September 2014 and the Department of Energy (DoE) Electricity Sub-Sector Cybersecurity Capability Maturity Model (ES-C2M2). Appendix C includes mapping of failure scenarios to NISTIR 7628 controls.

The failure scenarios are organized in six categories, corresponding to the domains identified in the National Institute of Standards and Technology (NIST) Special Publication 1108, *NIST Framework and Roadmap for Smart Grid Interoperability*

Standards, Release 1.0, Office of the National Coordinator for Smart Grid Interoperability.

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

In addition, there are failure scenarios in two additional categories: Generation (GEN) and Generic. Generic includes failure scenarios that may impact many of these functional domains.

Failure scenarios include malicious and non-malicious cyber security events such as:

- Failures due to compromising equipment functionality,
- Failures due to data integrity attacks,
- Communications failures,
- Human error,
- Interference with the equipment lifecycle, and
- Natural disasters that impact cyber security posture.

Impacts identified in the failure scenarios include loss of power, equipment damage, human casualties, revenue loss, violations of customer privacy, and loss of public confidence. Listed below are some potential impacts.

- A number of attack vectors may result in interference with delivery of or compliance with demand response messages. Any of these have the potential to unbalance power generation and load in a system that has been fine-tuned to anticipate power usage in accordance with demand response.

- Unintentional or intentional modification of time-of-use (TOU) pricing could result in generation/load imbalance leading to power loss.

- Repair of inadequately implemented distributed cryptographic functions for meter communication could be costly. There may be additional costs if actual violations of customer privacy have occurred.

- Interference with the time synchronization of Wide Area Monitoring, Protection and Control (WAMPAC) messages could limit the capability to respond to an imbalance of generation and load that has occurred for any reason.

In this version of the document, vulnerabilities use a common naming schema across all scenarios. The common form for a vulnerability consists of a *common vulnerability* and a *context*. Vulnerabilities identified in the failure scenarios are categorized into 23 vulnerability classes from NISTIR 7628 Volume 3. The mitigations for all scenarios also use a common naming schema, introduced in the prior version of this document. The common form for mitigations consists of a *common action* along with an *action application*. There are 22 groups of common actions across all scenarios. Analysis of mitigations across all scenarios showed that automatic and manual mitigations are nearly evenly applied.

The failure scenarios, impacts, and mitigations were developed from a “bottom-up,” rather than a top-down assessment of potential cyber security events. Their focus is on cyber security events; hence, they do not consider requirements that are outside this scope (e.g., redundancy that supports reliability, general cyber-physical requirements such as range checking for values, etc.). The failure scenarios included in this document are not intended to be a complete list of all possible failure scenarios, and their mitigations are a suggested list of recommendations intended to provide a variety of options. The scenario write-ups are brief, and commonly include specific details to aid understanding. This is in contrast to a single more general failure scenario that includes significant details to address all elements.

It is assumed that the readers of this document have knowledge of the electric sector and basic cyber security concepts.

The failure scenarios included in this document are not intended to be a complete list of all possible failure scenarios. Rather, they are a useful representative list of the cyber security challenges facing the electric sector. The scenario write-ups are brief, and commonly include specific details to aid understanding. This is in contrast to a single more general failure scenario that includes significant details to address all scenario elements.

Further work that extends these results are found in the following documents. The first document provides in depth analysis of a subset of high priority failure scenarios from the present document, using attack tree analysis methods. The second document illustrates how the failure scenarios and the ranking method in the present document can be used by a utility for risk assessment.

- "Analysis of Selected Electric Sector High Risk Failure Scenarios," Version 2.0, results from NESCOR TWG1 published at: http://www.smartgrid.epri.com/doc/nescor%20detailed%20failure%20scenarios%2009-13%20final.pdf

- "*Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology*" a joint DOE/EPRI effort published at: http://energy.gov/sites/prod/files/2014/05/f15/IntegratingElectricitySubsectorFailureScenariosIntoARiskAssessmentMethodology_1.pdf

2
HOW TO USE THIS DOCUMENT

This document provides a resource for utilities to gain an understanding of cyber security risks and potential mitigations in various functional domains. The material is designed to support risk assessment, policies, planning, procedures, procurement, training, tabletop exercises and security testing. This section outlines how a utility might use the document for these purposes, in conjunction with other related resources that have been developed for the electric sector.

2.1 Risk Assessment

Risk assessment involves identifying threats, vulnerabilities, and the potential impact and risk associated with the potential exploitation of those vulnerabilities. Appropriate mitigations are then identified to lower risk where deemed necessary. Vulnerabilities and mitigations in this document use a common naming schema that improves readability and comprehension, and enables their prioritization.

An approach to risk assessment leveraging this document could involve the following steps:

- An organization evaluates the failure scenarios in Section 5 to determine which scenarios are applicable to its current or future implementations.

- Systems owners and security personnel together assess the potential impact and risk to the organization. The failure scenario ranking criteria in Section 4 can be tailored as appropriate and used to perform this assessment.

- To change the risk exposure of the highest risk failure scenarios, security controls should be implemented to mitigate the potential vulnerabilities listed in the scenarios. Included for consideration within each failure scenario are potential mitigations developed by TWG1. There are other comprehensive industry standards, guidelines, and regulations that can also be applied to further lessen the impact and/or mitigate the scenarios. Two examples of such resources that are discussed in the following paragraphs are:

    - The National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628 Revision 1, *Guidelines for Smart Grid Cybersecurity*, September 2014

- The Department of Energy (DOE) The *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2),* February 2014

NIST has recognized the role of information technology in the Smart Grid and the need to protect it. NISTIR 7628 is a publication containing Guidelines for Smart Grid Cyber Security. The document provides numerous security controls that have been vetted by industry key players as both valuable and pertinent. A logical next step is to couple the NESCOR failure scenarios with the NISTIR 7628 security controls. Combining these efforts provides substantial knowledge to the electric sector in identifying key scenarios that have the potential to critically impact the business along with industry best practices for mitigating threats to the smart grid. Appendix C includes a mapping of the failure scenarios to the NISTIR 7628 requirement families. Asset owners can use such a mapping to select specific requirements to apply to their systems from the comprehensive set provided in the NISTIR 7628.

The DOE Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) provides guidance on the management and implementation of cyber security practices associated with the operation and use of operational technology and information technology. This document was also developed in partnership with many government agencies and industry professionals and stakeholders. The ES-C2M2 provides a valuable set of practices that measure the maturity of an organization's cyber security program. The practices given in the ES-C2M2 illustrate what a mature cyber security program looks like and can be directly correlated to security controls that, if implemented, may provide value to an organization. Failure scenarios of interest to an organization could be mapped to those ES-C2M2 practices associated with each maturity level that serve to mitigate the failure scenario. An organization that has implemented the maturity model could use such a mapping to predict (and then verify) those failure scenarios against which it should have significant protections due to its maturity level, and those to which it may be most vulnerable.

Section 1 references a separate document developed by DOE and EPRI to illustrate how to perform risk assessment leveraging the results of the present document, together with other resources available to the electricity subsector. Development of further detailed guidance is planned in the area of risk management, to relate and integrate these resources into an overall process.

2.2 Planning

Risk assessment as described in Section 2.1 is the key planning tool for implementation of an effective cyber security program. New cyber security technologies and practices for a utility are ideally driven by the results of the risk assessment process as well as industry regulations. Once the highest risk failure scenarios have been identified,

potential mitigations for these scenarios include both technology purchases as well as organizational processes that must be defined, vetted, and implemented.

2.3 Procurement

A utility may purchase devices, systems or integration services related to a particular domain covered in this document, such as smart meters (AMI) or management systems for distributed energy resources (DER). As part of the procurement process, the utility could walk through the failure scenarios for that domain in Section 5 of this document, and identify those scenarios applicable to a new device or system. The utility may use those scenarios and potential mitigations to define product procurement requirements. The list of desired mitigations may be enhanced using the NISTIR 7628 and the ES-C2M2 as described in Section 2.1. The utility may also use the failure scenarios to formulate questions to the vendor:

- How do users of your product typically achieve protection against the failure scenario?
- Does your product itself provide protection against this failure scenario? Why or why not?
- Are there potential mitigations listed under this scenario that your product supports?
- Are there other mitigations supported by your product that protect against this failure scenario?

2.4 Training

Full comprehension of this document assumes general cyber security awareness and a basic understanding of cyber security concepts such as access control, authentication and cryptography. Given this general background, this document can serve as a tool to bridge the gap between generic cyber security concepts and their specific potential impact on a utility's business. In particular, a utility may select failure scenarios from this document that are of specific interest to their business mission, tailor them for their organization, and use them as examples within utility-specific training programs focused on cyber security.

2.5 Tabletop Exercises

A tabletop exercise is a paper walkthrough of a potential event by representatives of the various players that would participate in responding to an actual instance of that event. A utility may find that many of the potential mitigations listed in Section 5 take the form of processes rather than technologies. In this case, a tabletop exercise is an excellent method to determine whether the mitigating processes are well-thought-out and fully understood by all relevant players in the organization.

2.6 Security Testing

The risk associated with some failure scenarios relevant to a particular utility may initially be unclear. This is because the existence of the relevant vulnerabilities associated with this scenario may likewise be unclear. In some cases, this uncertainty may be resolved by consulting documentation or system experts. In other cases, security testing may be identified as the only reliable method to determine if the relevant vulnerability exists. Hence an analysis of the relevance of the failure scenarios to a utility can yield a specific set of security tests for the purpose of defining the existence of specific vulnerabilities related to the scenarios.

The failure scenarios can also aid in scoping priorities for functional security testing. For example, a utility might select its top five ranked failure scenarios and run functional security tests of the cyber mitigations that protect against these scenarios, as well as table top exercises for the process mitigations for these scenarios.

3
FAILURE SCENARIO THREAT MODEL

A *threat model* includes a list of the threat agents that were considered when developing failure scenarios. A *threat agent* is a class of actors that could cause a failure scenario to occur in some specified domain, either as the sole cause or as a contributor to it. Typical examples of threat agents are state-sponsored groups or individuals, insiders (whether malicious or non-malicious), and recreational criminals.

3.1 Threat Model Background

The threat model for this effort has several purposes. The first purpose is to support development of appropriate mitigation strategies for a failure scenario. This requires understanding the causes of the failure scenario. To be effective, mitigation strategies must take into account the motivation, tactics, and capabilities of those threat agents that may cause the failure scenario to occur. A second purpose is to aid in identifying failure scenarios that could otherwise be missed altogether, due to a lack of understanding of the full set of threat agents and their characteristics. The third purpose is to aid in prioritizing failure scenarios for analysis and mitigation. Failure scenarios that are given high priority should be considered to be of serious interest to a capable threat agent. Utilities do not have unlimited resources to address all potential threats and failure scenarios and they need to focus on the failure scenarios that are the most critical to the organization. The list of high priority failure scenarios will vary from utility to utility.

Therefore, a threat model is useful to the extent that it supports these purposes. A threat agent category should define a group of actors with similar characteristics that may contribute in a similar way to similar kinds of failures. The same types of potential mitigations should be applicable to all the threat agents in a threat agent category; hence, the need for a common mitigation schema.

To scope the threat model more precisely, the team specified the term *failure scenario.* Specifically, these are *cyber security failure scenarios.* A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. The domain for the threat model here includes cyber security events that impact (1) the delivery of electricity, (2) the business of running a utility and/or (3) the interests of the customers of a utility. In the following discussion, the term the “electric sector cyber security domain” is used.

3.1.1 Methodology for Development of the Threat Model

To develop a threat model for the electric sector cyber security domain, TWG1 identified a number of existing “reference” threat models, described in Appendix A. These models identify threat agent categories used in other domains that share some characteristics with the electric sector cyber security domain. Those domains are: (1) missions for specific individual public and private sector organizations that provide critical infrastructure in Minnesota, (2) the energy infrastructure in Europe and (3) safety in general, specifically where the cause of failure is due to human error. The topic of human error was not included in the first two reference threat models. TWG1 members believed that human error should be incorporated in the threat model for the electric sector cyber security domain.

3.2 Electric Sector Cyber Security Threat Model

Table 1 below shows the TWG1 electric sector cyber security domain threat model that was developed using the reference threat models and tailored to the electric sector based on feedback from TWG1 participants. The reference threat models are included in Appendix A. In particular, the electric sector cyber security domain threat model incorporates the following elements:

- Adversaries with intent, driven by money, politics, religion, activist causes, recreation, recognition or simply malevolence
- Adversary activity may include spying or have direct impact on operations
- Insiders or outsiders, groups or individuals
- Failure in people, processes, and technology, including human error
- Loss of resources, in particular key employees or communications infrastructure
- Accidents
- Natural hazards as they impact cyber security.

Intentional adversaries are grouped to separate them by motive and modus operandi.

Table 1 - Electric Sector Cyber Security Domain Threat Model

Threat Agent	Subcategory	Example Members
Economic Criminals		

Threat Agent	Subcategory	Example Members
	Transnational or national criminal Organization	Former Soviet Union Mafia, extortion groups[1]
	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[2], Hamas
Hazards		
	Natural hazards	Tornados, pandemics, floods, earthquakes

[1] http://www.safetyissues.com/site/cyber_crime/cia_reveals_hacker_attacks_on_utilities.html?print
[2] http://en.wikipedia.org/wiki/Lashkar-e-Taiba

Threat Agent	Subcategory	Example Members
	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

Economic criminals are driven by money and malicious criminals are driven by emotion and the desire to harm. Recreational criminals are driven by the desire for fun or self-promotion.

“Other hazards to required resources” refers to loss or degradation of resources required to maintain cyber security, for reasons not otherwise covered in the threat model.

4
FAILURE SCENARIO RANKING

In addition to developing failure scenarios, TWG1 developed methods for prioritizing the failure scenarios. The approaches and results to date are included in this section and Appendix B.

The initial purpose for prioritizing failure scenarios was to determine work priorities for TWG1. The highest priority failure scenarios would be most important to analyze in detail beyond that provided in this document. Although prioritization of failure scenarios was for the work of TWG1, it is intended that utilities will adapt and tailor the prioritization methods for the purposes of (1) prioritizing their mitigation efforts and (2) incident response.

4.1 Detailed vs. High-Level Ranking

TWG1 developed and used two related ranking methods – a detailed method and a high-level method. The detailed method involves scoring several dozen criteria for each failure scenario, and deriving from these scores two composite scores, corresponding to impact and likelihood of the scenario. The high-level method involves scoring impact and likelihood for each scenario.

The detailed ranking method was developed first, and was applied to several examples to test and refine it. Based upon these trials, the group determined that while the detailed ranking provided valuable information, it would take TWG1 too long to execute it for the full set of scenarios. Hence the group developed a high-level ranking method that could be accomplished more quickly and achieve the TWG1 goal of selecting failure scenarios to analyze in further detail. This section documents both methods. Both can be used by utilities for their own prioritization efforts. The methods can also be used in a manner to complement each other – for example a high-level ranking could be done on all failure scenarios, and then detailed ranking performed on the top ranking subset obtained from the high-level ranking exercise.

TWG1 ultimately ranked all of the failure scenarios using the high-level method. Results are shown in Appendix B. A general understanding of the detailed ranking method will aid the reader in understanding the high level method.

4.2 Detailed Ranking Method

4.2.1 **Overview**

The detailed ranking method ranks the failure scenarios with respect to each other in terms of priority. The ranking method has two components. The first is the set of ranking criteria. These are the characteristics of a failure scenario that are evaluated as input to the ranking process. Examples are financial impact, impact on the distribution grid, and skill required by the threat agent to execute the scenario. The second component of the ranking method is how one combines the ranking criteria to arrive at a composite rank.

To rank failure scenarios, the scoring for each of the ranking criteria identified in Section 4.2.2 below would be used to provide an overall failure scenario that may be graphed. The graph may be divided into sections that identify High, Medium, or Low (H, M, or L) in two separate dimensions:

- Impact
- Effects on Likelihood and Opportunity

For example, a failure scenario might be ranked as (H, M), which means that it has high impact and medium likelihood. (For brevity, "Effects on Likelihood and Opportunity" will be referred to as "likelihood." This is not a probability value, but rather an examination of a set of factors that contribute to likelihood.) A utility may divide the graph into multiple sections for more granularity.

The following steps achieve such a ranking:

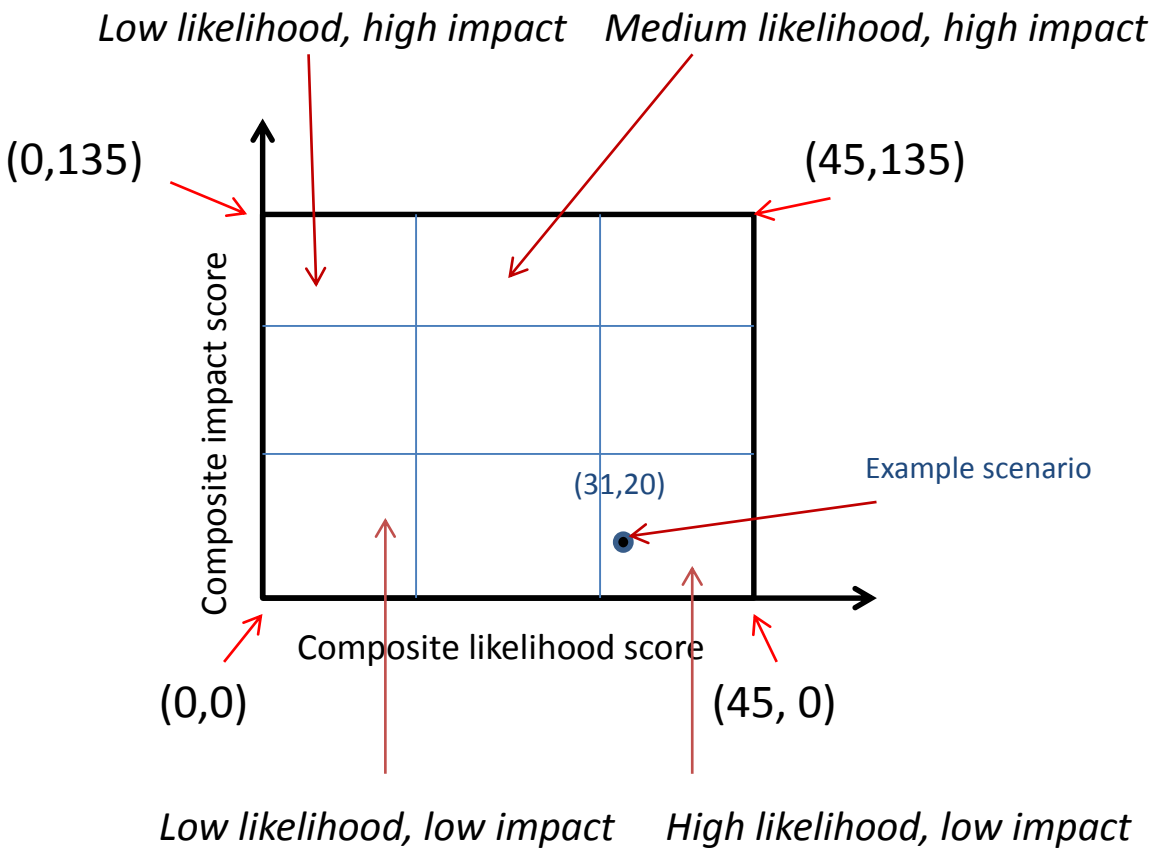
1. Score each failure scenario using each impact and likelihood criterion (each line item in Table 2 and Table 3, respectively). Additional scoring guidance is provided in Appendix B.1.

2. Combine the scores for the set of impact criteria, to create a single numerical composite impact score. Likewise, combine the scores for the set of likelihood criteria, to create an overall likelihood score. The straightforward method of adding the detailed criteria scores is used here, although other methods are possible. Appendix B.2.2 describes some potential refinements.

3. Determine ranges of composite scores for impact and likelihood that will represent a rank of H, M, and L in these dimensions, for a failure scenario.

   The third step can be done after ranking results for all scenarios have been compiled and their natural "clustering" understood. The results of steps 1 and 2 can be displayed in a graphical fashion as shown in Figure 1, where the example shown is described later in this section.

Figure 1. Graphing Ranking Results



The failure scenarios will naturally fall into clusters on the graph. The ranges for H, M, and L can be determined based upon these clusters, together with how the utility decides to address failure scenarios with each possible pair of rankings. These decisions can be calibrated by individually considering failure scenarios that fall near the "boundaries" of the ranking categories.

In prior versions of this document, the ranking method included the calculation of a single numerical rank based upon both impact and likelihood. This was based upon the standard multiplication of impact and probability to obtain risk. Feedback on this prior ranking method in use led to the modification to retain the two dimensions of the rank separately. The reasons for this are: (1) likelihood as defined here is not a probability and (2) the impact score is typically more accurate than the likelihood score. The effect of (1) is that since the impact score is not a probability, the units of the impact and likelihood scores are difficult to relate to each other, as is assumed for the standard risk equation. This raises a question when combining them mathematically. The effect of (2) is that a composite numerical score loses valuable accurate information regarding the severity of impact by combining it with a less accurate likelihood indicator.

4.2.2 **Detailed Ranking Criteria**

As described in the previous sub section, there are two categories of ranking criteria:

- Impact
- Effects on Likelihood and Opportunity

The following sections discuss these criteria and provide an example of how to evaluate them. The criteria for an example failure scenario are scored. The core element in the example failure scenario is a widely deployed smart meter that does not encrypt customer data.

Appendix B.4 lists additional proposed ranking criteria beyond those described in this section that may be useful for an individual utility to apply for planning or incident response purposes. Examples are: whether or not systems affected by a scenario have particular mitigations already in place, whether monitoring detected a particular incident, or whether a scenario has related regulatory issues. These criteria could not be assessed in general by TWG1 for a failure scenario, since they would be unique to particular utility architectures, incidents, and applicable regulations. However, they could be assessed by a single utility for their situation or for a particular incident.

4.2.2.1 Impact Criteria

Table 2 shows the impact criteria and associated scores for the example failure scenario. Impact is the effect of the failure scenario on the delivery of power, the business of the utility, and the interests of its customers. In the following discussion, these criteria are discussed and scored as shown in Table 2 for the example failure scenario.

System Scale: Describes whether the impact of this failure scenario is geographically localized, or may impact the entire system. The example failure scenario potentially affects the entire AMI system, since the faulty meter is widely deployed.

Safety Concern: Two safety criteria consider whether there is a potential for injuries or loss of life. This factor is considered for the public and the utility workforce. For the example failure scenario, first consider the case of public safety. An argument could be made that a threat agent might use unencrypted private information from a meter to put an individual in harm's way. In particular, knowledge of the pattern of electricity usage could allow a thief to better determine how or when to target a particular home. This is not a major impact on public safety, but the score acknowledges a potential impact. There is no safety concern related to this failure scenario for the utility workforce.

Ecological Concern: This criterion considers whether the failure scenario might cause damage to the environment. For example, burning or leaking of hazardous material

would be judged as “Permanent Ecological Damage.” There is no ecological concern related to the example failure scenario.

Financial Impact of Compromise on Utility: This criterion considers direct financial loss to the utility as a result of the failure scenario, without consideration of the restoration costs as defined below. A scale for costs is used that is relative to the amount of utility revenue. By this definition there is no financial impact of the compromise that happens in the example failure scenario.

Restoration Costs: Restoration costs include the cost to return the system to proper operation, not including any legal or other reparations as a result of the failure. A scale for costs is used that is relative to the total size of the utility operations and maintenance budget. In the example failure scenario, the utility will need to upgrade or replace all defective meters. Conservatively, this is scored as in the range of up to 1% of the operations and maintenance budget.

Negative impact on generation capacity: The scoring for this criterion considers the level of loss of generation capacity, and for how long this loss is sustained. In the example failure scenario, generation capacity is not impacted.

Negative impact on the energy market: Specific impacts identified are price manipulation, lost transactions, or loss of participation by market members (buyers or sellers). Scores 0, 1 and 3 mean respectively either no such impacts, local impacts or widespread occurrence of these impacts. A breakdown in key market functions that creates a non-operational market earns the highest score. The example failure scenario has no impact on the energy market.

Negative impact on the bulk transmission system: The scoring for this criterion uses DOE concepts defined for incident reporting[3]. In particular, a *major transmission system interruption* is defined as follows: “An event has occurred that required action(s) to relieve voltage or loading conditions; or transmission separation or islanding has occurred.” A *complete operational failure or shut-down of the transmission* system is defined as: “An emergency event where an electrically isolated or interconnected electrical system suffers total system collapse that results in the shutdown of the transmission …electrical system….” The example failure scenario has no impact on the bulk transmission system.

Negative impact on customer service: The scores for this criterion consider the delay a customer experiences in gaining resolution of their problem, and for how long this

[3]DOE form OE-417: ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT. http://www.oe.netl.doe.gov/oe417.aspx

condition persists. The example failure scenario could cause disruption to customer service due to increased call volume for more than a week if the meter issue becomes public knowledge. This is judged as closest in impact to the event described by score 3 – up to a 4 hr. delay in customer ability to contact the utility and gain resolution, lasting a week.

Negative impact on billing functions: Billing depends upon accurate power usage data. This criterion measures the number of customers for which the utility may lose the capability to generate accurate bills due to the failure scenario. The scores also consider whether or not the data is recoverable. The example failure scenario does not impact the billing function.

Destroys goodwill toward utility: This criterion measures the extent to which customers and the community look less favorably on the utility as a result of the occurrence of the failure scenario. It is scaled by the resulting level of decrease in interest by customers in participating in advanced programs such as smart meter deployments and demand response. The example failure scenario is likely to generate negative editorials on privacy against the utility and the dangers of the smart grid, resulting in a loss of trust and a drop in customer participation levels in advanced programs. This drop is unlikely to be extreme unless there is specific harm incurred to customers due to the smart meter – which were not assumed for the example. Therefore this criterion is scored a 3.

Immediate economic damage, Long term economic damage: Economic damage means a negative impact on the wealth and resources of a country or region. (This is distinct from a financial impact on an organization or individual.) The scoring for these criteria is based upon how widespread the damage is, and for how long it continues to have impact. The example failure scenario does not cause either immediate or long-term economic damage.

Causes a loss of privacy for a significant number of stakeholders: The scale for this criterion considers the number of customers who may have personal information disclosed due to the failure scenario. Personal information is defined as in Appendix E of the NISTIR 7628. The example failure scenario is given the highest score under this criterion, since patterns of energy usage could be determined from information flowing on the link from each smart meter to the utility, and it is assumed that thousands of customers have this meter.

Table 2 - Impact Criteria with Example Score

Criterion	How to score	Score
System scale	0: single utility customer, 1: neighborhood, 3: town or city, 9: potentially full utility service area and beyond	9
Public safety concern	0: none, 1:10-20 injuries possible, 3: 100 injured possible, 9: one death possible	1
Workforce safety concern	0: none, 3: any possible injury, 9: any possible death	0
Ecological concern	0: none, 1: local ecological damage such as localized fire or spill, repairable, 3: permanent local ecological damage, 9: widespread temporary or permanent damage to one or more ecosystems such as the Exxon Valdez or Chernobyl	0
Financial impact of compromise on utility	0: Petty cash or less, 1: up to 2% of utility revenue, 3: up to 5%, 9: Greater than 5%	0
Restoration costs - cost to return to normal operations, not including any ancillary costs	0: Petty cash or less, 1: < 1% of utility organization O&M budget, 3: <=10%, 9: > 10%	1
Negative impact on generation capacity	0: No effect, 1:Small generation facility off-line or degraded operation of large facility, 3: More than 10% loss of generation capacity for 8 hours or less, 9: More than 10% loss of generation capacity for more than 8 hours	0
Negative impact on the energy market	0: No effect, 1: localized price manipulation, lost transactions, loss of market participation 3: price manipulation, lost transactions, loss of market participation impacting a large metro area, 9: market or key aspects of market non operational	0
Negative impact on the bulk transmission system	0: No, 1: loss of transmission capability to meet peak demand or isolate problem areas, 3: Major transmission system interruption, 9: Complete operational failure or shut-down of the transmission system	0
Negative impact on customer service	0: No, 1: up to 4 hour delay in customer ability to contact utility, and gain resolution, lasting one day, 3: up to 4 hr delay in customer ability to contact utility and gain resolution, lasting a week, 9: more than 4 hr delay in customer ability to contact utility and gain resolution, lasting more than a week	0
Negative impact on billing functions	0: None, 1: isolated recoverable errors in customer bills, 3: widespread but correctible errors in bills, 9: widespread loss of accurate power usage data, unrecoverable	3

Criterion	How to score	Score
Destroys goodwill toward utility	0: No effect, 1: negative publicity but this doesn't cause financial loss to utility, 3: negative publicity causing up to 20% less interest in advanced programs, 9: negative publicity causing more than 20% less interest in advanced programs	3
Immediate economic damage - refers to functioning of society as a whole	0: none, 1: local businesses down for a week, 3: regional infrastructure damage, 9: widespread runs on banks	0
Long term economic damage	0: none, 1: (not used), 3: several year local recession, 9: several year national recession	0
Causes a loss of privacy for a significant number of stakeholders	0: none, 1: 1000 or less individuals, 3: 1000's of individuals, 9: millions of individuals	3
Total - impact		**20**

4.2.2.2 Criteria for Effects on Likelihood and Opportunity

Error! Reference source not found. lists criteria that influence the likelihood and opportunity for a threat agent to exploit a failure scenario. A utility can use these criteria to help assess the probability that a cyber security incident will occur. The criteria do not include specific probabilities, because such a prediction was believed to be speculative as well as dependent upon a number of intangible factors for a specific utility. For example, a terrorist organization would be more interested in attacking a "high profile" organization than one that is relatively unknown outside its customer base.

Initially this list included a criterion that measured how well known the vulnerabilities are, that are exploited in the failure scenario. This criterion was removed since in the Internet age it must be assumed that all vulnerabilities may become well known. "Security by obscurity" is a temporary condition at best.

For these criteria, scores get higher as the "cost" to the threat agent gets lower and therefore as the likelihood and opportunity increases. In prior versions of this document, the reverse was true, for reasons explained in Appendix **Error! Reference source not found.**. Feedback on the ranking method in use led to the approach presented here.

In the following discussion, criteria are defined that influence likelihood and opportunity, and scored as shown in Table 3 for the example failure scenario of a widely deployed smart meter that does not encrypt customer data.

Skill Required: This criterion rates the skill and specialized knowledge that it takes for a threat agent to cause the failure scenario to occur. For the example failure scenario, the score reflects the fact that there are available tools for capturing unencrypted data

on a network, and that there are likely to be available tools for interpreting the data flowing from a particular meter that do not require specialized knowledge to operate.

Accessibility (Physical): This criterion scores the difficulty of obtaining physical access that is required to cause a failure scenario. Accessibility ranges from easy and obvious to obtain for anyone, to not feasible to obtain. In the example failure scenario, physical access to tap into meter connections to the utility is publicly available and their locations are well-known.

Accessibility (Logical): This criterion in similar to the previous one. Logical access refers to any non-physical form of access required to cause a failure scenario, such as network access or a particular utility employee's phone number. The scoring of this criterion assumes that physical access has already been achieved. In the example failure scenario, there is no form of logical access needed, so this criterion is given the highest score.

Attack Vector: This criterion evaluates how easy it is to obtain the technical means to carry out a failure scenario, once physical and logical access have been achieved. The exploit may be simple to carry out with little further effort given physical and logical access. There may be tools available for download from the Internet, or available instructions for the exploit or for similar exploits, or the exploit may be theoretical at this time. For the example failure scenario, tools to sniff an unencrypted link are readily available. It is assumed that tools to interpret the data from a meter are available, though perhaps not as readily. It is also assumed that an exploit using these two tools has not been pre-packaged. However, similar data sniffing attacks on networks are commonplace. Hence this criterion is scored as a 3.

Common vulnerability among others: This criterion acknowledges that a vulnerability shared among many organizations and in many contexts is more likely to be exploited. For the example failure scenario, it is a reasonable assumption that other utilities have deployed the faulty meter, hence the score indicates that more than one utility could be affected.

Table 3 - Criteria for Effects on Likelihood and Opportunity with Example Score

Criterion	How to score	Score
Skill required	0: Deep domain/insider knowledge and ability to build custom attack tools, 1: Domain knowledge and cyber attack techniques, 3: Special insider knowledge needed, 9: Basic domain understanding and computer skills	9
Accessibility (physical)	0: Inaccessible, 1: Guarded, monitored, 3: Fence, standard locks, 9: Publicly accessible	9

Criterion	How to score	Score
Accessibility (logical, assume have physical access)	0: High expertise to gain access, 1: Not readily accessible, 3: Publicly accessible but not common knowledge, 9: Common knowledge or none needed	9
Attack vector (assume have physical and logical access)	0: Theoretical, 1: Similar attack has been described, 3: Similar attack has occurred, 9: Straightforward, for example script or tools available, simple once access is obtained	3
Common vulnerability among others	0: Isolated occurrence 1: More than one utility, 3: Half or more of power infrastructure, 9: Nearly all utilities	1
Total – effects on likelihood and opportunity		**31**

For the example failure scenario here, the results are:

- Impact result, total of all criterion scores: 20
  Effects on Likelihood and Opportunity result, total of all criterion scores: 31

4.3 High Level Ranking Method

The high level ranking method for failure scenarios uses the same concept as the detailed ranking method described above, except that only a total score was specified for the two criteria:

- Impact, considering all types of impacts
- Effects on likelihood and opportunity, considering the likelihood that the threat agent would have both the opportunity and the intent to carry out the failure scenario.

4.4 Use of Detailed Ranking Criteria for Incident Response

The ranking criteria in Section 4.2.2 can be used to assist utilities in rating a failure scenario that occurs – which would be a security incident.

The end result of the process will be to select one of the rating categories in the following table for the incident:

Table 4 - Incident Rating Categories

Category	
High	Requires immediate attention, recommendation to not proceed without mitigation

Category	
Moderate	Requires attention, recommendation to proceed with caution (Limit Exposure) or further mitigate
Low	Requires consideration and prioritization
Negligible	No mitigation required

The following is an example process for incident response.

A utility reviews the ranking criteria to make a qualitative judgment of the impacts relevant to the failure scenario as follows.

1. The utility evaluates the ranking criteria for the failure scenario (incident) and scores each criterion.

2. Based upon these scores, an incident is placed in one of the rating categories in the above table. For example, a utility may decide to count all the scores of 0, 1, 3, and 9 to determine an overall composite rating of a failure scenario. As an example of a counting approach, if more than two impact criteria are 9, or five are 3 or above, then the incident might be judged as high, as defined in Table 4. Another possible rule is that if *any* impact criterion is a 9, the incident must be rated either Moderate or High. Given that the utility is considering an incident that has already occurred, it is unlikely that the criteria concerning effects on likelihood and opportunity will be given weight in the analysis.

Using a simpler counting method rather than the full ranking method described in Section 4.2 has the advantage of speed in determining a response to an incident. This is because it may not be necessary to fill in all scores for an incident to determine that the incident needs immediate attention. For example, if there are more than two impact criteria scored as 9, the rating is High, without scoring all of the criteria.

For the example failure scenario, there is one impact criterion scored as 9.

Table 5 shows the reasoning for a utility's rating for the example failure scenario. This Moderate rating, based on Table 4, means that the failure scenario requires attention but does not indicate the need for a halt to operations related to the affected meters.

Table 5 - Incident Rating for Example Failure Scenario

CONCLUSIONS based on impact criteria			
Negligible **8 scores of 0**	**Low** **2 scores of 1**	**Moderate** **3 scores of 3** 	**High** **1 score of 9**

5
ELECTRIC SECTOR REPRESENTATIVE FAILURE SCENARIOS BY DOMAIN

5.1 Organization and Notation

Included in this section are the failure scenarios. They are organized in the six functional domains:

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

In addition, there are failure scenarios in two additional categories: Generation (GEN) and “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*. More details are provided in Section 6 and Appendix D. 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*. More details are provided in Section 7.1 and Appendix E. Common vulnerabilities and common mitigations are italicized throughout the document.

Additional detail to assist in assessing some broadly stated common vulnerabilities is provided in Appendix F, rather than repeated in every scenario that refers to these vulnerabilities. Vulnerabilities that have supplemental information included in Appendix F are annotated with an asterisk (*) in the failure scenarios.

5.2 Advanced Metering Infrastructure (AMI)

This section presents a set of failure scenarios 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.

Relevant Vulnerabilities:

- *System permits potentially harmful command sequences* such as a sufficiently large number of disconnects that may threaten system balance.

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:

- *Detect anomalous commands* (anomalous disconnect and reconnect commands) not stemming from the normal Customer Information System (CIS) system,
- *Use Role-Based Access Control (RBAC)* to limit who has access to sensitive functions,
- *Validate data* to ensure reasonableness of changes,
- *Generate alarms* for changes to sensitive data,
- *Create audit logs* to track who has made system configuration, software, or database additions or modifications,
- *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.),
- *Limit events* to no more than (n) number of disconnects (using any number of transactions) within a specified time period,
- *Require two-person rule* for greater than (n) number of disconnects within a specified time,

- *Cross check* with the billing system to ensure the customer has the appropriate status before the disconnect command is issued.

AMI.2 Authorized Employee Manipulates MDMS Data to Over/Under Charge

Description: The Meter Data Management System (MDMS) is accessed by an employee (coerced or disgruntled) who selects a few accounts to overcharge or undercharge. This could be done by altering usage or pricing data. It may also be accomplished using malware. When the bills are paid, either the utility receives more or less revenue. An audit uncovering this activity could cause embarrassment or financial burden to the utility.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to Meter Data Management System (MDMS) user billing data,
- *System assumes data inputs and resulting calculations are accurate* for customer energy billing calculations in the Meter Data Management System (MDMS),
- *System permits installation of malware** on the MDMS.

Impact:

- Utility may be liable for mischarging customers,
- Utilities will have to correct billing errors.

Potential Mitigations:

- *Detect unusual patterns* of energy usage (all utilities have some type of revenue protection scheme, but these may not be adequate),
- *Use RBAC* to limit access to sensitive functions,
- *Validate data* to ensure reasonableness for changes,
- *Generate alarms* on changes to sensitive data,
- *Create audit logs* of who has made software or database modifications,
- *Check software execution integrity*, since software may be compromised when loaded for execution,
- *Detect abnormal output* (unexpected data or destinations) in billing and AMI system network traffic,
- *Perform financial audit* to check for unexpected results,

- *Implement configuration* management,
- *Restrict physical access*,
- *Train personnel* regarding need to lock unattended workstations,
- *Detect physical intrusion* with the use of video surveillance,
- *Lock workstations* when workstations are unattended,
- *Check software file integrity* (digital signatures or keyed hashes) to validate software or firmware updates before installation and/or during operation.

AMI.3 Invalid Access Used to Install Malware Enabling Remote Internet Control

Description: A threat agent acquires physical and logical access to the utility enterprise network. The threat agent installs remote accessible malware allowing remote command and control of the AMI system accessible from any available Internet connection. Physical access may be achieved via poor locks, unlocked doors, stolen credentials, or social engineering.

Relevant Vulnerabilities:

- *System permits installation of malware** on the utility enterprise network or AMI implementation,
- *Internet connection may be misused by adversary,** specifically the connection from the Internet to the utility enterprise network or AMI implementation can serve as a command channel for malware on the AMI system,
- *Physical access may be obtained by unauthorized individuals* to the utility enterprise network or AMI implementation,
- *System relies on credentials that are easy to obtain for access* to the utility enterprise network or AMI implementation.

Impact:

- Potential remote command and control capability by a threat agent,
- Depending on the system's architecture and permissions, performance of meter disconnects.

Potential Mitigations:

- *Use RBAC* to limit who has access to the AMI system and the enterprise network,
- *Create audit logs* of who has made software additions or modifications,

- *Generate alerts* when software additions or modifications have been made,
- *Check software execution integrity*, since software may be compromised when loaded for execution,
- *Authenticate users* so that physical access to the system(s) does not automatically grant logical access,
- *Require multi-factor authentication* to gain access to sensitive systems,
- *Isolate networks* serving critical functionality such as control systems from the Internet,
- *Restrict Internet access* to deny controls systems networks access to or from the Internet,
- *Require video surveillance* to document who enters the server room,
- *Check software file integrity* (digital signatures or keyed hashes) to validate software or firmware updates before installation and/or during operation,
- *Restrict physical access* to the utility enterprise network or AMI implementation,
- *Protect credentials* for the enterprise network and/or AMI system,
- *Require strong passwords* for the enterprise network and/or AMI system,
- *Restrict configuration access* to limit who has access and can make configuration changes.

AMI.4 Overused Key Captured on Meter Bus Enables Usage Data Manipulation

Description: Meters are deployed with the same symmetric cryptographic key on all meters in the AMI implementation. A threat agent is able to acquire the secret encryption key after monitoring communications on the internal bus of one of these meters. The secret key is passed in the clear on the bus. Usage data is then manipulated to overstate/understate energy usage or to under/overstate energy production from Distributed Energy Resources (DERs).

Relevant Vulnerabilities:

- *Secret key is stored or transmitted in the clear* while in transit on the internal bus of a meter,
- *Encryption keys are shared* by multiple meters in an AMI implementation.

Impact:

- Continuous loss of revenue due to understated energy usage or overstated energy production,
- The utility may be liable for mischarging customers and may have to correct billing errors. If over-payments were received from customers, restitution would have to be paid to those customers,
- Loss of customer trust in the utility billing (negative publicity).

Potential Mitigations:

- *Require approved cryptographic algorithms* to protect the confidentiality of communications on the internal meter bus and the cryptographic keys,
- *Require approved key management* to protect the cryptographic keys
- *Require unique keys* (symmetric keys) for each deployed meter,
- *Detect unusual patterns* of energy usage on smart meters (all utilities have some type of revenue protection scheme, but these may not be adequate),
- *Perform financial audit* to check for unexpected results.

AMI.5 Mass Meter Rekeying Required when Common Key Compromised

Description: Meters are deployed with the same symmetric cryptographic key on all meters in the AMI implementation. Key compromise occurs in the field due to the ability to extract the secret key when in physical possession of a meter, or during distribution of keys to meters. In this failure scenario, no known financial or energy usage information is actually compromised due to the compromised key, but all the meters still need to be rekeyed to mitigate the potential for future malicious activities.

Relevant Vulnerabilities:

- *Encryption keys are shared* by multiple meters in an AMI implementation,
- *Secret key is stored or transmitted in the clear* on the meter,
- *Secret key is stored or transmitted in the clear* during transit to the meter during key distribution.

Impact:

- Negative publicity,
- Cost of rekeying meters.

Potential Mitigations:

- *Require unique keys* (symmetric key) for each meter,
- *Require approved key management*,
- *Require secure key storage* on meters.

AMI.6 One Compromised Meter in a Mesh Wireless Network Blocks Others

Description: An unauthorized entity installs rogue firmware or software on a single smart meter. This might be via direct access to the meter or via interception/modification of a legitimate meter update. The compromised meter software could report an understatement of usage, or cause sporadic failure of the self-test process to impede discovery. If meters in the system implement a mesh wireless network, the compromised meter might misroute communications from other meters, blocking the path back to the AMI headend for those meters and making those meters effectively "unresponsive."

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* for privileges to install firmware or software on a smart meter,
- *System permits unauthorized installation of software or firmware** on a smart meter.

Impact:

- Continuous loss of revenue for utility if modified software/firmware understates usage (impact scales as more meters are affected),
- Truck rolls needed to investigate compromised meter failure or nonresponsive meters due to misrouting.

Potential Mitigations:

- *Detect unusual patterns* of energy usage on smart meters (all utilities have some type of revenue protection scheme, but these may not be sufficient),
- *Require multi-factor authentication* for firmware or software updates,
- *Use Role-Based Access Control* to limit privileges to install software,
- *Check software file integrity* (digital signatures or keyed hashes) to validate software or firmware updates before installation and/or during operation.

AMI.7 Deployed Meters Containing Undesirable Functionality Need Repair

Description: Undesirable capabilities and features are discovered in smart meters deployed by a utility. This discovery may happen as the result of focused security research or because the utility discovers it has deployed a product containing the same compromised chipset used in a common consumer product.[4] For example, an additional communications channel could be available on the meter, which, if activated, permits offloading of personally identifiable information (PII) or interferes with the functioning of the devices. The compromised smart meters will need to be upgraded or replaced.

Relevant Vulnerabilities:

- *Physical access may be obtained by unauthorized individuals* via the smart meter interfaces which can permit modifying device functionality,
- *Presence of features or functions that may be misused by* users in a manner not intended by the designers of the smart meter.

Impact:

- Cost to upgrade or potentially replace meters,
- If violations of consumer privacy are proven, the utility may be subject to legal actions,
- If meters go “dead” or misstate usage, the utility would lose revenue from impacted customers until the meters are fixed or replaced.

Potential Mitigations:

- *Conduct penetration testing* of devices which includes security analysis of all device interfaces, regardless of their respective impact on meter functionality (such as labeling and internal Joint Test Action Group (JTAG) interfaces),
- *Require secure remote firmware upgrade* on the meter,
- *Require secure boot loader*,
- *Generate alarms* for unusual or unexpected meter operations,
- *Detect abnormal functionality* to identify network ports and services in use and generate alerts,
- *Cross check* network ports and services against intended applications,

[4] http://www.istognosis.com/en/technology-news/79-researchers-hack-toys-attack-iphones-at-toorcon

- *Generate alerts* for unapproved traffic.

AMI.8 False Meter Alarms Overwhelm AMI and Mask Real Alarms

Description: Either due to spoofed tamper alarms or design/implementation problems with the legitimate alarm capability, false meter alarms overwhelm the AMI system and/or cause real meter alarms to be disabled or ignored.

Relevant Vulnerabilities:

- *Alarm management system does not support required processing for legitimate alarm conditions** in the AMI system,
- *Alarm processing capability is overwhelmed by unnecessary alarms* in the alarm management component of the AMI system,
- *Inadequate criteria for determining which alarms deserve priority* in the alarm management component of the AMI system.

Impact:

- Disabling or ignoring of alarms leads to loss of metering tamper awareness and increases the impact of those failure scenarios in which meter tampering occurs.

Potential Mitigations:

- *Prioritize alarms* by type, location, and other criteria so that high-profile alarms can be distinguished and highlighted,
- *Authenticate messages* for receipt of tamper alarms,
- *Encrypt communication paths* for receipt of tamper alarms,
- *Protect against replay* involving receipt of tamper alarms,
- *Cross check* that tamper alarm is for a real meter,
- *Perform hardware acceptance testing* including tamper alarms,
- *Analyze anomalous events* that trigger alarms in order to aggregate alarms for reporting,
- *Cross check* outage alerts with existing technology such as the customer service systems.

AMI.9 Invalid Disconnect Messages to Meters Impact Customers and Utility

Description: A threat agent obtains legitimate credentials to the AMI system via social engineering. The threat agent may already have access to the network on which this system resides or may succeed in reaching the network from another network. The threat agent issues a disconnect command for one or more target meters. Alternatively, a disconnect may be placed in a schedule and then occur automatically at a later time.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* (via social engineering) in the AMI system,
- *Workforce may be unaware of recommended precautions* to prevent social engineering attacks,
- *System relies on credentials that are easy to obtain for access* to a meter disconnect command (single-factor authentication),
- *Network interconnections provide users and hardware/software entities with access unnecessary for their roles* from remote networks to network containing the AMI system.

Impact:

- Customers experience power outages,
- Utility may need to roll a truck to identify the problem,
- Utility loses revenue (scales based on number of meters affected),
- Threat agent may use power outage to mask criminal activity at customer sites.

Potential Mitigations:

- *Detect unusual patterns* of disconnects on smart meters,
- *Re-evaluate scheduled disconnects*,
- *Define policy* for mass meter disconnect,
- *Define procedures* for mass meter disconnect,
- *Require multi-factor authentication* for mass meter disconnect,
- *Train personnel* regarding social engineering techniques,
- *Restrict Internet access* using firewall rules,
- *Require VPNs* for internal connections from the Internet,

- *Detect unauthorized access* in network traffic between Internet and AMI headend,
- *Restrict network access* between Internet and AMI headend,
- *Restrict Internet access* for the AMI headend system,
- *Isolate networks* for the AMI headend system from the Internet,
- *Authenticate devices* connecting to the AMI headend system,
- *Require approved cryptographic algorithms* for the AMI headend system,
- *Enforce least privilege* to the minimum number of systems and/or individuals requiring MDMS access.

AMI.10 Unauthorized Pricing Information Impacts Utility Revenue

Description: The threat agent sends out unauthorized pricing information, such as Time-of-Use (TOU) pricing. This may result in either a loss or increase in utility revenue until the invalid price is recognized. At that point law suits may occur.

Relevant Vulnerabilities:

- *Network interconnections provide users and hardware/software entities with access unnecessary for their roles* at the enterprise boundary,
- *System relies on credentials that are easy to obtain for access* to pricing change functions,
- *System permits unauthorized changes* to accounts required to make TOU pricing changes,
- *Configuration changes are not verified for correctness* in pricing data (e.g., TOU pricing).

Impact:

- Potential for brownout or blackout depending upon the level of response from TOU participants,
- Utility will lose or gain revenue due to invalid prices,
- Lawsuits might be required to resolve the discrepancies.

Potential Mitigations:

- *Validate data* to detect a person overriding the calculated prices or entering inconsistent prices in the price calculation system,
- *Create audit log* when a person overrides the calculated prices or enters inconsistent prices in the price calculation system,
- *Generate alarms* when a person overrides the calculated prices or enters inconsistent prices in the price calculation system,
- *Restrict Internet access* using firewall rules,
- *Require VPNs* for internal connections from the Internet,
- *Detect unauthorized access* between the Internet and AMI,
- *Restrict network access* between the Internet and AMI,
- *Require multi-factor authentication* for price changes,
- *Enforce least privilege* to minimize personnel with access to perform price changes,
- *Protect credentials* permitting price changes, in both user and administrative processes,
- *Require two-person rule* for execution of price changes.

AMI.11 Spoofed Meter "Last Gasp" Messages Cause Fake Outage

Description: A threat agent is able to send many spoofed meter "last gasp" messages to the AMI MDMS, indicating a power outage. As more spoofed messages are sent, the *grid operator tries to reconfigure the grid to compensate, causing utilities to roll trucks to* determine why meters continue to be unresponsive. (Note: This is a special case of failure scenarios AMI.14 and DR.3.)

Relevant Vulnerabilities:

- *System permits messages to be modified by unauthorized individuals* in the path used to receive last gasp messages,
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the path used to receive last gasp messages,
- *A copy of a prior message or command is difficult or infeasible to distinguish from a new legitimate message or command* in the path used to receive last gasp messages.

Impact:

- Cost to roll trucks to investigate fake outages,
- Loss of revenue and creation of a customer service situation,
- Loss of confidence by customers due to visible attempts to repair non-existent problems. This may lead to reduced customer acceptance of advanced programs such as DR,
- Loss of true system state visibility.

Potential Mitigations:

- *Define procedures* to confirm an outage when receiving an AMI last gasp outage message,
- *Continue normal operations* rather than responding to AMI last gasp outage messages,
- *Verify load* at substation and line level to verify reduced demand associated with meters reporting last gasp messages,
- *Authenticate messages* that report last gasp messages from a meter,
- *Encrypt communication paths* for last gasp messages,
- *Confirm action* on receipt of last gasp messages by checking that a last gasp message is from a real meter,
- *Protect against replay* of last gasp messages,
- *Confirm action* after receiving its last gasp message from a meter.

AMI.12 Improper Firewall Configuration Exposes Customer Data

Description: A firewall rule is intentionally or unintentionally created allowing direct access from another network. Taking advantage of this rule, a threat agent subsequently gains access to the database that receives data from the customer accounts database. This enables the threat agent to steal customer personally identifiable information, including electricity usage data.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to the firewall,
- *System relies on credentials that are easy to obtain for access* to the database,
- *Default configuration allows access that is unnecessary after the system is operational.* This allows unnecessary access to the database,

- *Users lack visibility of threat activity* in the AMI system.

Impact:

- Potential for breach of customer privacy and loss of customer confidence.

Potential Mitigations:

- *Detect unauthorized access* between Internet and AMI consumer information,
- *Implement configuration management* to reduce the likelihood that a threat agent can compromise an entire system,
- *Conduct penetration testing* for changes to Internet-facing resources or high value targets,
- *Enforce least privilege* to limit database access to authorized applications and/or locally authenticated users,
- *Protect credentials* for access to the customer information database,
- *Create audit logs* of firewall rule changes and customer database accesses,
- *Detect unusual patterns* of database access,
- *Detect unauthorized configuration changes* to the firewall,
- *Require strong passwords* for access to the customer information database,
- *Require multi-factor authentication* for access to the customer information database.

AMI.13 Authorized User uses Unattended Console to Disconnect Customer

Description: An authorized user gains physical access to the operations room and subsequently an unattended console. The authorized user then disconnects service to a customer's house.

Relevant Vulnerabilities:

- *System permits bypass of access control mechanisms** when the user has physical access to the console,
- *Physical access may be obtained by unauthorized individuals* at an unattended user console,
- *Workforce may be unaware of recommended precautions* when leaving consoles unattended and unlocked.

Impact:

- Unexpected power outage for a single customer.

Potential Mitigations:

- *Restrict physical access* to operations room with sensitive consoles,
- *Train personnel* regarding need to lock unattended consoles,
- *Require video surveillance* for operations rooms containing sensitive user consoles,
- *Lock workstations* when unattended,
- *Confirm action* by requiring approval for some actions in the user interface design,
- *Lock workstation* for inactivity on non-safety-critical consoles,
- *Cross check* physical access identification with system identification to detect failure scenarios such as a threat agent using Person A's badge to access a physical console and subsequently logging into a system using Person B's credentials,
- *Require second-level authentication* to the application interface to initiate customer disconnect.

AMI.14 Breach of Cellular Provider's Network Exposes AMI Access

Description: A cellular phone provider's network is breached, allowing access to a private network leased to a utility for AMI command and control. The AMI implementation is vulnerable to replay attacks and DR messages are replayed to a group of customers. (Note: This is a special case of failure scenario DR.3.)

Relevant Vulnerabilities:

- *Publicly accessible and/or third party controlled links used* (e.g., commercial mobile, utility leased),
- *Cryptography used that employs algorithms that are breakable within a time period useful to the adversary*,
- *A copy of a prior message or command is difficult or infeasible to distinguish from a new legitimate message or command* in the AMI system.

Impact:

- Costs of customer service for complaints and investigations,
- Loss of revenue (if DR messages decrease power draw) or temporary loss of power to more critical uses (if messages increase power draw),
- Cost to re-secure the network.

Potential Mitigations:

- *Isolate networks* using different encryption keys to prevent a breach in one network from affecting another network,
- *Require approved cryptographic algorithms* at the link layer to prevent a threat agent from being able to affect the confidentiality and integrity on the AMI network if a breach should occur,
- *Protect against replay* using time-stamping, or other methods.

AMI.15 Inadequate Security for Backup AMI Enables Malicious Activity

Description: Inadequate security implementation in the AMI monitoring and control backup system allows a threat agent to execute an attack on the AMI implementation during a business continuity or disaster recovery scenario. Access to these backup systems allows a threat agent to perform malicious activity such as mass disconnects of meters, stopping or modifying DR messages, or creating large numbers of problem meter reports.

Relevant Vulnerabilities:

- *Weaker security architecture at backup sites,*
- *Inadequate continuity and recovery security architecture* used in business continuity and disaster recovery planning and procedures.

Impact:

- Power and revenue loss for disconnected customers,
- Outages due to inadequate power available at peak times,
- Cost for rolling trucks to investigate problem meters,
- Additional operational strain on the utility during a business continuity/disaster recovery situation.

Potential Mitigations:

- *Restrict physical access* for backup sites comparable to normal operational sites,

- *Require video surveillance* for backup sites comparable to normal operational sites,
- *Detect physical intrusion* for backup sites comparable to normal operational sites,
- *Emphasize security management* in business continuity and disaster recovery planning, procedures, and execution,
- *Define policy* to include risk and vulnerability assessments in business continuity and disaster recovery testing.

AMI.16 Compromised Headend Allows Impersonation of CA

Description: The private key for the certificate authority (CA) used to set up a Public Key Infrastructure (PKI) at the headend is compromised, which allows a threat agent to impersonate the CA.

Relevant Vulnerabilities:

- *Cryptography used that employs algorithms that are breakable within a time period useful to the adversary* for protection of the private CA key,
- *Security design does not consider the system lifecycle* in the headend.

Impact:

- Costs incurred for rekeying,
- Potential for power overload if the threat agent is able to introduce malicious nodes in the metering system,
- Potential to perform security-relevant tasks such as firmware upgrades, configuration changes, etc. that are initiated from the CA.

Potential Mitigations:

- *Require approved key management* including secure generation, distribution, storage, and update of cryptographic keys.

AMI.17 Malicious Creation of Duplicate APN Prevents Valid AMI Messages

Description: A malicious individual creates a duplicate Access Point Name (APN) for the Group Special Mobile (GSM)-based cellular communications on an AMI network. The meters that are within the range then associate with the fake APN and do not receive messages from the AMI network.

Relevant Vulnerabilities:

- *System permits unauthorized changes* in the routing mechanisms of the cellular network,
- *System relies on credentials that are easy to obtain for access* for reconfiguration of the AMI network.

Impact:

- Denial of Service for cellular-based functions within the AMI network,
- Cost to roll a truck to investigate unresponsive meter and to read meter data,
- Inability for meters to receive DR messages could cause customers to either pay more for power or experience a loss of power,
- If exploited on a large scale, potential outages could occur due to a utility's inability to implement DR.

Potential Mitigations:

- *Verify mode* of GSM-based communications for AMI operate only in 3G mode,
- *Require fail-over* for cellular-based functions fail over to an alternative non-wireless technology such as power line carrier (PLC),
- *Protect credentials* for modifying the configuration of the AMI network,
- *Require strong passwords* for modifying the configuration of the AMI network,
- *Require multi-factor authentication* for modifying the configuration of the AMI network,
- *Detect unusual patterns* of traffic on the AMI cellular network.

AMI.18 Unauthorized Devices Create DoS and Prevent Valid DR Messages

Description: Unauthorized devices gain access to a home area network (HAN). The devices can then be used to create a Denial-of-Service (DoS) condition so that DR messages cannot reach end customer devices. (Note: this is a special case of DR.1.)

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to the HAN,
- *Network interfaces permit unnecessary traffic flows* instead of only flows to the HAN router/gateway/trust center.

Impact:

- Inability to receive DR messages may cause affected customers to either pay more for power or to suffer a loss of usage of a device requiring power,
- Utility will have associated customer service and troubleshooting costs,
- If exploited on a large scale, potential outages could occur due to utility inability to implement DR.

Potential Mitigations:

- *Restrict device access* to the HAN network,
- *Authenticate devices* accessing the HAN network.

AMI.19 Out of Sync Time-stamping Causes Discard of Legitimate Commands

Description: Time-stamping, sometimes used to detect replay attacks, gets out of sync between a meter and its respective AMI headend system, causing the meter to ignore legitimate commands it interprets as a potential replay attack. This causes loss of advanced metering functionality such as two-way communications, remote connect/disconnect, and metrology.

Relevant Vulnerabilities:

- *A copy of a prior message or command is difficult or infeasible to distinguish from a new legitimate message or command* for meter commands from the AMI headend,
- *System permits unauthorized changes* to the time synchronization between meters and the AMI headend,
- *System permits unauthorized changes* to timestamps on meter commands from the AMI headend.

Impact:

- Higher cost, or no cost savings, to read meter data if remote reading fails,
- If exploited on a large scale, outages could occur due to utility inability to implement DR,
- Cost of associated customer service, late invoicing, and troubleshooting efforts.

Potential Mitigations:

- *Require reliable external time source* for the meter's time-stamping functionality,
- *Cross check* periodically, the results of the time synchronization protocol,
- *Check software execution integrity* of the time synchronization protocol, since software may be compromised when loaded for execution,
- *Verify time synchronization* in the time synchronization protocol,
- *Protect against replay* using session tokens.

AMI.20 Independent Energy Generator Causes Lower TOU Pricing

Description: An independent energy generator bribes an AMI operator to lower time-of-use (TOU) pricing to increase demand.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to the TOU pricing implementation.

Impact:

- Utility may lose revenue due to lower prices charged customers at a large volume.

Potential Mitigations:

- *Create audit logs* to record TOU pricing changes,
- *Require two-person rule* for major changes,
- *Implement configuration management* to reduce the likelihood that one person can implement a change that impacts the entire system.

AMI.21 Stolen Field Service Tools Expose AMI Infrastructure

Description: A utility's field service laptop and optical probe are lost or stolen, exposing the software to control components of the AMI infrastructure (e.g., meters and concentrators) to any user.

Relevant Vulnerabilities:

- *Physical access to mobile devices may enable logical access to business functions by unauthorized individuals** to software components of the AMI infrastructure.

Impact:

- Potential for unexpected and perhaps intermittent power loss for a targeted customer or for a large number of customers, and associated revenue loss for a utility,
- Impact may continue even after the laptop is retrieved if a copy of the laptop's OS and/or applications can be exfiltrated or recreated by the threat agent.

Potential Mitigations:

- *Configure for least functionality* on the field service laptop,
- *Encrypt data at rest* on the field service equipment laptop,
- *Track asset* (phone home) for the field service equipment laptop,
- *Require credential revocation* for laptops,
- *Sanitize device* with remote wipe capability for lost field assets.

AMI.22 Wireless Access to AMI Administration Causes Invalid Disconnect

Description: A threat agent gains wireless access to a web-based administration page on an AMI device that controls the ability to disconnect power from the device.

Relevant Vulnerabilities:

- *System permits wireless access by unauthorized parties** to the wireless network used to control an AMI device,
- *System relies on credentials that are easy to obtain for access* to the web-based administration page used to control an AMI device.

Impact:

- Unexpected power loss for the customer.

Potential Mitigations:

- *Require multi-factor authentication* for privileged functionality,
- *Restrict application access* to web-based administration,
- *Require approved cryptographic algorithms* to protect the wireless network.

AMI.23 Meter Authentication Credentials are Compromised and Posted on Internet

Description: A utility deploys all AMI devices with the same authentication credentials granting privileged access via the local infra-red port, and the credentials are compromised and posted on the Internet.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to AMI devices (hardcoded passwords),
- *Shared credentials are used for access* to AMI devices.

Impact:

- Potential for unexpected and perhaps intermittent power loss for a targeted customer or for a large number of customers, and associated revenue loss for a utility.

Potential Mitigations:

- *Require multi-factor authentication* for privileged functionality,
- *Verify absence of hardcoded credentials* on AMI equipment,
- *Require password rule enforcement* including rule that limits sharing of a password by many meters.

AMI.24 Weak Cryptography Exposes AMI Device Communication

Description: An AMI vendor implements weak cryptography that is easy to crack, allowing access to and modification of configuration or data on that interface.

Relevant Vulnerabilities:

- *Cryptography used that employs algorithms that are breakable within a time period useful to the adversary* to control access to configuration or data in AMI implementation.

Impact:

- Cost to upgrade or to replace all devices, if upgrade is not feasible. This impact is expected whether or not a threat agent ever uses this vulnerability to launch an attack,
- Loss of customers' private information, and associated costs,

- Mass disconnect of meters potentially causing circuit breaker trips, resulting in temporary outages until power on the grid can be rebalanced.

Potential Mitigations:

- *Require approved cryptographic algorithms*,
- *Define procedure* in change and configuration management policies and procedures to allow future cryptographic changes,
- *Define procedure* to include security, including cryptography, in the purchasing process,
- *Perform security testing* of security controls during system acceptance testing.

AMI.25 Known but Unpatched Vulnerability Exposes AMI Infrastructure

Description: A threat agent is able to gain access to the AMI system by exploiting a known vulnerability that has not yet been patched. The threat agent is unable to access the AMI applications but can access other AMI devices and the headend system.

Relevant Vulnerabilities:

- *Software patches are not checked regularly to ensure that they are current* in the AMI devices and headend system.

Impact:

- Access to an AMI headend, via an unpatched firewall and operating system for example, could permit a threat agent to shut down the AMI headend,
- Outages caused by an AMI headend shut down due to the utility's inability to implement DR at peak times,
- Customer service and troubleshooting costs.

Potential Mitigations:

- *Maintain patches* including a severity rating (e.g., critical, important, moderate, low) and timeframes for patching vulnerabilities based on severity,
- *Detect unauthorized access* in network traffic to the AMI headend servers,
- *Generate alarms* for unauthorized access to the AMI headend servers,
- *Restrict network access* to the AMI headend servers,

- *Define procedures* for equipment purchase, to ensure timely availability of validated security updates from vendor,
- *Perform security testing* to validate that the system as purchased is current with respect to security updates.

AMI.26 AMI Billing Cards are Compromised Incurring Loss of Revenue

Description: The smart cards or magnetic cards for AMI billing are compromised. Example compromises include tampering with cards to change the credit amount, erasing the logic that decrements the credit amount remaining, or forging cards.

Relevant Vulnerabilities:

- *System assumes data inputs and resulting calculations are accurate* on smartcards inserted into a meter,
- *System permits unauthorized changes* to AMI billing information on smartcards.

Impact:

- Loss of revenue.

Potential Mitigations:

- *Design for security* in the payment system,
- *Check software file integrity* (digital signatures or keyed hashes) to the card contents,
- *Authenticate data source* i.e., smart cards or magnetic cards for AMI billing,
- *Perform security testing* as a part of system acceptance testing.

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.

Relevant Vulnerabilities:

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

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 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,
- *Configure for least functionality* by removing unnecessary interfaces and labeling from production devices.

AMI.28 Failed Patching Causes AMI Devices to Stop Operating

Description: A utility attempts to patch the AMI devices, but fails. Many AMI devices are no longer able to operate due to the failed patching process.

Relevant Vulnerabilities:

- *Software patches may be applied without verifying continued system operation* in the realistic environment of a large footprint operation.

Impact:

- Cost to utility to repair or replace devices,
- Lack of capability to invoice customers, causing temporary financial loss,
- Loss of capability to perform DR, which may cause outages during periods of peak use,
- Cost of handling customer service situation.

Potential Mitigations:

- *Require fail-safe rollback* for the patching process,
- *Test before installation* to troubleshoot problems by testing a (non-production) set of meters prior to applying patches to production units.

AMI.29 Unauthorized Device Acquires HAN Access and Steals Private Information

Description: An unauthorized device gains access to the HAN and uses the web interface to obtain private information. Examples of such information are patterns of energy usage and the presence of medical devices.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to the HAN.

Impact:

- Privacy violations for customers,
- Loss of public confidence in AMI, even if the utility is not held legally responsible for the privacy violations,
- Costs of privacy breach notification if required of the utility.

Potential Mitigations:

- *Require approved cryptographic algorithms* for protection of the HAN,
- *Require multi-factor authentication* for access to the HAN,
- *Minimize private information* in HAN systems and devices.

AMI.30 Threat Agent Performs Unauthorized Firmware Alteration

Description: A threat agent installs rogue firmware on multiple smart meters, bypassing any protection mechanism (e.g., checksums, signatures) and fully controlling smart meter behavior. This might be achieved via direct access to meters, via interception/modification of legitimate meter updates or via access to the headend.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to install firmware on the meter,

- *System permits installation of malware** on a meter.

Impact:

- Continuous loss of revenue for utility if modified firmware understates usage (impact scales as more meters are affected),
- Truck rolls needed to investigate compromised meter failure or nonresponsive meters.

Potential Mitigations:

- *Detect unusual patterns* of energy usage on smart meters (all utilities have some type of revenue protection scheme, but these may not be sufficient),
- *Require multi-factor authentication* for firmware updates,
- *Check software file integrity* (using digital signature or keyed hash) code files to validate firmware updates before installation,
- *Use Role-Based Access Control* to limit privileges to install firmware.

AMI.31 Rogue Firmware Enables Unauthorized Mass Remote Disconnect

Description: A threat agent prepares smart meter firmware containing malware and manually installs it on a target smart meter in each neighborhood. The single insertion point in each neighborhood becomes the bot master for a smart meter based botnet. The bot master acquires the IP address for the neighborhood's headend at the utility and spoofs that address. As other smart meters attempt to connect to the headend, the bot master sends a firmware update command to the smart meters and transmits the malicious firmware to each victim. Individual bots propagate the malicious firmware throughout the neighborhood and use them to achieve a mass remote disconnect scheduled at the same time.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to communicate to the meter with the privileges of the headend, such as updating meter firmware,
- *System permits unauthorized installation of software or firmware** such as the propagation of unauthorized firmware to meters by a compromised headend system.

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:

- *Detect anomalous commands* (disconnect and reconnect commands) on the network not stemming from the normal Customer Information System (CIS) system,
- *Require multi-factor authentication* for firmware updates,
- *Check software file integrity* (digital signature or keyed hash) on code files to validate firmware updates before installation.

AMI.32 Power Stolen by Reconfiguring Meter via Optical Port

Description: Many smart meters provide the capability of re-calibrating the settings via an optical port, which is then misused by economic thieves who offer to alter the meters for a fee, changing the settings for recording power consumption and often cutting utility bills by 50-75%. This requires collusion between a knowledgeable criminal and an electric customer, and will spread because of the ease of intrusion and the economic benefit to both parties.

Relevant Vulnerabilities:

- *Insiders with high potential for criminal or malicious behavior have access to critical functions or sensitive data,* in particular, procedures and equipment for modifying meter configurations,
- *System relies on credentials that are easy to obtain for access* to the meter optical port, which in many cases allows reconfiguration of the meter settings (the optical port password may be found unencrypted on the meter or in field equipment that accesses the meter),
- *System permits unauthorized changes* to the configuration that determines how power consumption is recorded,
- *System relies on credentials that are easy to obtain for access* (via password) to field tool or third party installations of software that can reconfigure meters.

Impact:

- The utility experiences a loss of revenue due to under billing.

Potential Mitigations:

- *Require password rule enforcement* (not the same password for all meters),
- *Detect unusual patterns* of energy usage on smart meters (all utilities have some type of revenue protection scheme, but these may not be sufficient),
- *Detect unauthorized configuration changes* on the meter,
- *Verify personnel* with extensive background checks on utility employees and contract maintenance personnel, especially those that directly interact with field devices,
- *Use Role-Based Access Control* to limit privilege to change meter settings that determine how power consumption is recorded,
- *Protect credentials* to meter optical port, within administrative processes, on meter and in field equipment.

5.3 Distributed Energy Resources (DER)

This section presents a set of failure scenarios 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).[5] 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.

- *Field 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.

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

DER.1Inadequate 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.

Relevant Vulnerabilities:

- *Physical access may be obtained by unauthorized individuals* to DER settings through the DER system user interface,
- *Default password is not changed* for the DER system,
- *System permits unauthorized changes* to anti-islanding protection in the DER system due to poor configuration design,
- *Commands or other messages may be inserted on the network by unauthorized individuals** between the user interface and the DER system, that result in unauthenticated changes to sensitive parameters.

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,
- *Change default access credentials* after installation,
- *Enforce limits in hardware* so that no setting changes can damage equipment,
- *Train personnel* on secure networking requirements so that DER owners will understand the impact of bypassing security settings,
- *Require approval* of next level of management for critical security settings.

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.

Relevant Vulnerabilities:

- *Network is connected to untrusted networks,* specifically the DER operational network is connected to the company's wireless corporate network,
- *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,
- *System permits wireless access by unauthorized parties** to the wireless network in the DER system,
- *Unnecessary access is permitted to system functions* in the DER system,
- *Users lack visibility to the failure of the system to respond to commands* by the utility for the DER system.

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,
- *Authenticate devices* so that any new connections support only authorized equipment,
- *Detect unauthorized configuration changes* to the DER system,

- *Configure for least functionality* by limiting the types of traffic, shutting down certain ports, etc.,
- *Authenticate messages*, including their source and destinations, in communication protocols used between DER system components,
- *Require acknowledgements* in communication protocols used for critical commands from the utility to DER systems,
- *Require failure messages* in communication protocols used for critical commands from the utility to DER systems,
- *Train personnel* (DER system installers) to ensure that the recommended access control security settings are enabled,
- *Require secure factory settings* for configuration and network parameters by default,
- *Authenticate users* who make modifications to secure configuration and network parameters,
- *Require approved cryptographic algorithms* to protect DER wireless network,
- *Use Role-Based Access Control* to limit privileges to safety critical functions,
- *Limit remote modification* of functional and security settings for the DER system.

DER.3 Malware Introduced in DER System During Deployment

Description: A threat agent, possibly a disgruntled employee of the DER vendor or a DER implementation company, makes malicious software changes to equipment software or firmware. This malware causes large numbers of DER systems to ignore certain critical commands from the utility. For example, after some future date, it prevents the DER systems from limiting their energy output when so commanded and then locks out any other commands.

Relevant Vulnerabilities:

- *Insiders with high potential for criminal or malicious behavior have access to critical functions or sensitive data* when granted access to software and firmware in equipment that is at the vendor factory or during implementation,
- *System permits unauthorized installation of software or firmware** in DER equipment,

- *System relies on credentials that are easy to obtain for access* to modify software or firmware on systems post-delivery,
- *System permits unauthorized installation of software or firmware** in the DER system.

Impact:

- Loss of a transformer,
- Financial loss to utility,
- Financial loss to DER owner,
- The combined effect causes a large reverse power flow in a substation and causes severe damage to a substation transformer. All DER software/firmware will have to be updated.

Potential Mitigations:

- *Cross check* software/firmware before installation by comparing with a known good version (a “gold disk”),
- *Require on-going validation* of software/firmware,
- *Authenticate users* for access to modify software/firmware,
- *Verify personnel* with background checks on DER development personnel, implementers, and contract maintenance personnel, especially those that interact directly with the DER interface to the utility,
- *Use Role-Based Access Control* to limit privileges to modify software/firmware after installation,
- *Test for malware* in DER systems.

DER.4 Confidential DER Generation Information Stolen to Harm Customer

Description: A utility is monitoring the energy and ancillary services provided by an industrial or commercial customer’s DER system. The communication protocol that transports this information is intercepted and a threat agent gains access to the private generation data from the DER system because the protocol provides either no confidentiality or inadequate confidentiality. This private data is used to harm the customer.

Relevant Vulnerabilities:

- *System makes messages accessible to unauthorized individuals* in the communication protocol of the DER system,
- *System makes private data accessible to unauthorized individuals* in the communication protocol of the DER system.

Impact:

- Utility is sued for financial damages due to lost customer privacy,
- Utility reputation is damaged for not providing security for private information.

Potential Mitigations:

- *Encrypt communication paths* used for confidential or private information.

DER.5 Trojan Horse Attack Captures Confidential DER Generation Information

Description: A DER system installed for the mutual benefit of a utility partnership with an industrial or commercial customer contains a Trojan horse, either embedded at the factory, added during installation, or inserted by maintenance personnel. The Trojan horse captures confidential market-related information from both the utility and the partner. An industrial competitor uses this market information to the detriment of both the utility and the customer.

Relevant Vulnerabilities:

- *System permits installation of malware** in the supply chain for the DER system.

Impact:

- Utility suffers from financial losses due to market manipulation by the industrial competitor,
- Utility is sued for financial damages due to lost customer confidentiality,
- Utility reputation is damaged for not being able to secure confidential information.

Potential Mitigations:

- *Test before installation* of the DER system, for the presence of malware,
- *Test after installation* of the DER system, for the presence of malware,
- *Require assured maintenance* by security-certified maintenance organizations that can be trusted not to install malware,
- *Test after maintenance* for malware in all DER systems,

- *Create audit log* of all changes to software and firmware, linking the updates to roles,
- *Protect audit logs* from deletion of records unless a security authority is notified,
- *Verify personnel* with background checks on DER development personnel, implementers, and contract maintenance personnel with privileges to modify firmware or software,
- *Use Role-Based Access Control* to limit privileges to modify firmware or software after installation,
- *Restrict access* at factory for modifying software and firmware,
- *Require authentication* to modify firmware or software after installation,
- *Configure for least functionality* by disabling backdoor vendor/maintenance ports.

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.

Relevant Vulnerabilities:

- *System permits potentially harmful command sequences* in the application-to-application messaging scheme of the DER storage system,
- *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.

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,
- *Protect against replay* in communication protocols used to manage DER systems,
- *Create audit log* of out-of-sequence data,
- *Generate alarms* for system owners when out-of-sequence data is detected.

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.

Relevant Vulnerabilities:

- *System permits messages to be modified by unauthorized individuals* in the time synchronization communication protocol,
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the time synchronization communication protocol,
- *System takes action before confirming changes with user* in the DER management system.

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,
- *Check message integrity* in the time synchronization communication protocol,

- *Cross check* operationally critical actions with the utility DER management system before acting.

DER.8 EV Charging Station Ignores Utility Command to Limit Fast-Charging

Description: A charging station employee (with system administrator authority) wants to increase the revenue of an electric vehicle (EV) charging station acting as a DER system. The employee modifies a utility command to “curtail the fast-charging rate” or to change the time-stamp when the fast-charging limit command was received. During a peak period, many EVs simultaneously start charging, causing the distribution transformer to fail.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to instructions received from the utility regarding permitted charging operations.

Impact:

- Transformer is damaged,
- Lawsuits between the utility and the EV charging station over responsibility for the cost to replace the failed transformer.

Potential Mitigations:

- *Require read-only access* to timestamps for stored copies of commands received from utility,
- *Require non-repudiation* for all critical commands between the utility and the customer system.

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.

Relevant Vulnerabilities:

- *System permits messages to be modified by unauthorized individuals,*

- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message*.

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,
- *Validate data* in DER systems messages as reasonable and within the DER intrinsic capabilities,
- *Generate alarms* for messages that fail message authentication,
- *Create audit log* of messages that fail message authentication,
- *Require non-repudiation* to validate receipt of messages.

DER.10 Threat Agent Modifies FDEMS Efficiency Settings

Description: A malicious individual accesses a FDEMS in a small- to medium-sized commercial or industrial site, and modifies the energy output, the volt-var curves, or other DER efficiency settings that were requested by the utility.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to critical settings in FDEMS,
- *Unnecessary network access is permitted* to the FDEMS network,
- *Unnecessary access is permitted to the operating system* hosting the FDEMS applications,
- *Physical access may be obtained by unauthorized individuals* to the FDEMS system,
- *System relies on credentials that are easy to obtain for access* to the FDEMS network,

- *System relies on credentials that are easy to obtain for access* that allows modification of the FDEMS settings.

Impact:

- The utility loses financially due to the need to purchase higher costing energy and/or to operate the power system less efficiently,
- The customer experiences higher costs due to not meeting the utility efficiency requests.

Potential Mitigations:

- *Restrict application access* for all FDEMS user interface interactions,
- *Authenticate users* for all FDEMS user interface interactions,
- *Change default credentials* for FDEMS after installation,
- *Use RBAC* in the FDEMS system,
- *Enforce least privilege* to access the FDEMS operating system and physical host,
- *Enforce restrictive firewall rules* for access to the FDEMS network,
- *Require multi-factor authentication* for users requesting remote access to the FDEMS,
- *Protect credentials* that allow access to the FDEMS network,
- *Protect credentials* for the FDEMS application or operating system that permit access to modify the FDEMS settings,
- *Train personnel*, including the FDEMS owners and administrators, on secure networking requirements.

DER.11 Threat Agent Shuts Down Commercial/Industrial FDEMS

Description: A threat agent gains access to a FDEMS in a small- to medium-sized commercial or industrial site, such as a shopping center, university campus, hospital complex, or manufacturing facility and installs malicious software. At a pre-planned time, the virus planted by the threat agent causes a synchronized shut down of all the DER systems on the site, either causing a complete or partial outage of the facility or forcing the facility to purchase additional power from the grid.

Relevant Vulnerabilities:

- *Unnecessary network access is permitted* to the FDEMS network,

- *Unnecessary access is permitted to the operating system* hosting the FDEMS applications,
- *Physical access may be obtained by unauthorized individuals* to the FDEMS system,
- *System takes action before confirming changes with user* to shutdown DER systems in the FDEMS,
- *System relies on credentials that are easy to obtain for access* to the FDEMS network,
- *System relies on credentials that are easy to obtain for access* that allows modification of the FDEMS software.

Impact:

- Depending upon the size of the facility, this unplanned loss of DER energy could cause power quality problems on the utility grid, including low voltage, harmonics, and a possible temporary feeder outage,
- The utility pays more for energy than necessary,
- The utility experiences loss of reputation,
- The customer experiences higher costs due to not meeting the utility requests.

Potential Mitigations:

- *Enforce least privilege* to access the FDEMS operating system and physical host,
- *Enforce restrictive firewall rules* for access to the FDEMS network,
- *Require multi-factor authentication* for users requesting remote access to the FDEMS,
- *Require application whitelisting* on the FDEMS,
- *Generate alerts* upon shutdown of site DER systems,
- *Protect credentials* that allow access to the FDEMS network,
- *Protect credentials* for the FDEMS operating system that permit access to modify the FDEMS software,
- *Use Role-Based Access Control* to limit the privilege to install software on the FDEMS host,
- *Train personnel*, including FDEMS owners and administrators, on secure networking requirements.

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 cause the substation to have power quality problems, including tripping of the transmission line breaker.

Relevant Vulnerabilities:

- *Unnecessary network access is permitted* for the FDEMS network,
- *Unnecessary access is permitted to the operating system* hosting the FDEMS applications,
- *Physical access may be obtained by unauthorized individuals* to the FDEMS system,
- *System relies on credentials that are easy to obtain for access* to the FDEMS network,
- *System relies on credentials that are easy to obtain for access* that allows modification of the FDEMS settings.

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,
- *Authenticate users* for all FDEMS user interface interactions,
- *Enforce changing default credentials* as a system enforced step during installation,
- *Use RBAC* in the FDEMS system,
- *Enforce least privilege* for access to the FDEMS operating system and physical host,
- *Enforce restrictive firewall rules* for access to the FDEMS network,

- *Protect credentials* that allow access to the FDEMS network,
- *Protect credentials* for the FDEMS application or operating system that permit access to modify the FDEMS settings,
- *Require multi-factor authentication* for users requesting remote access to the FDEMS.

DER.13 Custom Malware Gives Threat Agent Control of FDEMS

Description: A threat agent compromises the operating system/operating environment platform of a FDEMS and installs malware. The malware leverages automated machine-to-machine authentication mechanisms and/or compromises stored cryptographic authentication keys to allow it to impersonate the authorized FDEMS software. This gives the threat agent complete control over all of the FDEMS resources and remote resources controlled or managed by the FDEMS.

Relevant Vulnerabilities:

- *Physical access may be obtained by unauthorized individuals* to embedded equipment in the supply chain, installation organization or maintenance organization,
- *Network interfaces permit unnecessary traffic flows* between the FDEMS and the Internet, allowing for Internet-based malware delivery mechanisms,
- *Software patches are not checked regularly to ensure that they are current* permitting compromise of the FDEMS platform,
- *System relies on credentials that are easy to obtain for access* to install software on the FDEMS platform.

Impact:

- The FDEMS owner may experience loss of revenue as well as possible penalties for not responding as contracted,
- Over a long period while avoiding detection, the threat agent can cause changes to the FDEMS commands to benefit a rival FDEMS installation,
- Other unexpected impacts, since the threat agent has undetected control of the FDEMS.

Potential Mitigations:

- *Require secure boot loader*,

- *Check software execution integrity,* since software may be compromised when loaded for execution,
- *Check software file integrity* for software executables and images,
- *Check OS integrity* (e.g., virtual machine monitoring, rootkit detection, etc.),
- *Protect credentials* required for installing software on the FDEMS platform, in user and administrative processes,
- *Maintain patches* on the FDEMS system,
- *Create audit log* to capture commands.

DER.14 DER Systems Shut Down by Spoofed SCADA Control Commands

Description: A threat agent spoofs DER SCADA control commands to perform emergency shutdowns of a large number of DER systems simultaneously.

Relevant Vulnerabilities:

- *System permits messages to be modified by unauthorized individuals* in the DER SCADA communication protocols,
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the DER SCADA communication protocols,
- *Users lack visibility of threat activity,* specifically messages sent to DER systems but not originated by the SCADA system,
- *Unnecessary access is permitted to system functions* for the DER SCADA system, permitting an adversary to gather information about how to spoof shutdown messages.

Impact:

- Power system instability, including outages and power quality problems,
- Utility legal costs related to DER owner litigation for loss of revenue.

Potential Mitigations:

- *Limit events*, specifically the number of shutdown events of DER systems within a specified time period,
- *Use RBAC* in the DER SCADA,
- *Authenticate data source* for the DER SCADA protocols,

- *Authenticate messages* that convey the DER SCADA control commands,
- *Validate inputs* (as a consistency check) for the DER SCADA control commands,
- *Require intrusion detection and prevention* as part of DER SCADA network management.

DER.15 Threat Agent Spoofs DER Data Monitored by DER SCADA Systems

Description: A threat agent modifies the industrial and the larger commercial DER data being monitored by the utility distribution DER SCADA system in real-time, altering the load value so that it is much higher than the actual value. Although this modification does not affect the monthly revenue metering for these DER systems, it causes the utility to request and pay for additional ancillary services from a neighboring DER storage system.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to load value data in the DER SCADA communication protocols,
- *System assumes data inputs and resulting calculations are accurate* between load value and meter values,
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the DER SCADA communication protocols,
- *Users lack visibility of threat activity,* specifically adversary presence on the network capable of intercepting and modifying messages.

Impact:

- Increased utility costs for unnecessary ancillary services,
- Utility legal costs for finding and litigating the threat agent.

Potential Mitigations:

- *Use RBAC* for the DER SCADA,
- *Authenticate data source* for the DER SCADA protocols,
- *Authenticate messages* that convey the DER SCADA control commands,
- *Require intrusion detection and prevention* as part of DER SCADA network management.

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.

Relevant Vulnerabilities:

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

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,
- *Authenticate messages* communicated in the DER SCADA network,
- *Use RBAC* in the utility's DER SCADA system,
- *Validate inputs* that the DER system receives from the DER SCADA system,
- *Protect credentials* that allow access to the DER SCADA network,
- *Protect credentials* for DER SCADA application and operating system.

DER.17 Utility DERMS Miscalculates DER Energy/Service Requests

Description: A malicious individual modifies the utility DERMS system power flow analysis function (input, output, or power flow configuration) that determines what energy and ancillary services to request from the DER systems. Under these modifications, the results still remain "reasonable," but lead to benefits to some DER systems and to the detriment of others.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to the DERMS system,
- *System assumes data inputs and resulting calculations are accurate* in the software application and configuration data that provides DERMS power flow analysis functionality,
- *System permits unauthorized changes* to the DERMS system power flow analysis function.

Impact:

- Financial gain for certain DER systems at the expense of the utility and/or other DER owners,
- Legal costs for litigation with adversely affected DER owners.

Potential Mitigations:

- *Use RBAC* in the utility's DERMS system to limit those users authorized to change pricing signals,
- *Require multi-factor authentication* for operationally critical modifications,
- *Require intrusion detection and prevention* as part of the DERMS network and system management capabilities,
- *Create audit log* for changes to DERMS power flow analysis configuration data,
- *Generate alerts* if DERMS power flow analysis configuration data or DERMS software is changed, or is changed at an unexpected time or to an unexpected value (based on the logging information).

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).

Relevant Vulnerabilities:

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

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,
- *Require intrusion detection*, as part of DERMS network and system management capabilities,
- *Require multi-factor authentication* for operationally critical functions, such as modifying configuration files,
- *Authenticate messages* for administrative messages received by the utility DERMS,
- *Check message integrity* for administrative messages received by the utility DERMS.

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.

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,
- *Unnecessary access is permitted to system functions* in the DERMS system that modify settings that impact individual DER 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,
- *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,
- *Users lack visibility that unauthorized changes were made* to DERMS functions.

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,
- *Validate inputs* in the DERMS control commands,
- *Authenticate messages* received by the DERMS from FDEMS systems,
- *Check message integrity* for messages received by the DERMS from an FDEMS.

DER.20 Compromised DERMS Weather Data Modifies DER Output Forecasts

Description: A threat agent accesses the DERMS system and modifies the weather data being used to forecast loads and DER generation/storage. Consequently, less than optimal requests are sent to DER systems, causing financial impacts to the utility.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to the DERMS system,
- *System permits messages to be modified by unauthorized individuals* for the DERMS data access from remote locations,
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* for the DERMS data access from remote locations,
- *Users lack visibility that unauthorized changes were made* to DERMS data.

Impact:

- Inefficient or cost-ineffective power system operated by the utility,
- Financial impact to 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 access weather data,
- *Authenticate messages* in the DERMS communication protocols,
- *Check message integrity* for the DERMS control commands,
- *Validate inputs* (for consistency) in the DERMS control commands.

DER.21 DER System Registration Information Stolen from DERMS

Description: A threat agent accesses the DERMS systems and steals the customer DER registration information, using it for industrial espionage or other purposes, causing confidentiality impacts to these utility customers. For example, if stolen, this information could allow other DER owners to manipulate the retail (or wholesale) energy markets, for instance by bidding in prices or energy products that make it less likely the DER system (whose data was stolen) would be willing/able to bid, or if they did bid, making it less cost-effective for them.

Relevant Vulnerabilities:

- *Unnecessary access is permitted to system functions* in the DERMS system,
- *System makes private data accessible to unauthorized individuals* while at rest,
- *System relies on credentials that are easy to obtain for access* to customer DER registration information.

Impacts:

- Breach of utility confidential information,
- Financial losses due to the security breach.

Potential Mitigations:

- *Use RBAC* in the utility's DERMS system,
- *Encrypt data at rest*, specifically DER registration data,
- *Require approved cryptographic algorithms* for encrypting DER registration data,
- *Require intrusion detection and prevention* as part of the DERMS network and system management capabilities,
- *Protect credentials* that permit access to customer DER registration data,
- *Create audit log* that records accesses to the registration data files.

DER.22 DELETED

DER.23 Utility Makes Incorrect Decisions Based on Invalid DER Information

Description: A threat agent obtains control of the DER management system of a Retail Energy Provider (REP) (who might be a department within a utility or could be a Third Party). The REP then provides invalid information to the utility grid operators on the future availability of large amounts of DER energy and ancillary services. This causes the grid operator to make less-than-optimal market decisions on purchasing energy and ancillary services.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to the DER system.

Impact:

- Potential financial losses (or gains) for the customers owning the DER systems,
- Major financial and reputation losses for the REP.

Potential Mitigations:

- *Protect credentials* for modification of planning data to be provided to the utility from the REP,
- *Use Role-Based Access Control* to limit privilege to modify planning data to be provided to the utility from REP,
- *Require strong passwords* for modification of planning data to be provided to utility from the REP,
- *Require multi-factor authentication* for modification of planning data to be provided to utility from the REP,
- *Require non-repudiation* for data communicated to the utility from the REP,
- *Create audit log* of interactions with the DERMS system that would have impact on the data ultimately sent to the utility.

DER.24 Retail Energy Provider Misuses Confidential/Private Information from DERMS

Description: A Retail Energy Provider (REP) that manages a group of DER systems normally receives commands from the DERMS on what energy levels and ancillary services that group of DER systems should provide. A threat agent accesses confidential or private information in the DERMS DER database on customers who own DER systems, and uses that information to “market” to those customers.

Relevant Vulnerabilities:

- *System makes private data accessible to unauthorized individuals* while in storage,
- *System relies on credentials that are easy to obtain for access* to read private DER data, when communicating using the REP to DERMS protocol,
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the DERMS communication protocols used to access REP systems,
- *Unnecessary access is permitted to system functions* in the DERMS.

Impact:

- Utility legal costs related to DER owner litigation for loss of confidential and private information.

Potential Mitigations:

- *Use RBAC* at the REP and in the utility's DERMS system,
- *Authenticate messages* in the DERMS protocols,
- *Create audit log* of all accesses to confidential information in the DERMS system,
- *Isolate functions* for retrieval of DER data required by an REP from the DERMS and for retrieval of private data associated with a DER,
- *Generate alerts* in the case of unauthorized access to confidential information, and send them to the affected parties.

DER.25 Threat Agent Unexpectedly Reduces Retail Energy Provider Output

Description: A threat agent obtains control of the DER management system of a REP (who might be a department within a utility or could be a Third Party). The REP provides information to the utility grid operators that all DER systems will continue to function normally but then the compromised DER management system shuts down large amounts of DER energy and ancillary services.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to the DER management system,
- *System assumes data inputs and resulting calculations are accurate* in the data from the REP.

Impact:

- Potential power outages for the grid operator,
- Potential financial losses for customers owning the DER systems,
- Potential major financial and reputation losses for the REP.

Potential Mitigations:

- *Restrict application access* to the DER management system,
- *Protect credentials* for access to functions that determine the energy to be available from an REP,

- *Require strong passwords* for access to functions that determine the energy to be available from an REP,
- *Require multi-factor authentication* for access to functions that determine the energy to be available from an REP,
- *Cross-check* the DER data provided to the utility with the DER system performance.

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.

Relevant Vulnerabilities:

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

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,
- *Confirm action* to disconnect microgrid with the microgrid operator, if microgrid status indicates that pre-established disconnect conditions have been met.

5.4 Wide Area Monitoring, Protection, and Control (WAMPAC)

This section presents a set of failure scenarios 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." [6] "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.

NOTE: In Table 6, presented are the possible impact of the WAMPAC failure scenarios, 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 6 that is applicable to it.

Table 6 - Impact Examples by System State and Type of WAMPAC Application

		Normal	Alert / Emergency
Monitoring	*Data loss*	• No impact	• 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
	Altere	• Control actions that create undesirable state	• Incorrect actions to be taken

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

		Normal	Alert / Emergency
Local Protection	*Data loss*	• No impact	• Failure in taking action, if no alternative data source is available
	Altered data	• Triggered protection mechanisms when not required • Line trip (which can be recoverable) • Improper synchronous closing, leading to equipment damage	• 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*	• No impact	• 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	• 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*	• Control actions that create undesirable state	• 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	• Taking action when none is necessary, such as opening/closing switches, turning on or shutting down generation • Failure to take action, when needed, leading to voltage or frequency conditions that could have been prevented	• 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.

Relevant Vulnerabilities:

- *Network interfaces permit unnecessary traffic flows* for the network hosting the PTP server,
- *Unnecessary system services are configured to run* on the PTP server,
- *System may become overwhelmed by traffic flooding or malformed traffic* because of deficiencies in the network stack, PTP implementation or required auxiliary services,
- *Unnecessary access is permitted to critical functions* in the PTP service.

Impact:

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

Potential Mitigations:

- *Restrict network service access* to the PTP service,
- *Isolate functions* between the PTP service and the auxiliary services running on the same server (e.g., resource prioritization),
- *Configure for least functionality* the PTP server,
- *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,
- *Require intrusion detection and prevention,*
- *Test before installation* to verify that the IDS/IPS solution does not compromise normal operation of the system,
- *Restrict network access* to the network hosting the PTP server,

- *Restrict access* to the GPS clock (locally or via the network).

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).

Relevant Vulnerabilities:

- *Unnecessary access is permitted to networking components* for WAMPAC networking devices,
- *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),
- *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),
- *System permits networking components to be accessed by unauthorized individuals** (e.g., routers, switches, etc.),
- *Software patches are not checked regularly to ensure that they are current on the network components* (e.g., routers, switches, etc.).

Impact:

- All impacts presented in Table 6, as potentially caused by altered measurements or loss of measurements.

Potential Mitigations:

- *Encrypt link layer* on the WAMPAC network,
- *Encrypt application layer* on the WAMPAC network,
- *Check message integrity* (digital signatures) of commands and data received by the WAMPAC components,
- *Restrict network access* to the WAMPAC network,
- *Detect unauthorized devices* in the WAMPAC network ,
- *Maintain patches* on WAMPAC networking components,

- *Use Role-Based Access Control* to limit privileges to access WAMPAC networking components,
- *Authenticate users* of WAMPAC networking components,
- *Detect unusual patterns* in WAMPAC components traffic communications.

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.

Relevant Vulnerabilities:

- *Network interfaces permit unnecessary traffic flows* to the PDC,
- *Design permits unnecessary privileges** to the PDC,
- *Users lack visibility that unauthorized changes were made* to the PDC configuration,
- *System relies on credentials that are easy to obtain for access* to configuration and programming software on the PDC,
- *Remote access may be obtained by unauthorized individuals** to the PDC.

Impact:

- All impacts presented in Table 6, as potentially caused by loss of measurements.

Potential Mitigations:

- *Require redundancy* in PDCs using vendor diversity,
- *Restrict network service access* at multiple layers to prevent unauthorized individuals from gaining access to the PDC,
- *Restrict remote access* to the PDC,
- *Detect unauthorized connections* captured in the communication patterns to and from the PDC,
- *Enforce restrictive firewall* rules for access to the PDC host network,

- *Require multi-factor authentication* for remote access to PDC configuration functions,
- *Use Role-Based Access Control* to limit privilege to modify the PDC configuration,
- *Require approved cryptographic algorithms* for authentication and message integrity on the WAMPAC network.

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.

Relevant Vulnerabilities:

- *Unnecessary network access is permitted* on the network hosting the authentication database,
- *Credentials are accessible in the clear* while in transit or at rest,
- *System permits bypass of access control mechanisms*,*
- *System permits unauthorized changes* to the PDC/PMU configuration, which may include connection information.

Impact:

- All impacts presented in Table 6, as potentially caused by altered measurements.

Potential Mitigations:

- *Authenticate devices* to the PDC, including coverage of all possible paths for communication, including any "back doors" remaining from development,
- *Restrict network service access to all interfaces on the PDC,*
- *Protect credentials* used to authenticate the PMU to the PDC,
- *Change default credentials*,
- *Encrypt data at rest*, specifically credentials,
- *Encrypt communication paths* used to transmit credentials,

- *Require approved key management,*
- *Restrict remote access* to the network hosting authentication database,
- *Require intrusion detection and prevention* for the network hosting authentication database,
- *Authenticate users* to the network hosting authentication database*,*
- *Detect unauthorized access* to the network hosting authentication database,
- *Protect security configuration* that lists the systems permitted to connect to the PDC.

WAMPAC.5 Improper Phasor Gateway Configuration Obscures Cascading Failures

Description: An authorized or unauthorized insider (e.g., social-engineered by a threat agent or accidentally) is able to gain access and misconfigures a phasor gateway, allowing less synchrophasor measurement data to be shared with other phasor gateways or altering the tagging of PMU ID associated with the shared data. This action results in a delay in other utilities' visibility to a cascading failure across utilities.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to configuration and programming software on the phase gateway,
- *Configuration changes are not verified for correctness,*
- *Remote access may be obtained by unauthorized individuals** to the phasor gateway,
- *Critical components exhibit single point of failure* such as phasor gateways.

Impact:

- All impacts presented in Table 6, as potentially caused by altered data or loss of data, for Special Protection applications.

Potential Mitigations:

- *Require reconfiguration in test mode* for gateways,
- *Require two-person rule* of test results that must be verified and approved by personnel/entities other than those that carried out the reconfiguration,
- *Require redundancy* of phasor gateways (vendor diversity),

- *Require multi-factor authentication* for remote access to phasor gateway configuration functions,
- *Use Role-Based Access Control* to limit privilege to modify the phasor gateway configuration,
- *Detect unauthorized configuration* at the gateway level.

WAMPAC.6 Compromised Communications between PMUs and Control Center

Description: WAMPAC communications are slowed down or stopped by manipulating the communications link between the PMUs and the control center. This might be done by attacking network components such as routers, or gaining access to the network and employing a flooding attack.

Relevant Vulnerabilities:

- *Unnecessary network access is permitted* to network components,
- *Users lack visibility of threat activity,* specifically unexpected access to network components or unusual traffic on the network,
- *System relies on credentials that are easy to obtain for access* to the WAMPAC network.

Impact:

- All impacts presented in Table 6, as potentially caused by loss of measurements.

Potential Mitigations:

- *Detect unauthorized access* in network traffic on the PMU/PDC communication links,
- *Restrict network access* on the PMU/PDC communication links,
- *Restrict network access* through traffic throttling mechanisms such as router access control lists (ACLs) and firewalls,
- *Require redundancy* for the stability analysis using SCADA data (using independent communication networks),
- *Require intrusion detection and prevention*,
- *Test before installation* of an IDS/IPS solution to verify that it does not compromise normal operation of the system.

WAMPAC.7 Compromised WAMPAC Historical Data Impacts Grid Stability

Description: An insider is able to gain unauthorized access to the network to which a WAMPAC historian is connected and to the historian host/database software's credentials, assuming credentials are in place. The insider corrupts or deletes the measurement data from the database.

NOTE: The impact of the failure scenario presented below is assessed under the assumption that WAMPAC is using the long term historical data for forensic analysis and the short term historical data for can be used for damping oscillations (in minutes) or voltage/frequency stability (in seconds).

Relevant Vulnerabilities:

- *Network interfaces permit unnecessary traffic flows* to the historian,
- *Unnecessary network access is permitted* allowing access to the historian,
- *Users lack visibility of unapproved access** on the WAMPAC network,
- *Users lack visibility that unauthorized changes were made* to the WAMPAC historian database,
- *System relies on credentials that are easy to obtain for access* to configuration and programming software on the historian,
- *Remote access may be obtained by unauthorized individuals** to the historian from remote networks.

Impact:

- All impacts presented in Table 6, as potentially caused by loss of data, for Monitoring and Control applications.

Potential Mitigations:

- *Restrict remote access* to the historian,
- *Restrict application access* to prevent unauthorized individuals from gaining access to the historian,
- *Require read-only access* to historian data,
- *Detect unauthorized connections* in communications to and from the historian,
- *Detect abnormal behavior* on the measurement database,
- *Generate alerts* for unexpected activity on the measurement database,

- *Enforce restrictive firewall rules* for access to the historian,
- *Require multi-factor authentication* for remote access to modify data managed by the historian,
- *Use Role-Based Access Control* to limit privilege to modify data managed by the historian,
- *Check message integrity* (use cryptography) on the WAMPAC network.

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.

Relevant Vulnerabilities:

- *System permits unauthorized changes* at the manufacturer,
- *Users lack visibility that unauthorized firmware has been install*ed before running it,
- *System permits unauthorized installation of software or firmware*.*

Impact:

- All impacts presented in Table 6, 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,
- *Check software execution integrity* for the firmware, since software may be compromised when loaded for execution,
- *Require redundancy* in PMUs/PDCs using vendor diversity,
- *Restrict system access* for firmware install/updates.

WAMPAC.9 DELETED

WAMPAC.10 Compromised PMU/PDC/Phasor Gateway Metadata

Description: A threat agent is able to gain unauthorized access to the credentials of the PMU/PDC/Phasor Gateway metadata that describes the data structure, assuming credentials are in place, and corrupts or deletes the associated metadata from the database.

Relevant Vulnerabilities:

- *Users lack visibility of unapproved access** on the WAMPAC backend,
- *Unnecessary network access is permitted* to the WAMPAC backend network hosting the gateway metadata database,
- *System relies on credentials that are easy to obtain for access* to the gateway metadata database.

Impact:

- All impacts presented in Table 6, as potentially caused by altered measurements,
- Significant effort/cost invested in troubleshooting the systems given the inconsistencies in PMU data attribution.

Potential Mitigations:

- *Detect unauthorized configuration* in the configuration databases,
- *Restrict database access* to applications that require access,
- *Require multi-factor authentication* for local administrators that require access,
- *Restrict network access* to the WAMPAC backend network,
- *Encrypt data at rest* for database contents related to the PMU configurations.

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 failure scenario presented below is assessed under the assumption that WAMPAC is used as part of a special protection scheme (SPS).

Relevant Vulnerabilities:

- *Unnecessary network access is permitted* to network components,
- *Users lack visibility of threat activity,* specifically unexpected access to network components or unusual traffic on the network,
- *System relies on credentials that are easy to obtain for access* to the WAMPAC network.

Impact:

- All impacts presented in Table 6, 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,
- *Verify correct operation* by using redundant measurements (redundant PDCs) at each substation end transmitted through an independent communication network to double-check the transmitted measurements,
- *Detect unauthorized access* on the substation communication links,
- *Restrict network access* on the substation communication links,
- *Restrict network access* to throttle network traffic, using solutions such as router access control lists (ACLs) and firewalls,
- *Require intrusion detection and prevention*,
- *Require strong passwords* for access to the WAMPAC network,
- *Require multi-factor authentication* for access to the WAMPAC network,
- *Protect credentials* used to access the WAMPAC network in both user and administrative processes,
- *Test before installation* of an IDS/IPS solution to verify that it does not compromise normal operation of the system.

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.

Relevant Vulnerabilities:

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

Impact:

- All impacts presented in Table 6, 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),
- *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),
- *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.

5.5 Electric Transportation (ET)

This section presents a set of failure scenarios for the Electric Transportation (ET) domain. ET systems are set up to include components starting “from the Electric Vehicle (EV) and the Electric Vehicle Supply Equipment (EVSE) to the EV Management Server that communicates with the EVSEs. The EV may have an in-vehicle system that is connected to the battery through the vehicle’s Car Area Network (CAN) that exchanges data with the EVSE via a wireless channel or PLC. […] ET systems also include other intermediate devices. A meter measures power usage for each EVSE. A gateway collects data from the meters and the EVSEs and transmits the data to the EV Management Server.”[6]

ET.1 Custom Malware causes EV Overcharge and Explosion

Description: A threat agent directly accesses and compromises the Electric Vehicle (EV) firmware or inserts a Trojan horse to always indicate the EV is undercharged. Consequently, the battery becomes overcharged and may eventually explode.

Relevant Vulnerabilities:

- *Design, implementation, or maintenance permits system to enter a hazardous state* by overcharging or draining the battery beyond limits,
- *System permits unauthorized changes* to EV firmware using easily accessible interfaces,
- *System permits unauthorized changes* to EV firmware.

Impact:

- Possible loss of life and property damage,
- A tragic accident can lead to a loss of public confidence.

Potential Mitigations:

- *Protect from overcharge* by using a fail-safe battery hardware, providing a physical prevention of such an attack,
- *Check software execution integrity* in EV firmware, since software may be compromised when loaded for execution,
- *Authenticate users* that modify firmware.

ET.2 Simultaneous Fast Charges cause Transformer Overload

Description: A threat agent is able to compromise a fast-charging station management system. When a large number of electric vehicles are connected to charging stations, the threat agent modifies the charge-staggering algorithm such that fast-charging begins concurrently for all the EVs, thus overloading the distribution transformer, causing a local outage, and preventing the EVs from being charged.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to the fast-charging station management system software and configuration,

- *Design, implementation, or maintenance permits system to enter a hazardous state* by letting circuits become overloaded in the distribution transformer.

Impact:

- Power outage to EVs and the charging station,
- Damage to the distribution transformer.

Potential Mitigations:

- *Authenticate users* for access to configuration and software files for the fast-charging station management system,
- *Check software file integrity* of fast-charging station management software and configuration files,
- *Generate alarms* on changes to settings such as the number of EVs allowed to charge simultaneously in the design of the management,
- *Require circuit breaker* to avoid overloading of distribution transformer.

ET.3 Virus Propagated between EVs and EV Service Equipment (EVSE)

Description: A threat agent such as a disgruntled employee or an employee subjected to social engineering could inject a virus into the computer system of an EV at an EV maintenance center or at a factory. Although not present today, future wireless communication technologies for Vehicle-to-Infrastructure (V2I) could enable a vehicle to establish additional data communications channels through which the virus infects public charging stations. A public charging station may in turn infect other EVs. The virus could harm other key functions for car safety in the EV as well as charging functions in the EV and EVSE (Electric Vehicle Service Equipment).

Relevant Vulnerabilities:

- *System permits installation of malware** in an EV, at the EV factory and maintenance center,
- *System permits installation of malware** in the public charging station system,
- *Critical communication paths are not isolated from communication paths that require fewer protections to operate,** specifically, EV charging and conventional data transmission during charging,
- *System permits installation of malware** in the public charging station system or EV being charged, during charging,

- *Critical functions are not isolated from those that require fewer protections to operate,** specifically car safety functions in the EV are not isolated from the more vulnerable battery related functions.

Impact:

- For affected EVs, range from minor nuisances to major safety problems which could cause loss of life,
- For affected EVSE's, potential for arbitrary malfunctions and revenue loss due to shutting down charging stations for troubleshooting,
- Negative publicity concerning EVs,
- Litigation for owner of charging station.

Potential Mitigations:

- *Implement configuration management* of all code changes for EV software at the factory and maintenance center,
- *Verify personnel* at the factory and maintenance center,
- *Conduct code review* of EV software at the factory and maintenance center,
- *Vulnerability scan before installation* of EV software at the factory and maintenance center,
- *Create audit log* of all code changes to EV software at the factory and maintenance center,
- *Maintain anti-virus* to check the public charging station system for any new, unauthorized software already present or detected in communications with the electric vehicles,
- *Isolate networks* within the vehicle, to separate the charging signals from other signals,
- *Isolate functions,* specifically charging functions from safety-related functions within electric vehicles,
- *Check software execution integrity* of EV software, since software may be compromised when loaded for execution,
- *Detect abnormal functionality* (e.g., brake malfunctioning),
- *Detect unusual patterns* of data transfer during charging,

- *Analyze anomalous events* to determine if any anomalous behavior is caused by malicious code of EVs.

ET.4 EV Charging Locations Disclosed via Utility Database

Description: A threat agent cracks through an enterprise firewall and exploits a weak operating system password. Because of a poor database server security configuration, the threat agent is able to obtain confidential utility records regarding charging locations for specific vehicles from the database.

Relevant Vulnerabilities:

- *Unnecessary access is permitted to the database* in the firewall protecting the EV database server,
- *System relies on credentials that are easy to obtain for access* to the EV database server,
- *Unnecessary access is permitted to the database* in the database server.

Impact:

- Privacy violation for customers,
- Potential cost to the utility because of privacy lawsuits by customers,
- Potential legal action by government or regulatory agencies against the utility if applicable privacy laws are violated,
- Decrease in usage of utility charging stations and public relations issue for the utility.

Potential Mitigations:

- *Detect abnormal behavior* in enterprise perimeter protections,
- *Require password rule enforcement*,
- *Encrypt data at rest* for database contents containing charging locations,
- *Restrict database access* to applications that require them,
- *Restrict database access* to local administrators that use strong authentication.

ET.5 Compromised Protocol Translation Module Enables Control of EVs

Description: A threat agent is able to hack a protocol translation module that translates demand response messages to an electric vehicle, from the Open Automated Demand Response protocol (OpenADR) as used by the utility, to Smart Energy Profile (SEP) 2.0 as used by the vehicle. Consequently, the agent is able to send any desired command to a vehicle or possibly to a large number of vehicles.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to code in the protocol translation module.

Impact:

- Potential for turning charging on or off for a large number of vehicles within a short time period,
- Inconvenience to customers,
- Cost of customer service situations,
- Potential to overpower and damage transformer in a neighborhood.

Potential Mitigations:

- *Restrict occurrence* of charging stations in a neighborhood based upon transformer capabilities,
- *Check software file integrity* of translation modules.

ET.6 EVSE Connects Wirelessly to Wrong Meter and Compromises Billing

Description: Although this is not currently done, an EVSE in the future may connect wirelessly to a meter for identifying the meter to be responsible for the charge. The EVSE attaches to the incorrect meter. This causes the wrong entity to be billed for any vehicle using the misconfigured EVSE.

Relevant Vulnerabilities:

- *Inadequate binding of meter with energy users authorized to charge to that meter,*
- *Users lack visibility that unauthorized changes were made* in the association between an EVSE and its smart meter.

Impact:

- Cost of billing disputes that could be raised by any customer,
- Delay or loss of payment to the utility,
- Likely cost to upgrade or replace the smart meter and/or EVSE.

Potential Mitigations:

- *Authenticate devices* between the EVSE and the smart meter,
- *Require physical connection* specifically a wired connection between the EVSE and smart meter,
- *Prevent modification* of the EVSE so that the definition of an associated meter can only be changed by the customer that owns the meter.

ET.7 Private Information Disclosed in Transit between EV and EVSE

Description: Private information exchanged between an EV and an EVSE is captured by a threat agent. For example, this might be information related to the EV owner's payment method, current location or home location. Such data exchanges are not currently done but are anticipated in the future.

Relevant Vulnerabilities:

- *System makes private data accessible to unauthorized individuals* in the EV/EVSE communications channel.

Impact:

- Loss of customer privacy,
- Decreased acceptance of electric vehicles.

Potential Mitigations:

- *Encrypt communication paths* between an electric vehicle and the EVSE.

ET.8 Customer Misuses their EV Registration ID to Obtain Preferential Rate

Description: In a utility service territory where EVs are given preferential or special rates for electricity, a customer may misuse their EV registration identifier to power other electrical devices from the EVSE, thus getting that preferential rate for non-EV uses. In the case of Society of Automotive Engineers (SAE) J1772, the EV responds to the EVSE by clamping a 12V pulse width modulation (PWM) signal to either 3, 6, or 9

volts, depending on its status. A threat agent could plug a non-EV load into the EVSE and mimic the signal by using off-the-shelf resistors and diodes.

Relevant Vulnerabilities:

- *System permits device identifier to be misused* to charge non-EV items when charging takes place based upon an EV registration identifier.

Impact:

- Loss of revenue to a utility,
- The non-EV load may draw too much current and blow the fuse of the EVSE or trip the local circuit breaker.

Potential Mitigations:

- *Authenticate devices* with charging protocol that uses not easily forgeable data sent by the EV that allows the utility to determine it is an EV. Currently, an EV does not exchange any data with the EVSE during charging. Future EV systems are expected to have additional communications channels for data exchange with the EVSE usable for this purpose,
- *Detect unusual patterns* specifically power usage patterns at preferential rates from units that do not appear to be an EV. Potential monitoring methods could use Revenue Protection schemes that identify charging beyond the charging limit of the EV, or note that the real EV is charging at the same time but at a different location from the fake EV.

ET.9 EV Registration ID Stolen or Purchased to Obtain Preferential Rate

Description: EV registration identities are stolen and used directly by the thief, or bought and sold in the black market so that they can be used to obtain preferential rates. This is of concern to a utility when the ID is used to identify the customer's payment method and/or the ID is used to charge a non-EV.

Relevant Vulnerabilities:

- *System permits device identifier to be misused* to masquerade as valid customer whose EV is being charged when charging takes place based upon the identifier.

Impact:

- Illegitimate charges billed to legitimate owner of the EV registration ID,

- Cost of associated customer service situation for this owner,
- Likely loss of revenue by the utility.

Potential Mitigations:

- *Require PIN* (or verification code) with use of registration identity,
- *Require lockout* for multiple failed retries,
- *Authenticate devices* with charging protocol that authenticates specific vehicles associated with a registration identity. This would require significant administration by the utility,
- *Verify EV owner* association with the EV ID (e.g., user ID or license ID),
- *Create audit log* for all uses of the EV ID,
- *Detect unauthorized use* of the EV ID,
- *Learn from others* such as credit card companies and ATMs when designing processes for EVs: (a) Cancellation of ID and reissuance of a new one, (b) Refunds to customers for fraudulent charges,
- *Isolate functions,* specifically, EV registration identity from payment method.

ET.10 High Priority EV Registration Identity Misused to Obtain Faster Charging

Description: The registration identity of a high priority EV (such as a fire truck, ambulance, or police car) is copied and used by a normal priority vehicle to get high priority (faster) charging at a charging station.

Relevant Vulnerabilities:

- *System permits device identifier to be misused* to masquerade as a high priority EV that is being charged.

Impact:

- Possibility for slower charging of high priority or other normal priority vehicles.

Potential Mitigations:

- *Require PIN* or verification code (VIN number) with use of the EV registration identity,
- *Require lockout* for multiple failed retries,

- *Authenticate devices* with charging protocol that uses not easily forgeable data sent by the EV that allows the utility to determine that a high priority EV is being charged. Such vehicles could have a PKI certificate, for example. This may be feasible for public EVs although difficult for all EVs.

ET.11 All EV Registration IDs Stolen from Utility

Description: A utility has all its EV registration identities stolen and must therefore re-issue new registration identities to all EVs.

Relevant Vulnerabilities:

- *Unnecessary network access is permitted* for utility networks or databases that store or transmit registration identities,
- *Unnecessary access is permitted to the database* that stores registration identities,
- *System makes private data accessible to unauthorized individuals* in the storage of registration identities,
- *System permits device identifier to be misused* to masquerade as a trustworthy transaction. The ID could be misused by another person if the user's identity is not verified at the point of use. It can be misused for another EV if the EV is not authenticated when charging takes place.

Impact:

- Cost of reissuing identities and verifying receipt of new identities so that stolen ones can be cancelled,
- Loss of revenue while any stolen identities remain valid,
- Inconvenience to customers,
- Cost of handling customer service situations.

Potential Mitigations:

- *Require PIN* or verification code with use of registration identity**,**
- *Require lockout* for multiple failed attempts,
- *Require authentication* using a charging protocol that authenticates the specific EV being charged and that the EV is associated with the registration identity,

- *Enforce least privilege* by defining the set of insiders authorized to access registration identities,
- *Create audit log* of the individual viewing registration identities,
- *Restrict remote access* to the database,
- *Restrict file access* to database files from the host operating system,
- *Restrict network access* to the network hosting the database,
- *Encrypt data at rest* for database files containing EV registration identities,
- *Encrypt communication paths* of network traffic containing EV registration identities.

ET.12 Unavailable Communication Blocks Customer Use of EV Preferential Rate

Description: An EV owner belongs to utility A and uses the “utility smart card” to charge his EV at a utility B's charging station. If the two utilities have a business contract so that the owner must receive a special rate, the communications between the two utilities must be protected. A threat agent could compromise the communication paths or involved systems, so that utility B is unable to obtain information from utility A regarding the EV owner's rate. As a result, the customer may not receive the preferential rate.

Relevant Vulnerabilities:

- *Critical components exhibit single point of failure* such as communication paths or databases used to verify registration identities between utilities.

Impact:

- Customer inconvenience,
- Cost of customer service situation handling complaints and coordinating refunds with servicing utility. It is assumed that customers will still be able to charge their EVs by using standard credit cards so they are not denied service.

Potential Mitigations:

- *Require resiliency* in communication paths for verifying registration identities,
- *Learn from others* such as credit card company concepts like using a central verification service that provides redundancy and resiliency,

- *Choose own rate* at individual charging stations, regardless of the customers' utility membership (like existing gas stations).

ET.13 Invalidated EV Registration ID Blocks Customer use of Preferential Rate

Description: A threat agent (possibly a disgruntled employee) accesses the utility's EV registration database and invalidates selected EV registration identities. This would prevent those EVs from charging at the preferential rate if they were allowed to charge.

Relevant Vulnerabilities:

- *Unnecessary network access is permitted* to utility networks or databases that store registration identities,
- *Unnecessary access is permitted to the database* that stores registration identities,
- *Users lack visibility that unauthorized changes were made* via transactions that impact the EV registration ID database.

Impact:

- Serious inconvenience and embarrassment to customers in any situation where credit cards or other billing methods using the regular electricity rate are not available. One example is a visitor to any non-retail location where the party responsible for the electricity account for the facility visited is not expected to pay the visitor’s bills (such as a contractor travelling to a job site or a professor’s visit to a colleague),
- Cost of customer service situations to handle complaints and to coordinate refunds with other utilities. This assumes that in a retail situation the customer will still be able to charge their EV by using standard credit cards so they are not denied service. Also assumed is that when at home, the customer would be billed at the standard rate if their registration identify was invalid.

Potential Mitigations:

- *Create audit log* of administrative activity that invalidates a registration identity using the customary user interface,
- *Generate alarm* for administrative activity that invalidates a registration identity using the customary user interface,

- *Enforce least privilege* for individuals authorized to use this customary user interface,
- *Create audit log* of all methods of access to view the databases,
- *Restrict remote access* to the database,
- *Restrict network access* to the network hosting the EV registration ID database,
- *Restrict file access* to applicable database files via the host operating system.

ET.14 EV Charging Process Slowed by Validation Delay of EV Registration ID

Description: A threat agent (possibly a disgruntled employee who wants to embarrass the utility) modifies the verification software that accesses the utility's EV registration database, and introduces random delays in validating EV identities when the vehicles are trying to charge. This would slow down, but not necessarily prevent charging.

Relevant Vulnerabilities:

System permits unauthorized changes to software.

Impact:

- Inconvenience to customers,
- Cost of handling customer complaints,
- Cost of troubleshooting problem,
- Embarrassment to the utility,
- Creates poor perception of the usability of EVs.

Potential Mitigations:

- *Create audit log* of who has made software additions or modifications,
- *Check software execution integrity* of all live executables, since software may be compromised when loaded for execution,
- *Require redundancy* for ways to verify the EV without directly accessing the EV registration system,
- *Isolate functions* of the vehicle charging process from the validation of EVs (such as a driver pumps gas in a gas station).

ET.15 Malware Causes Discharge of EV to the Grid

Description: A threat agent compromises the Vehicle-to-Grid (V2G) protocol that allows bi-directional flows of electricity. The threat agent may hack a protocol translation module directly or insert malware in the charging station management system. The malware could cause vehicles to discharge partially or completely without the owner's consent.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to code in the charging station management system and protocol translation module,
- *Design, implementation, or maintenance permits system to enter a hazardous state* by overloading of the distribution transformer if many EVs are discharged,
- *System takes action before confirming changes with user* causing EVs to be discharged without owner's consent.

Impact:

- Critical damage to electric vehicles,
- Inconvenience to customers,
- Cost of customer service situations,
- Violation of customer contracts and loss of customer confidence,
- A sudden, large amount of electricity from EVs could damage a transformer in a neighborhood.

Potential Mitigations:

- *Enforce hardware limits* for circuit in EVs that stops discharging below a user-defined threshold,
- *Generate alarms* for utility on detection of abnormal discharging behaviors in the charging station,
- *Require circuit breaker* to avoid reverse-directional overpower to the distribution transformer,
- *Authenticate users* seeking access to software files for charging station management system,
- *Restrict file access* to software files for charging station management system,
- *Confirm action* to discharge the EV with the EV owner,

- *Check software file integrity* of charging station management and protocol translation module software files.

ET.16 An EV is Exploited to Threaten Transformer or Substation

Description: A threat agent exploits an in-vehicle system at an EV to inject malware to an EVSE in a charging station. In the near future, such systems will be connected both to the battery via a vehicle data bus (e.g., CAN bus) and to the EVSE via wireless channels (e.g., ZigBee). Once compromised, an EVSE may infect other EVSEs, creating a botnet. The compromised EVSEs could simultaneously charge or discharge all the plugged EVs, thus overloading the distribution transformer. Alternatively, they may launch an attack directly to a charging station management system or to a distribution operator system that controls the transformer and the substation.

Relevant Vulnerabilities:

- *System permits installation of malware** in the EVSE during charging between the EV and the EVSE (ET.3),
- *System permits installation of malware** due to the malware spreading between EVSEs on the network hosting the EVSEs for the charging station,
- *System permits unauthorized changes* to the in-vehicle system,
- *System permits installation of malware** in public charging station systems,
- *Shared credentials are used for access* to nearby EVSEs,
- *Design, implementation, or maintenance permits system to enter a hazardous state* by allowing overloading of the distribution transformer.

Impact:

- Potential to overpower and damage transformer in a neighborhood,
- Temporarily loss of capability for charging station to service customers,
- Potential damage to electric vehicles,
- Revenue loss of the owner of the charging stations due to their damage,
- Violation of customer contracts and loss of customer confidence.

Potential Mitigations:

- *Restrict application access* to the charging station management system,

- *Check software execution integrity* of the charging station management system , since software may be compromised when loaded for execution,
- *Detect abnormal output* containing messages from EVs (ET.3) and EVSEs,
- *Analyze anomalous events* in EVs to detect malicious code,
- *Maintain patches* in the charging station system,
- *Maintain anti-virus* in the charging station system,
- *Require unique keys* in the EVSE,
- *Detect unusual patterns* of data transfer during charging between the EVSE and the EV,
- *Detect unusual patterns* of data transfer between EVSEs and between the EVSE and the charging station management system,
- *Check software execution integrity* of the in-vehicle system,
- *Require circuit breaker* to avoid overloading the distribution transformer.

5.6 Demand Response (DR)

This section presents a set of failure scenarios 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.”**Error! Bookmark not defined.**

DR.1 Blocked DR Messages Result in Increased Prices or Outages

Description: A threat agent blocks communications between a demand response automation server (DRAS) and a customer system (smart meters or customer devices). This could be accomplished by flooding the communications channel with other messages, or by tampering with the communications channel. These actions could prevent legitimate DR messages from being received and transmitted. This can occur at the wired or the wireless portion of the communications channel.

Relevant Vulnerabilities:

- *Physical access may be obtained by unauthorized individuals* to communications channel components,

- *Unnecessary access is permitted to the communications channel*,
- *Publicly accessible and/or third party controlled links used* in DRAS/customer communication channels,
- *System relies on communications that are easy to jam* in wireless DRAS/customer communications channels,
- *System permits unauthorized changes* to the messaging interface components of the DRAS,
- *System permits unauthorized changes* to the messaging components of the customer systems,
- *Users lack visibility of threat activity* specifically unusual traffic load on the communications channel from the DRAS to customer systems or interactions with channel components not originated by the DRAS.

Impact:

- The effects would be correlated to the extent of blockage:
    - If the blockage is local, the impact may be limited to increased energy charges to consumers,
    - Blockage of DR messages on a larger scale, particularly messages to large industrial customers, may cause outages at a local or regional level if demand is too great and increased energy costs to customers over a larger area,
- In sell-back or brokerage scenarios, the blockage of DR signals may result in increased prices for electricity for the utility company and be instrumented for considerable financial gain for parties selling electricity back to the utility company.

Potential Mitigations:

- *Require safe mode* in the energy management settings if expected DR messages are not received within the appropriate time window,
- *Require acknowledgment* of link status including information on the health of the communications link,
- *Restrict remote access*,
- *Restrict network access,*
- *Require intrusion detection and prevention,* where feasible along the communications channel,

- *Detect unauthorized access*,
- *Restrict physical access* to communications channel components,
- *Authenticate users* seeking access to modify DRAS software,
- *Authenticate users* seeking remote access to modify customer DR software,
- *Require acknowledgment* from devices indicating what commands they received,
- *Use Role-Based Access Control* to limit privilege to modify the DRAS and customer end messaging interface components of the DRAS communication channel,
- *Check software file integrity* for DRAS and customer end messaging interface components of the DRAS communication channel,
- *Require redundancy* for wireless connections as part of the communications strategy for critical DR customers,
- *Detect abnormal output* in the results of DR commands to validate reasonability of load/generation results by non-DRAS (such as e.g., SCADA) systems.

DR.2 Private Information is Publicly Disclosed on DRAS Communications Channel

Description: A threat agent eavesdrops on traffic on the network between a DRAS and a customer system. This could leak private information to the threat agent. This might be the easiest attack that the agent can launch while not being detected by utilities.

Relevant Vulnerabilities:

- *Physical access may be obtained by unauthorized individuals* to communications channel components,
- *Unnecessary access is permitted to the communications channel,*
- *Publicly accessible and/or third party controlled links used* in DRAS/customer communications channels,
- *Encryption keys are shared* by multiple computers on the DRAS network,
- *System makes messages accessible to unauthorized individuals* (easy to tap) in wired/wireless communications channels in the DRAS network,
- *Users lack visibility of threat activity* specifically the presence of unknown entities creating traffic on the DRAS/customer communication channel.

Impact:

- Malicious eavesdropping can reveal private information that may be made public. This violates customer privacy,
- Potential for lawsuits and fines against the utility,
- Loss of public confidence in the utility and the DR program, resulting in resistance to both.

Potential Mitigations:

- *Restrict remote access* to DRAS/customer communications channels,
- *Restrict network access* where feasible along the DRAS/customer communications channel,
- *Require intrusion detection and prevention,* where feasible along the communications channel,
- *Detect unauthorized access*,
- *Restrict physical access* to communications channel components,
- *Require unique keys* per meter for messages being transferred,
- *Require approved cryptographic algorithms* to protect the confidentiality of communications.

DR.3 Messages are Modified or Spoofed on DRAS Communications Channel

Description: A threat agent obtains access to the communications channel between the DRAS and the customer DR system, modifies on-going traffic or communications, inserts false messages, or launches a replay attack. The DRAS and the customer system could receive an unauthorized message or a corrupted message. Such a message may cause unintentional (often unfavorable) behaviors of these systems. (Note: Spoofed last gasp messages as in AMI.11 is an important special case of this failure scenario.)

Relevant Vulnerabilities:

- *System permits messages to be modified by unauthorized individuals* between the DRAS and customer DR component,
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* between the DRAS and customer DR component,

- *Physical access may be obtained by unauthorized individuals* to communications channel components,
- *Unnecessary access is permitted to the communications channel,*
- *Publicly accessible and/or third party controlled links used,*
- *Users lack visibility of threat activity* specifically the presence of unknown entities with access to the DRAS/customer communication channel.

Impact:

- A false message may request the DRAS to reduce power supply or to trigger an inappropriate DR event,
- A false message may deliver information indicating cheaper prices to consumers, which encourages them to increase power consumption during on-peak periods,
- Possible service impacts on various (possibly quite large) scales,
- Potential power loss,
- The utility may have financial impacts.

Potential Mitigations:

- *Check message integrity* (digital signatures or message authentication codes) to verify the authenticity and integrity of DR messages in customer equipment,
- *Authenticate messages* from customer DR systems,
- *Protect against replay* in DR messages using timestamps, sequence numbers, or cryptographic nonces,
- *Validate data* to ensure the DR data is reasonable,
- *Restrict network access* to the network hosting the DRAS system and the network on the customer side and elsewhere along the communications channel,
- *Require intrusion detection and prevention* where feasible along the communications channel,
- *Detect unauthorized access*,
- *Detect unusual patterns* and include a human in the decision loop when unexpected patterns or inputs are recognized on DRA,
- *Restrict physical access* to communications channel components,

- *Detect abnormal output* in the results of DR commands to validate reasonability of load/generation results by non-DRAS systems (such as SCADA).

DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages

Description: A threat agent maliciously modifies the DRAS configuration to send (or not send) DR messages at incorrect times and to incorrect devices. This could deliver a wrong, but seemingly legitimate set of messages to the customer system.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to DRAS configuration,
- *Users lack visibility that unauthorized changes were made* in the DRAS configuration,
- *Unnecessary network access is permitted* to the network on which the DRAS resides,
- *System relies on credentials that are easy to obtain for access* to the DRAS configuration.

Impact:

- A false message may deliver information indicating lower prices to consumers, which encourages them to increase power consumption during on-peak periods,
- Damage to the smart grid infrastructure with possible service impacts from small to large scale,
- Potential power loss,
- The utility may have financial impacts,
- In sell-back or brokerage scenarios, withholding of DR signals at the source DRAS may result in increased prices for electricity to the utility and be instrumented for considerable financial gain for parties selling electricity back to the utility company,
- Loss of public confidence in utility and DR program,
    - The customer, receiving an unintended DR message, may reduce power consumption without seeing any benefit applied in their bill.

Potential Mitigations:

- *Restrict remote access* specifically to only those systems that are allowed remote access to the DRAS systems,
- *Restrict remote access* to DRAS configuration functions,
- *Restrict network access* to the network hosting the DRAS,
- *Use RBAC* to limit access to the DRAS configuration,
- *Require two-person rule* on manual overrides or configuration changes in the DRAS,
- *Generate alerts* on changes to the DRAS configuration,
- *Detect abnormal output* in the results of DR commands to validate reasonability of load/generation results by a non-DRAS (maybe SCADA) system.

DR.5 Non-specific Malware Compromises DRAS or Customer DR System

Description: The DRAS or customer DR system is infected by non-specific common malware. This malware may consume system resources, thus slowing other system processes or may attempt to compromise typical components such as databases. This could cause the DRAS to fail to send DR messages when needed or to disclose customer information in its database. It could cause the customer system not to execute the contractual terms of the DR service although it receives legitimate DR messages.

Relevant Vulnerabilities:

- *Software patches are not checked regularly to ensure that they are current*,
- *The list of signatures used for detection of attacks is no longer current,*
- *Unnecessary system services are configured to run* on un-blocked or unnecessary opened ports,
- *Remote access may be obtained by unauthorized individuals** to the customer system from remote networks,
- *Physical access may be obtained by unauthorized individuals* to the DRAS (e.g., to use a Universal Serial Bus (USB) device).

Impact:

- Unstable power balance at the utility due to failure to communicate or execute reduction of power demand during on-peak periods, possibly resulting in loss of power for some customers,

- Potential revenue loss due to failure to communicate or execute a return to non-peak conditions in which customers may increase usage,
- Capture and exfiltration of sensitive DR information would violate customer privacy,
- Loss of public confidence in the utility and DR program.

Potential Mitigations:

- *Maintain patches* in the DRAS and customer DR systems,
- *Maintain anti-virus* in the DRAS and customer DR systems,
- *Configure for least functionality* by limiting open ports and installed functions in the DRAS and DR customer systems,
- *Restrict physical access* to DRAS or its input interfaces (e.g., Universal Serial Bus (USB), compact disk - read only memory (CD-ROM)),
- *Authenticate users* for remote access to a customer DR system.

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.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to software in the DRAS,
- *Users lack visibility that unauthorized changes were made* to the DRAS software,
- *Unnecessary system services are configured to run* on un-blocked or unnecessary open ports,
- *Unnecessary network access is permitted* to the network on which the DRAS resides.

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,
- *Restrict remote access* to the networks hosting the DRAS systems,
- *Restrict network access* to the networks hosting the DRAS systems,
- *Use RBAC* to limit access to the DRAS software files,
- *Check software file integrity* for the DRAS software,
- *Require application whitelisting* on the DRAS,
- *Configure for least functionality* by making unavailable any unnecessary functions and ports on the DRAS systems.

DR.7 Custom Malware Compromises Customer DR System

Description: A threat agent injects a malware into a customer DR system that runs an OpenADR client program at the gateway of the customer domain. The malware might be controlled remotely by the agent or could directly change the behaviors of the customer DR system without any remote connection. As a consequence, the compromised DR system sends incorrect DR messages back to the DRAS. For instance, it sends a false DR registration message to the DRAS, when registering the customer's capability of energy reduction - the false message informs the DRAS that the customer is able to reduce 500kW, although he cannot. Alternatively, the compromised DR system sends a false DR report message to the DRAS, after the DR event finishes - the false message informs the DRAS that the customer reduced 500kW, although the customer actually reduced 100kW.

Relevant Vulnerabilities:

- *Software patches are not checked regularly to ensure that they are current* resulting in vulnerabilities that support the injection of custom malware,
- *The list of signatures used for detection of attacks is no longer current* resulting in vulnerabilities that support the injection of custom malware,
- *Unnecessary system services are configured to run* on un-blocked or unnecessary open ports,
- *Unnecessary access is permitted to system functions* in the customer DR program,

- *System assumes data inputs and resulting calculations are accurate* in customer energy usage,
- *System permits unauthorized changes* to software in the customer DR system,
- *Users lack visibility that unauthorized changes were made* to the customer DR software.

Impact:

- Incorrect estimation of the total energy reduction before/during/after the DR event period, which can lead to the failure of the DR program,
- Potential power outages for the grid operator,
- The utility may have financial impacts - it computes customer incentives based on customer energy usage information,
- Loss of public confidence in the utility and DR program.

Potential Mitigations:

- *Maintain patches* on the customer DR system,
- *Maintain anti-virus* on the customer DR system,
- *Authenticate users* seeking remote access to a customer DR system,
- *Enforce least privilege* for access to the customer DR program,
- *Restrict remote access* to the customer network,
- *Cross check* customer DR performance with messages received from the customer DR system,
- *Configure for least functionality* by making unavailable any unnecessary functions and ports on the customer DR system,
- *Require message verification* for customer messages.

5.7 Distribution Grid Management (DGM)

This section presents a set of failure scenarios 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.

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,
- *System makes messages accessible to unauthorized individuals* in wireless radio signals.

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 spread-spectrum radios*, with channel-hopping or switch to alternate communication paths. Examples include:
    - Switching from licensed band(s) to unlicensed band(s),
    - Switching from unlicensed band(s) to licensed band(s),
    - Transition from RF to fiber or copper land-lines,
    - Transition from RF to dialup (possibly with degraded performance),
- *Require redundancy* in communications channels when the wireless channel is no longer available,
- *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,
- *Require redundancy* via selected AMI meters or alternative devices that provide redundant monitoring information that is out-of-band of compromised communications.

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.

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,

- *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.

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,
- *Verify personnel* (customers) sharing the network are reputable, security conscious and using network resources appropriately,
- *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,
- *Require redundancy* via selected AMI meters or alternative devices that provide redundant monitoring information that is out-of-band of compromised communications.

DGM.3 Malicious Code Injected into Substation Equipment via Physical Access

Description: A threat agent injects malicious code into substation equipment 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.

Relevant Vulnerabilities:

- *Unnecessary access is permitted to system functions* via engineering and console ports of substation equipment,
- *System permits unauthorized changes* to software and information,
- *Physical access may be obtained by unauthorized individuals,*
- *Enabled but unused ports* (unused engineering and console ports).

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,
- *Check software execution integrity* of software in substation equipment, since software may be compromised when loaded for execution,
- *Configure for least functionality* by disabling unused console and engineering ports on intelligent electronic devices (IEDs),
- *Create audit log* of substation actions,
- *Generate alarms* for any serious anomalies, such as connection changes and device configuration changes in substations,
- *Restrict physical access* to substation using, for example, card swipes, pin codes, etc.,
- *Require video surveillance* of the human interfaces to the DGM equipment,
- *Restrict access* to engineering functions,
- *Maintain latest firmware* for substation equipment,
- *Maintain patches* for substation equipment,
- *Use Role-Based Access Control* to limit privileges for functions using engineering and console ports of substation equipment,
- *Authenticate users* for access to engineering and console ports where feasible,
- *Restrict port access* of device ports on substation equipment.

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.

Relevant Vulnerabilities:

- *Unnecessary access is permitted to the communications channel* for remote substation WAN communications,
- *Software patches are not checked regularly to ensure that they are current*,

  System permits bypass of physical access controls via dialup LSS or wireless access.

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,
- *Create audit log* of substation actions,
- *Generate alarms* for any serious anomalies, such as connection changes and device configuration changes,
- *Maintain patches* for all substation communication equipment,
- *Maintain anti-virus* on substation equipment,
- *Require application whitelisting* on substation equipment,
- *Authenticate users* in the substation network (possibly two factor authentication),
- *Require VPNs* in the substation network.

DGM.5 Remote Access Used to Compromise DMS

Description: A threat agent compromises distribution management system (DMS) functionality through remote access modification of executable programs and libraries, rendering the DMS inoperable.

Relevant Vulnerabilities:

- *System permits unauthorized changes* to software files,
- *Software patches are not checked regularly to ensure that they are current,*
- *Remote access may be obtained by unauthorized individuals** to DMS systems,
- *System relies on credentials that are easy to obtain for access* to systems.

Impact:

- Reduced situational awareness and impaired ability to react to fluctuations in load and apply controlled remedies,
- Possible increase in outage durations,
- Decrease in operational efficiency and increase in utility power losses,
- Decrease in service reliability,
- Decrease in customer satisfaction.

Potential Mitigations:

- *Maintain patches* on DMS systems,
- *Create audit log* of all program changes and updates,
- *Detect abnormal behavior* of voltage on feeders via selected AMI meters or alternative devices that provide redundant information,
- *Check software file integrity* (digital signatures) for driver installation,
- *Require intrusion detection and prevention* on DMS hosts,
- *Implement configuration management* for all software updates including patches and firmware updates,
- *Maintain anti-virus* on DMS hosts,
- *Require application whitelisting on DMS hosts,*
- *Require multi-factor authentication* for remote access,
- *Use Role-Based Access Control* to limit privileges to modify software files,

- *Require backup* of DMS when primary DMS is inoperable.

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.

Relevant Vulnerabilities:

- *System permits messages to be modified by unauthorized individuals* in the communications between field devices and the DMS,
- *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,
- *System makes messages accessible to unauthorized individuals.*

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,
- *Detect unusual patterns* of inputs that could indicate they are not trustworthy, by comparing inputs to each other and previous inputs,
- *Restrict communication access*,
- *Encrypt communication paths*.

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.

Relevant Vulnerabilities:

- *System assumes data inputs and resulting calculations are accurate* for QoS mechanisms that rely on devices to report their own classification,
- *Network interfaces permit unnecessary traffic flows* to communication networks.

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 for trust* by analysis of equipment profiles,
- *Restrict network access* to the control system network,
- *Encrypt communication paths* to prevent spoofing,
- *Authenticate users* to prevent spoofing.

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.

Relevant Vulnerabilities:

- *System permits unauthorized changes* during software/firmware development,
- *System permits unauthorized changes* to software/firmware at suppliers of equipment, maintenance, and transportation,
- *System permits unauthorized changes* to software/firmware by utility employees with access to modify field equipment.

Impact:

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

Potential Mitigations:

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

DGM.9 Weakened Security during Disaster enables DGM Compromise

Description: A threat agent could take advantage of the confusion, lack of security, and hasty reconstitution of the distribution grid after a disaster. For example, a threat agent could delay the recovery effort by leveraging temporary communications with low security to access DMS to switch breakers. Likewise this objective could be achieved by

subverting weak physical security at substations (due to damage or communication outages) to access engineering or console ports or relays to change settings and render them inoperable. Further, the interception of temporary communications with low security might support reconnaissance of high priority vulnerabilities to aid in future attacks.

Relevant Vulnerabilities:

- *Emergency response policy, procedures, or execution intentionally disregards security controls to speed recovery,*
- *Emergency response procedures unintentionally omit security controls* either in the procedures themselves or during their execution

Impact:

- Delay, damage, disruption, or denial of the recovery effort,
- Damage, disruption, or destruction of a system or components long after the disaster recovery,
- Theft of historian, configuration, or customer information that could support future attacks.

Potential Mitigations:

- *Implement configuration management* of the DGM systems before and after disasters,
- *Define policy* for emergency response that ensure security during a recovery effort,
- *Prioritize recovery activities* for physical security including personnel authentication and access control during the recovery effort,
- *Review recovery response* after the disaster to verify repairs, configurations, and changes are correct,
- *Verify correct operation* on the DGM systems before deployment.

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.

Relevant Vulnerabilities:

- *Workforce may be unaware of recommended precautions* to block social engineering attacks, such as impersonating persons of authority, phishing and rogue USB devices,
- *Physical access may be obtained by unauthorized individuals* to DMS,
- *Users and hardware/software entities are given access unnecessary for their roles* to critical DMS functions,
- *Insiders with high potential for criminal or malicious behavior have access to critical functions or sensitive data* in the DMS system.

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,
- *Require synchronous functions* for closing control, surge arrestors, or pre-insertion resistors to minimize capacitor bank switching transients,
- *Restrict physical access* to engineering consoles and HMIs,
- *Enforce least privilege* for access to critical DMS functions,
- *Verify personnel* that have access to critical DMS functions,
- *Require single sign-on* practices.

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 control rooms,

substations, and on pole tops - 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.

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,
- *System relies on credentials that are easy to obtain for access* to company computers,
- *Physical access may be obtained by unauthorized individuals* to proprietary utility documents and information,
- *Configuration changes are not verified for correctness* to prevent and detect human error in data center configuration (e.g., Ethernet cable plugged into wrong port),
- *System permits unauthorized changes* by allowing remote access for vendors to do application maintenance and troubleshooting,
- *System makes messages accessible to unauthorized individuals* in the distribution control communication channel,
- *System design limits opportunity for system recovery using reconfiguration* such as distribution networks that are more radial in nature than meshed, making network reconfiguration to restore power more difficult.

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,
- *Train personnel* to protect company information and documents from unauthorized disclosure,
- *Define policy* on handling sensitive information. This includes substation one-line diagrams, equipment information, communication architectures, protection schemes, load profiles, etc.,
- *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,
- *Create audit log* of all changes in HMI control actions,
- *Generate alerts* for all changes for all changes in HMI control actions,
- *Restrict remote access* of vendor connections (e.g., physically disconnect remote connections when not in use),
- *Encrypt communication paths* for distribution control communications,
- *Require two-person rule* for to verify correct DMS configuration,
- *Implement configuration management* for configuration documents,
- *Confirm action* to modify data center physical configuration,
- *Isolate networks* (distribution control networks) by segmenting the distribution control network itself.

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.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* between the transformer and the substation controller,
- *System makes messages accessible to unauthorized individuals* in the wireless communication channel,
- *Emergency situations may not have the appropriate replacement equipment,* some of which require long lead times for repair or replacement (custom built transformers).

Impact:

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

Potential Mitigations:

- *Authenticate users* of wireless communications,
- *Encrypt communications paths* for wireless communications,
- *Design for trust* by replacing wireless communications with wired ones,
- *Create audit log* of all changes in control functions and set points,
- *Generate alerts* for unusual changes in control functions and set points.

DGM.13 Poor Account Management Compromises DMS and Causes Power Loss

Description: After a maintenance employee retires, computer services personnel forgot to deactivate the employees account on the DMS network. A week later, a threat agent uses the employee's credentials to access the DMS network. The threat agent alters DMS switching schedules so that automated and manual switching actions trip the wrong lines after a fault or before maintenance to cause power interruptions for critical loads, such as hospitals or prisons.

Relevant Vulnerabilities:

- *Workforce not trained in proper procedures* to check for human error in account management,
- *Adherence to policies and procedures degrades over time* introducing human error in account management,

- *Human error in adherence to policies and procedures* to check for human error in account management.

Impact:

- Loss of critical customer power,
- Possible loss of human lives,
- Negative publicity.

Potential Mitigations:

- *Require credential revocation* in a timely manner for passwords of former employees,
- *Perform audit* of live accounts periodically to verify and encourage adherence to procedures,
- *Generate alarms* for loss of power to ensure timely restoration of power.

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.

Relevant Vulnerabilities:

- *Physical access to a serial port may enable logical access by unauthorized entities* to communications at substations,
- *System relies on credentials that are easy to obtain for access* to substation relays and RTU (e.g., no passwords or default passwords),
- *Publicly accessible and/or third party controlled links used*,
- *System makes messages accessible to unauthorized individuals* using public communications channels without encryption.

Impact:

- Loss of customer power,
- Monetary loss,

- Negative publicity.

Potential Mitigations:

- *Authenticate users* of serial communications using strong passwords,
- *Encrypt communication paths* for serial communications using low latency encryption devices,
- *Design for trust* and migrate serial communications to field devices from public phone lines to private communication channels.

DGM.15 Threat Agent Causes Worker Electrocution via Remote Access to Distribution System

Description: A threat agent performs reconnaissance of utility maintenance operations to identify current or scheduled maintenance on distribution lines and equipment performed by utility linemen. The threat agent gains access to selected elements of the utility DMS system - which includes all distribution automation systems and equipment in control rooms, substations, and on pole tops - via remote connections. After gaining the required access, the threat agent energizes distribution lines or equipment that are under maintenance by linemen to elicit injury or death by electrocution. 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.

Relevant Vulnerabilities:

- *Critical operations are not locked out during maintenance* (automation system actions),
- *Physical access to mobile devices may enable logical access to business functions by unauthorized individuals** for linemen and maintenance personnel company laptops used for remote connections,
- *System relies on credentials that are easy to obtain for access* to company computers,
- *Physical access may be obtained by unauthorized individuals* to proprietary utility documents and information,

- *Configuration changes are not verified for correctness* to prevent and detect human error in data center configuration (e.g., Ethernet cable plugged into wrong port),
- *System permits unauthorized changes* by allowing remote access for vendors to do application maintenance and troubleshooting,
- *System makes messages accessible to unauthorized individuals* in distribution control communications,
- *System design limits opportunity for system recovery using reconfiguration* such as distribution networks that are more radial in nature than meshed, making network reconfiguration to restore power more difficult.

Impact:

- Maintenance personnel injury or death,
- Damage to company reputation,
- Financial loss,
- Possible customer and utility equipment damage.

Potential Mitigations:

- *Define procedures* that disallow remote DMS control actions on lines and equipment that are under maintenance,
- *Require strong passwords* with complexity requirements on company devices and systems,
- *Train personnel* (operations and maintenance employees) to protect company information and documents from unauthorized disclosure,
- *Define policy* on handling sensitive information. This includes one-lines, equipment information, communication architectures, protection schemes, load profiles, etc.,
- *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,
- *Create audit log* of all changes in HMI control actions,
- *Generate alerts* for all changes in HMI control actions,

- *Restrict remote access* of vendor connections (e.g., physically disconnect remote connections when not in use),
- *Encrypt communication paths* for distribution control communications,
- *Require two-person rule* to verify DMS configuration,
- *Implement configuration management* of DMS configuration documents,
- *Confirm action* to modify the data center physical configuration,
- *Isolate networks* (distribution control network) by segmenting the distribution control network itself.

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 (**Error! Reference source not ound.**). 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 or the SCADA Front End Processor (FEP) at the headend can be affected by manipulating command and control messages in the direction of the substation or information messages in the direction of the head end. In the case of non-operational data exchanges, IED settings can be potentially manipulated.

Relevant vulnerabilities:

- *Physical access may be obtained by unauthorized individuals* to the utility or Telco/ISP,
- *Unnecessary network access is permitted* allowing access of threat agent to the demarc or within the service providers network CSU/DSU,

- *System relies on credentials that are easy to obtain for access* to substation gateway/RTU or SCADA FEP,
- *Users lack visibility of unapproved access** to the demarc,
- *Commands or other messages may be inserted on the network by unauthorized individuals** in the communication protocol,
- *System makes messages accessible to unauthorized individuals* over the serial link,
- *Message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the communication protocol,
- *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.

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 and the cryptographic keys,
- *Implement approved key management* to protect the cryptographic keys,
- *Detect unusual patterns* of energy usage on Generation Automation (all utilities have some type of revenue protection scheme, but these may not be adequate),
- *Detect unauthorized access* in network traffic between substation and headend,
- *Require authentication* on all data exchanges,
- *Encrypt communication paths* for serial messaging by using bump-in-the-wire solution,

- *Require multi-factor authentication* by Telco/CSP to the device containing CSU/DSU units through service level agreement (SLA),
- *Require tamper detection and response* by Telco/CSP for the Demarc through SLA,
- *Restrict physical access* by implementing personnel security control procedures.

5.8 Generation

Generation applications in the bulk generation domain are the first processes in the delivery of electricity to customers. Electricity generation is the process of creating electricity from other forms of energy, which may include a wide variety of sources, including chemical combustion, flowing water, wind, solar radiation, and geothermal heat. The scenarios that follow are not intended to be comprehensive but provide examples that range from an event that could threaten grid stability to those with localized business impacts illustrating the various types of vulnerabilities germane to power generation.

GEN.1 Threat agent adds spurious trip parameters on remotely located plant support equipment and trips unit offline

Description: A threat agent gains physical access to a river water pump house, connects a laptop to the local controls network, and adds a time-delay trip to the circulating water pumps triggered off of a normal value. This causes loss of cooling water flow resulting in the loss of condenser vacuum tripping the turbine and causing the plant to be tripped off line.

Relevant Vulnerabilities:

- *Physical access may be obtained by unauthorized individuals* as many sites have pump houses well outside of the security perimeter of the plant,
- *System relies on credentials that are easy to obtain for access* to make configuration changes to the equipment controls
- *System permits unauthorized changes* to the configuration,
- *Commands or other messages may be inserted on the network by unauthorized individuals* resulting in unauthenticated changes to sensitive parameters

Impact:

- Inadequate cooling water to the condenser will lead to a loss of vacuum that will trip the turbine,
- Improper cooling water levels could damage the condenser and turbine,
- Lost generation,
- Time and expense to diagnose the problem,
- Plant thermal cycle gives greater opportunity for boiler tube leak.

Potential Mitigations:

- *Restrict physical access* to the pump house using, for example, card swipes, pin codes, etc.,
- *Require video surveillance* of the human interfaces to the pump house equipment,
- *Define procedures* to evaluate the credibility of high intake level readings from a pump house. For a spurious reading, other plant indications related to open loop cooling system would not be consistent,
- *Require periodic physical surveillance* of intake structures and equipment, (new common mitigation),
- *Restrict physical access* by implementing personnel security control procedures,
- *Restrict configuration access* to limit who has access and can make configuration changes,
- *Authenticate users* for all user interface interactions,
- *Authenticate users* so that physical access to the system(s) does not automatically grant logical access,
- *Generate alarms* on remote equipment when there is evidence of tampering of controls and instrumentation.

GEN.2 Fuel handling system inoperable after incorrect programmable logic controller motor start parameters are loaded from corrupted reference configuration

Description: An employee that has access to a laptop with the configuration files for the fuel handling programmable logic controllers makes accidental changes to

parameters that affect the logic for disabling the main conveyor on plugged fuel chutes at a key transfer point. These changes will go unnoticed until the next time the laptop is used to load the configuration into the networked programmable logic controllers. Once the altered parameters are loaded – the conveyor continues to run even when the chute is plugged. This will continue until the control logic can be reconfigured and verified. When the chute is plugged, coal will begin to pile up quickly and spill.

Relevant Vulnerabilities:

- *Configuration changes are not verified for correctness* as an individual user is able to modify the referenced configuration.

Impact:

- Resources required to diagnose and repair the control logic,
- Coal falling from high elevation can damage equipment and endanger personnel,
- If the logic is not repaired in time, the plant's generation would be compromised.

Potential Mitigations:

- *Create audit log* of all changes to programmable logic controllers,
- *Implement configuration management* to reduce the likelihood that a threat agent can compromise an entire system. (Note: Storing the master copy of the programmable logic controller configuration for the system on a laptop allows for untracked changes to the master configuration,
- *Restrict configuration access* to limit who has access and can make configuration changes,
- *Require two-person rule* for configuration changes,
- *Validate data* to ensure correctness of changes,
- *Check software file integrity* (digital signatures or keyed hashes) to validate software or firmware updates before installation and/or during operation.

GEN.3 Threat actor causes chemical spill using vendor remote access

Description: A representative of a vendor contracted to manage inventory and chemistry within the generation plant has remote, logical access through an insecure cellular connection. Remote access grants configuration control to the storage tank level instrumentation signals, day tank levels, and pump settings. A threat agent utilizes the cellular connection to access the system and modify the level indication causing the tanks to be overfilled with hazardous chemicals.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to potentially damaging controls,
- *Users lack visibility of unapproved access* to the configuration controls,
- *Remote access may be obtained by unauthorized individuals,*
- *Users lack visibility that unauthorized changes were made* to the configuration parameters.

Impact:

- Hazardous chemical spills of any size are reportable to environmental authorities,
- Personnel and equipment are endangered by the uncontrolled hazardous chemical release,
- Impact may continue even after the laptop is retrieved if a copy of the laptop's operating system and/or applications can be exfiltrated or recreated by the threat agent.

Potential Mitigations:

- *Generate alerts* when changes are made to the control system,
- *Create audit logs* to track who has made system configuration modifications,
- *Restrict configuration access* to limit who has access and can make configuration changes,
- *Require approval* of all changes through the configuration management process,
- *Require two-person rule* for configuration changes to include a local resource,
- *Design for security* in the generation plant system.

GEN.4 Protective disconnect relays disabled on switchgear damaging generator

Description: A technician installing replacement relays in a switchyard encounters an error on a generator protection relay that has remote access enabled. The technician – unfamiliar with this error - engages a public Internet message board to get diagnostic information for the relay. A threat agent - posing as an expert on the message board – targets the technician with a spear phishing attack to gain credentials necessary for remote access. The threat agent then acquires access to the generator protection relay and changes the configuration causing it to not open when appropriate. The failure of the protective relay to disconnect keeps the generator tied to the grid during a plant shutdown. This “motors” the generator and significantly damages the generator and keeps the plant off-line until the generator can be repaired off-site.

Relevant Vulnerabilities:

- *System relies on credentials that are easy to obtain for access* to the network interface device,
- *System permits potentially harmful command sequences* by allowing for disabling the disconnect capability to be modified remotely,
- *Remote access may be obtained by unauthorized individuals,*
- *Workforce may be unaware of recommended precautions* to block social engineering attacks, such as spear phishing,
- *Workforce not trained in proper procedures* to securing identifying information and avoiding spear phishing techniques.

Impact:

- Damage to the generator,
- Loss of revenue affected generating units until generator can be repaired which is usually performed off-site,
- Depending on generating contracts, cost of replacement power while unit is out.

Potential Mitigations:

- Authenticate users that modify configuration settings,
- Require multi-factor authentication for remote connection to the substation,
- Restrict configuration access to limit who has access and can make configuration changes,
- Train personnel regarding spearphishing,
- Create audit logs of configuration changes.

GEN.5 Main transformer is out-of-service after being damaged through deluge system being remotely activated

Description: A malicious technician within the company contracted to monitor and service the fire protection system on the plants substations installs a leave behind wireless network device during periodic maintenance. Using remote access and control of the system, the technician then alters the system settings, specifically, blocking the logic that generates fire alarms on the fire panel in the Main Control Rooms so no alarms are received in the control room. The technician then provides a false fire detection signal to the system. The fire signal activates the deluge system on the main turbine. This causes damage to the main turbine. The plant trips offline and the main turbine is disabled.

[Note: For systems which only operate during emergencies, but which could damage or incapacitate equipment if caused to operate spuriously, it would seem prudent to periodically verify setpoints and control configurations.]

Relevant Vulnerabilities:

- *Unnecessary access is permitted to critical functions* such as commands to activate the deluge system and to make changes to the alerting logic,
- *System permits unauthorized changes* to the system settings,
- *Configuration changes are not verified for correctness* to prevent and detect unauthorized setting changes.

Impact:

- Units served by the fire protection system will trip offline resulting in associated costs to restart the unit and to purchase replacement power and challenges grid stability at the moment that the plant is taken offline,

- Any unexpected plant trip stresses the major plant components (generator, turbine and boiler) leading to a reduction in the expected life of the components and a greater possibility of damage when the unit restarts,

- Long term down time of plant if damage to transformer is severe because of long lead time of new equipment.

Potential Mitigations:

- *Prevent remote modification* of critical control logic, (new mitigation),
- *Require physical connection* to perform changes to critical control logic and to activate fire protection system,
- *Implement configuration management* (e.g., periodic verification of set points and control logic) to reduce the likelihood that one person can implement changes that impact the system,
- *Restrict configuration access* to limit who has access and can make configuration changes,
- *Detect unauthorized devices* – in this case, rouge wireless devices,
- *Configure for least functionality* by removing unnecessary interfaces from production devices.

GEN.6 Precipitator HMI interface disabled through malware introduced through update

Description: A vendor is onsite and updating an HMI for the precipitator and installs software using a USB drive that is infected with malware. The malware disables the HMI for the precipitator, consequently disabling the local control capabilities for the precipitator. The loss of control can result in an environmental violation and will require the system to be restored. Restoration of the system may require that the precipitator be taken off line.

Relevant Vulnerabilities:

- *Workforce not trained in proper procedures* through allowing a USB drive with malware to be connected to a network resource,
- *System permits installation of malware.*

Impact:

- Cost in diagnosis and system reconfiguration and testing,
- Potential environmental violation,
- Potential for propagation to other systems

Potential Mitigations:

- *Train personnel* regarding use of USB drives and proper anti-malware techniques (e.g., scanning drives, alternate installation protocols, etc.),
- *Require two-person rule* for configuration changes,
- *Test for malware* before updating the software,
- *Create audit logs* of configuration changes.

GEN.7 Hijacked Selective Catalytic Reduction System (SCR) is disabled leading to shutdown of power plant

Description: A vendor technician performs maintenance on the Programmable Logic Controller that controls the Ammonia Distribution system for the Selective Catalytic Reduction System (SCR). The technician installs malware-corrupted firmware – either inadvertently or maliciously - into the programmable logic controller when making the repairs. The malware executes when the unit is at full power and shuts the ammonia injection down. This causes the NOx discharge to continue to trend up above the permitted limit. Operations takes action to reduce power to limit the NOx discharge. A forced derate is put in place, but NOx continues to rise. Finally, the decision is made to remove the unit from service to troubleshoot the problem.

Relevant Vulnerabilities:

- *System permits installation of malware* onto the firmware of the programmable logic controller.

Impact:

- Fines from unexpected emission exceedance leading to violation of environmental license,
- Stricter emissions parameters by environmental regulator,

- Unit derate resulting in loss of revenue until the utility can satisfy regulatory requirements related to incident,
- The abrupt shutdown of the SCR system stresses the components of the system and increases the likelihood of equipment damage.

Potential Mitigations:

- *Test for malware* before maintenance by performing a check on the installation media,
- *Check software file integrity* (using digital signature or keyed hash) to validate firmware updates before installation,
- *Test for malware* after maintenance by scanning any serviced components for malware.

GEN.8 Plant tripped off-line through access gained through improperly configured diagnostic device on vendor maintained equipment

Description: A technician leaves their laptop – previously infected by a virus – connected to the DCS network to run a diagnostic on smart valves. The laptop is connected to both the centralized remote monitoring system and the plant controls system, because the laptop remains connected to the corporate wireless network. The virus propagates to other computers on the system and starts polling networked assets sending commands that cause a flood of traffic in the DCS network and the centralized remote monitoring system. The commands overwhelm the processing ability of the network causing a logical failure and triggering a shutdown of the plant.

Relevant Vulnerabilities:

- *System may become overwhelmed by traffic flooding or malformed traffic* through the DCS network,
- *System permits wireless access by unauthorized parties* to the DCS network,
- *Unnecessary access is permitted to networking components* by putting a diagnostic component on the DCS network with unnecessary visibility to other components,

- *Network interfaces permit unnecessary traffic flows* through the “dual-homed” laptop.

Impact:

- Infected assets will have to be cleaned and verified to be virus-free and – in some cases – reconfigured and verified operational,
- Any unexpected plant trip stresses the major plant components (generator, turbine, and boiler) leading to a reduction in the expected life of the components and a greater possibility of damage when the unit restarts.

Potential Mitigations:

- *Require safe mode* for the DCS in a transient network traffic situation,
- *Detect unusual patterns* as the DCS traffic flows are routine: network components can be configured to not generate rapid and random communications,
- *Train personnel* in proper configuration requirements for assets connected to the DCS system,
- *Authenticate devices* connecting to the DCS network,
- *Enforce least privilege* for access to the DCS.

GEN.9 Failure of continuous emission monitoring systems (CEMS) leads to violation

Description: The Continuous Emissions Monitoring System (CEMS) is configured for a connection to the plant control system and a remote connection to allow remote monitoring by the vendor. A threat agent launches a spearphishing attack that is successful with one connected user. The threat agent uses the acquired credentials to access the CEMS to modify the control signal to provide false information to both the remote monitoring center and the control room. The false control signal shows a lower emission point giving the plant indication to cut back on emissions control. The lower control increases the actual emissions above the allowable rates set in the air permit. The situation persists long enough to lead to a violation of the plant emissions permit.

Relevant Vulnerabilities:

- *Workforce not trained in proper procedures* to securing identifying information and avoiding spear phishing techniques,

- *Workforce may be unaware of recommended precautions* to block social engineering attacks, such as spear phishing,
- *Remote access may be obtained by unauthorized individuals,*
- *System permits unauthorized changes* through remote configuration capabilities.

Impact:

- Unexpected exceedance on the plants environmental emissions leads to violation of environmental license with the regulator and subsequent fines,
- Stricter emissions parameters are specified by the environmental department,
- Bad press for the utility because environmental incidents are public record.

Potential Mitigations:

- *Train personnel* regarding social engineering techniques,
- *Require read-only access* for remote monitoring capabilities,
- *Require two-person rule* for major changes.

GEN.10 Threat agent causes grid instability through control of dedicated data and voice lines between system operating center and plant

Description: Combined voice and data communication lines between the system operating center (also known as “dispatch” or generation controls center) that regulates the plant output are maintained by the phone company. The lines are clearly marked as being dedicated for this purpose to ensure that phone repair technicians take special care around these lines. The utility uses the existing system and does not encrypt the data. A threat agent gains physical access to these lines and connects them to their own networking components to allow for remote access – setting up a man-in-the-middle attack. The threat agent sends erroneous signals to the plant to rapidly cut back on power output during a period of high load on the grid. Insufficient power and high load leads to grid instability.

Relevant Vulnerabilities:

- *Physical access may be obtained by unauthorized individuals* to communications channel components,
- *Unnecessary access is permitted to the communications channel* in that the lines are unnecessarily marked by the phone company,
- *System permits unauthorized changes* to commands,
- *Publicly accessible and/or third party controlled links* used in plant/system operating center communication channels.

Impact:

- The magnitude depends on grid conditions at the time (e.g., brownout, rolling blackout, etc.).

Potential Mitigations:

- *Restrict physical access* to communications channel components,
- *Restrict remote access,*
- *Encrypt communication paths* to prevent man-in-the-middle attacks,
- *Restrict network access,*
- *Require acknowledgment* from devices indicating what commands they received,
- *Require redundancy* in communications methods (e.g., back-up phone lines or cellular for voice communications).

GEN.11 Outage extended due to DCS HMI being disabled from malware exploiting a known, unpatched vulnerability

Description: A stable build of the DCS software was released. Several months later, the Distributed Control System (DCS) software is upgraded during a planned outage as suggested by the vendor. The upgrade process is lengthy and a number of security-related patches for the operating system were available to be installed. The decision is made to install older patches but delay installing the most recent patches to get the

DCS operational and get the plant on-line. During the update process for the older patches, a technician uses an infected USB/laptop device on a computer in the DCS network. The malware exploits a vulnerability that was addressed in a recent patch that was not installed. The malware then spreads to the HMI stations interrupting communications through excessive network traffic impacting the control system processors. This delays the startup until the malware can be removed, the system can be patched, and the DCS reconfigured.

Relevant Vulnerabilities:

- *System permits installation of malware* on the HMI machines,
- *Workforce may be unaware of recommended precautions* regarding USB/laptop usage,
- *System may become overwhelmed by traffic flooding or malformed traffic* because of an exploited vulnerability,
- *Software patches are not checked regularly to ensure that they are current* on the DCS operating system.

Impact:

- Outage extended past the original plan leading to lost generation revenue.

Potential Mitigations:

- *Check software execution integrity,* since software may be compromised when loaded for execution,
- *Train personnel* under a user awareness training program that includes portable media guidelines,
- *Maintain patches* and fully evaluate the risk of delaying patches against the potential impact of the patch,
- *Restrict system access* for firmware install/updates,
- *Detect abnormal output* (unexpected communications).

GEN.12 Chemical inventory process control system not properly patched leading to compromised inventory controls of hazardous chemicals

Description: A threat agent is able to gain access to the corporate chemical inventory process control system by exploiting a known vulnerability that has not yet been patched. Once the threat agent is able to access the chemical inventory process control

system, the threat agent is able to adjust the inventory levels preventing needed chemicals from being ordered.

Relevant Vulnerabilities:

- *Software patches are not checked regularly* to ensure that they are current in the corporate chemical inventory process control system,
- *Unnecessary access is permitted to critical functions.*

Impact:

- Potential impact on production depending on the chemicals that are missing when needed.

Potential Mitigations:

- *Maintain patches* on corporate chemical inventory process control system,
- *Restrict access* to the corporate chemical inventory process control system,
- *Require authentication* to critical data.

GEN.13 Utility competitor gains advantage using Monitoring & Diagnostic (M&D) center to gain sensitive information on upcoming generation availability

Description: An authorized user with the appropriate credentials is bribed or coerced by a threat agent to expose operational data on a dozen generation facilities through the M&D Center. The user collects information on the previous day's operation, critical equipment status, and operational plans – including outage schedule - for the upcoming week. The authorized user sends the data to the threat agent via e-mail. The threat agent then uses the information to inform competitors bidding into the power market.

Relevant Vulnerabilities:

- *Users and hardware/software entities are given access unnecessary for their roles*. The M&D center has access to both plant operational and information informing strategic power market decision which may not be necessary for the core function of the M&D center,
- *Network interfaces permit unnecessary traffic flows* to the Internet.

Impact:

- Utility loss of revenue due to disadvantage in bidding into power markets.

Potential Mitigations:

- *Enforce least privilege* for access to the various databases and plans,
- *Detect abnormal output* (unexpected data or destinations) in operations network traffic.

GEN.14 Generation assets taken off line by disrupted microwave communications

Description: A criminal threat agent is able to gain access to the Microwave Communication used for the long-distance communication among the plant switchyard assets, transformer telemetry, and the system operator constituting a Wide Area Network (WAN) of system interconnects. The threat agent has acquired the equipment needed to receive and transmit microwave communications. By establishing a line-of-sight position with the plant communication tower the agent is able to intercept information from over-the-air communications. These communications include substation telemetry and plant status information and can be used to control system response to interconnects. The threat agent determines the location needed to access the system to monitor critical communications of plant and switchyard status. Though a man-in-the-middle attack, the threat agent is able to send erroneous messages that generate a transformer fault. This, in turn, prompts automatic protective actions to open breakers isolating the main transformer. This disconnects the plant from the grid taking the unit offline and making the generation asset unavailable to the wider system.

Relevant Vulnerabilities:

- *System permits potentially harmful command sequences* to be transmitted by a threat agent,
- *Commands or other messages may be inserted on the network by unauthorized individuals,*
- *Spoofed signal is either difficult or infeasible to distinguish from a legitimate signal.*

Impact:

- Loss of Generation by separating the plant from system,
- System reliability is challenged by the unauthorized disconnection.

Potential Mitigations:

- *Authenticate messages* communicated among assets over the interconnect network,
- *Validate signal* by verifying certain commands (e.g., disconnect) among assets,
- *Define contingency plan* for handling interconnects if the microwave WAN is in operable,
- *Require safe mode* by having standard operating procedures that allow the interconnect protocols to operate in a default state,
- *Encrypt communication paths* to prevent man-in-the-middle attacks,
- *Require redundancy* of communications of interconnect states for assets on the microwave WAN (e.g., rolling over to a system on the companies intranet temporarily, etc.).

GEN.15 Plant tripped off-line through access gained through a compromised vendor remote connection

Description: The threat agent, a disgruntled vendor employee, uses the authorization credentials and verification procedure to a secure remote maintenance solution. The remote access solution involves a vendor-maintained asset on the DCS network that prompts the utility to grant the asset access to the DCS network. In addition to the prompt, the procedure requires a separate call from the vendor to the utility describing the need to remotely connect before the utility will complete the connection. The threat agent claims the need to collect routine system performance information. The utility connects the vendor maintained computer to the DCS network, giving the threat agent access. The payload delivered by the threat agent is a modified system file that starts polling networked assets sending commands that cause a flood of traffic in the DCS network. The commands overwhelm the processing ability of the network causing loss of DCS control of the plant. On loss of plant control the assigned operator initiates an immediate unit trip.

Relevant Vulnerabilities:

- *System may become overwhelmed by traffic flooding or malformed traffic* through the DCS network,
- *Insiders with high potential for criminal or malicious behavior have access to critical functions or sensitive data,*
- *Publicly accessible and/or third-party control links used,*
- *Design permits unnecessary privileges,*

- *Presence of features or functions that may be misused by users,*
- *System permits installation of malware*
- *Users lack visibility of threat activity,* specifically unexpected access to network components or unusual traffic on the network,
- *Users and hardware/software entities are given access unnecessary for their roles* to perform duties that should be separated,
- *Users lack visibility that unauthorized changes were made* to the DCS,
- *System permits unauthorized changes* by allowing remote access for vendors to do monitoring and maintenance.

Impact:

- Affected assets will have to be restored and verified operational,
- Trips result in costs to restart the unit and to purchase replacement power. An unexpected and sudden trips challenge grid stability at the moment that the plant is taken offline,
- Any unexpected plant trip stresses the major plant components (generator, turbine, and boiler) leading to a reduction in the expected life of the components and a greater possibility of damage when the unit restarts.

Potential Mitigations:

- *Train personnel* in proper configuration requirements for assets connected to the DCS system,
- *Enforce least privilege* for access to the DCS by limiting remote administrative access through vendor monitoring employee sessions for cases of configuration and file system changes,
- *Restrict remote access* to not allow direct file transfer as a default privilege,
- *Require second-level authentication* requiring management authorization for configuration changes and file transfers and “escorted remote access” requiring live monitoring of vendor access for potentially damaging actions,
- *Restrict configuration access* to limit who has access and can make configuration changes,
- *Create audit logs* through the ability to record the remote access session,
- *Detect unauthorized configuration changes* to the asset,

- Automated *configuration change detection*,
- *Detect unauthorized access* in network traffic between the vendor and the DCS device,
- *Require intrusion detection,*
- *Detect abnormal behavior* in machines and flag this behavior,
- *Require application whitelisting* on the DCS network.

GEN.16 Black-Start Disruption

Description: The physical attack is preceded by a cyber attack using malware to indicate false current/voltage transformer (CT/VT) readings. The malware's intent in generating these readings is to falsely indicate the existence of 3 phase shorts[7] on one or more transmission facilities. The goal of the cyber attack is to create conditions that lead to unnecessary automated responses by select transmission protection equipment. The desired effect of these responses is to cause protection relays to open and close breakers in a manner that results in grid instability leading to the shutdown of electricity generation serving the grid segment under attack. The physical portion of the attack consists of destroying navigation locks or water level control gates on one or more hydroelectric units designated as "black-start" facilities. Destruction of the locks or gates results in the loss of water containment. While water volumes behind the generating units remain sufficient for black-start power generation, the force of water movement past the damaged locks or gates will hinder repairs. By the time the water levels have receded to a point which allows repair, the levels will likely be too low to support the level of power generation needed to conduct normal black-start operations. The results of the attack may be extended depending upon the time needed to raise the water to a level sufficient for power generation

Relevant Vulnerabilities:

- *System permits installation of malware,*
- *Physical access may be obtained by unauthorized individuals* to control system devices,
- *System permits unauthorized changes* to the configuration.

Impact:

[7] http://www.engineering.schneider-electric.dk/Attachments/ed/guide/protection_guide_mv.pdf, Page 52.

- Affected assets will have to be restored and verified operational,
- Time and expense to diagnose the problem,
- The magnitude depends on grid conditions at the time (e.g., brownout, rolling blackout, etc.).

Potential Mitigations:

- *Test for malware* before updating the software,
- *Restrict physical access*,
- *Detect unauthorized configuration changes.*

5.9 Generic

This section presents a set of failure scenarios which are generic. Particular cases of these generic failure scenarios can be found among the failure scenarios 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 failure **scenarios.**

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.

Relevant Vulnerabilities:

- *Users and hardware/software entities are given access unnecessary for their roles* to perform duties that should be separated,
- *System permits unauthorized changes,*
- *Users lack visibility of unapproved access** when privileges are elevated for access to security-relevant or operationally critical functions,
- *Speed of incident response process is not appropriate for incident*.

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 duty*,
- *Use RBAC* to limit access,
- *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),
- *Define procedures* for processing suspected or confirmed security incidents involving an insider,
- *Define procedures* concerning access to security-relevant and operationally critical functionality.

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.

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,
- *Users lack visibility of unapproved access** to show remote command and control of a business asset has been obtained,
- *Users lack visibility of threat activity* between the business operations network and the Internet to notice when an incident is occurring,
- *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.

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

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.

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.

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 permanently physically disabling unnecessary interfaces with epoxy or other methods, or physically removing them,
- *Configure for least functionality* by using software controls or other non-physical methods to disable unnecessary interfaces on equipment,
- *Verify settings* on equipment before the equipment is installed in the field,

- *Test before installation* of equipment in the field,
- *Vulnerability scan before installation* of equipment in the field,
- *Require periodic walk-downs* of equipment to help ensure there are not any new unauthorized devices connected,
- *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,
- *Train personnel* under a user awareness training program that includes portable media guidelines.

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.

Relevant Vulnerabilities:

- *Sensitive data remains on disposed equipment* and allows a threat agent to acquire and reverse engineer equipment,
- *System permits unauthorized changes* in the supply chain.

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,
- *Define policy* addressing disposal which prevents the acquisition of sensitive parts from excessed or disposed devices,

- *Require approved cryptographic algorithms* to prevent a threat agent from reverse engineering devices which are acquired outside of the legitimate supply chain,
- *Perform audit* of the supply chain periodically, to ensure adequate quality control,
- *Detect abnormal behavior* that may indicate supply chain issues, such as unauthorized communications or behavior by deployed devices in the system network,
- *Test before installation*, to detect unwanted functionality before putting devices into production. The objective is to validate functionality and usability.

6 Common Vulnerability Analysis

In previous working drafts of this document, relevant vulnerabilities identified within each short failure scenario were described inconsistently within and across domains (AMI, DER, etc.). This created a challenge when attempting to analyze and prioritize the vulnerabilities presented in the failure scenarios for the purpose of risk management. Lacking naming conventions, one also could not identify those common vulnerabilities that contributed to many failure scenarios. Section 5 above of this document version presents those vulnerabilities normalized to a common form. This form consists of a common vulnerability (highlighted in *italics* within each vulnerability listed in Section 5) together with a context that further specifies the vulnerability as it applies to the specific scenario. These changes enabled automated analysis of vulnerabilities, in particular counting the frequency of occurrence of vulnerabilities.

The common vulnerability analysis task also incorporated two additional goals:

- Improve the naming of vulnerabilities that had a name of the form "lack of a mitigation," and

- Classify vulnerabilities and examine the frequency of occurrence of vulnerability classes in the failure scenarios.

Regarding the first goal, TWG1 members had observed that many (though not all) vulnerabilities had names that asserted the lack of a mitigation. For example, some original vulnerability names were:

- Inadequate controls on software installation, configuration, and integrity
- Weak or no cryptography on the internal bus
- Inadequate network segmentation and perimeter protection.

The members believed that in many cases, this naming approach did not aid the reader in understanding the vulnerability, that is, why the mitigation was needed. The name for the vulnerability focused on the solution and not on the problem. Revising the vulnerability names would assist readers less familiar with the field of cyber security. Further, the original naming approach made the process of identifying related mitigations seem "too easy," since to repair the lack of a mitigation, one simply implements the mitigation stated as lacking in the description of the vulnerability. It was believed that this structure did not provide sufficient information to the reader. This approach obscured the key point that there might be other mitigations available for

solving the problem. Hence it was taken as a goal to eliminate vulnerability names that named mitigations, and replace them by a name for the underlying problem.

The process for common vulnerability analysis identified 82 common vulnerabilities. These were grouped under the vulnerability classes from NISTIR 7628 Volume 3. Appendix D presents the list of common vulnerabilities and this grouping. The mapping from original vulnerability names to their new form is described in the separate document "Electric Sector Failure Scenarios Common Vulnerabilities and Mitigations Mapping."

6.1 Process

Initially, all vulnerabilities were studied and an initial set of common vulnerabilities created. These vulnerabilities were placed into NISTIR 7628 classes.

The team reviewed the overall common vulnerability draft list and categorization and discussed changes to meet the goals of the project. During this review, there was a concern that some of the new vulnerability names appeared too general, such as *design permits unnecessary access* or *access controls can be bypassed*. It was recognized that these vulnerabilities had important special cases. However, the important sub cases do not fully characterize the vulnerability, so the general name is more accurate. Further, it would be repetitive to list these sub cases in every scenario. Hence this information was developed and is presented separately in Appendix F.

After this first revision, a review was performed for each individual scenario. The review addressed the concern that once the names for mitigations identified as lacking in the vulnerabilities sections were eliminated, that those mitigations would be lost if they were not specifically identified in the mitigations section. To address this issue, new mitigations were added to a number of scenarios that previously were identified as "lacking" in the vulnerabilities section.

The common vulnerability analysis was performed by TWG1 after the common mitigations analysis described in Section 7 and naming the problem frequently resulted in more clarity in the scenario. The following example illustrates this revision. The arrow indicates the conversion from the prior vulnerability name to the new vulnerability name):

- No security monitoring on the WAMPAC network-> *users lack visibility to threat activity,* specifically unexpected access to network components or unusual traffic on the network

- Lack of proper pairing for the HAN router/gateway/trust center and devices -> *network interfaces permit unnecessary traffic flows* instead of only flows to the HAN router/gateway/trust center

In other cases, the new name selected for the vulnerability appeared too high level and the team observed that it read like an "impact," as in

- Inadequate controls on firewall changes -> *system permits unauthorized changes* to the firewalls

Nevertheless, it was believed that the new form would encourage the reader to think through what kinds of authorized changes could occur, and therefore what types of controls were needed to minimize their occurrence. Thus the *system permits unauthorized changes* common vulnerability represents all weaknesses that would permit unauthorized changes to occur. Several other common vulnerabilities are similarly structured.

In other cases, it did not seem feasible to eliminate the "negative" form of the vulnerability and still have it remain meaningful, so the common vulnerability form still has this aspect, as in:

- *software patches are not checked regularly to ensure that they are current*
- *configuration changes are not verified for correctness*

Finally, some original vulnerabilities implied a number of underlying problems and therefore mapped to several common vulnerabilities, as in:

- Insufficient integrity protection of the path used to receive last gasp messages (able to insert, modify, and/or replay messages) *->all three revised vulnerabilities:*
    - *system permits messages to be modified by unauthorized individuals* in the path used to receive last gasp messages
    - *message modified by an adversary is either difficult or infeasible to distinguish from a valid message* in the path used to receive last gasp messages
    - *a copy of a prior message or command is difficult or infeasible to distinguish from a new legitimate message or command* in the path used to receive last gasp messages

6.2 Results

This analysis was based on the working draft version 1.0 of the NESCOR Failure Scenarios document, dated September 2013. The scenarios expressed more than 250

unique vulnerabilities. There were ultimately 82 common vulnerabilities categorized into 23 vulnerability classes. Not all NISTIR 7628 vulnerability classes were represented in the failure scenarios. For example the following were not represented:

- Inadequate Security Oversight by Management
- Inadequate Risk Assessment Process
- Many types of software vulnerabilities, such as Buffer Overflow, Session Management Vulnerability, Logging and Auditing Vulnerability.

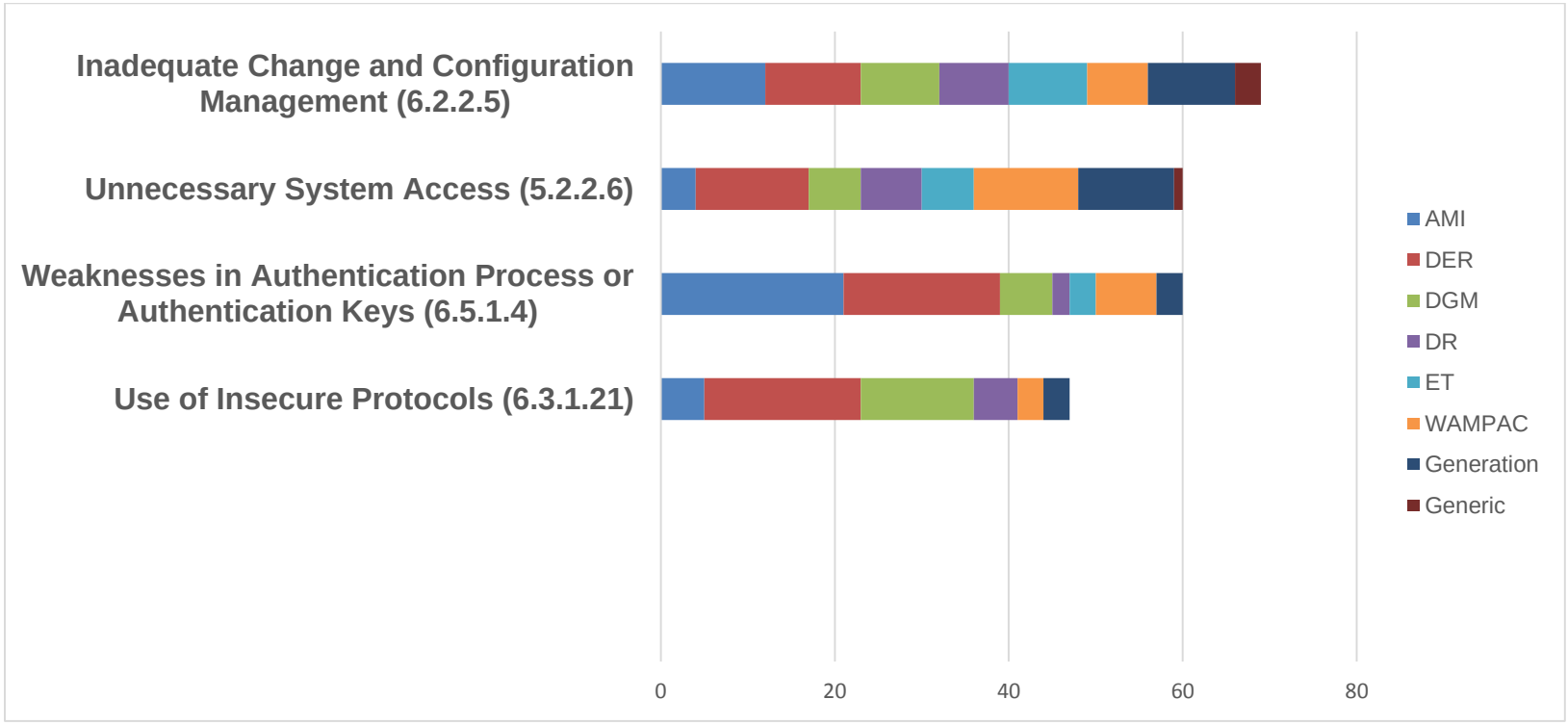
Most classes that did not appear were at the highest and lowest level of granularity among the NISTIR classes. This is a reasonable outcome, because:

- Although a failure scenario could be a result of, for example, inadequate security oversight by management, the scenario cites a more specific vulnerability that was present due to that lack of oversight, and

- The failure scenarios do not name specific low level software vulnerabilities, but identify inadequate development processes as the root vulnerability for scenarios enabled by cyber security software "bugs."

Figure 2 displays the top four classes and the frequency of their occurrence by application domain for Version 3 of this document. The top four most frequent vulnerability classes were Inadequate Change and Configuration Management; Unnecessary System Access; Weaknesses in Authentication Process or Authentication Keys; and Use of Insecure Protocols. The top four represent the most common vulnerabilities classes selected. The prominence of the second and third of these in the areas of authentication and access control is not surprising, since these areas are understood to be key tenets of cyber security. *Inadequate Change and Configuration Management* may be unexpected at the top of the list - however it reflects the fact that maintaining integrity of the system on an ongoing basis is critical for control systems. The prominence of *Use of Insecure Protocols* reflects the many scenarios in which a threat agent attacks interfaces between communicating systems. Frequency is not the only consideration when prioritizing vulnerabilities, since the risk associated with the enabled threat is also important. However, frequency provides a useful rough indicator.

Figure 2. Observed Frequency of Vulnerability Classes



6.3 Summary

This section provides the results of the development of common vulnerabilities. The effort also revised vulnerability names to capture the underlying problem rather than describe the vulnerability as lack of a mitigation. The benefit of this change is that the new names provide insight into the core problem represented by a vulnerability, before the reader selects solutions (mitigations). This task included identifying common vulnerabilities, grouping related vulnerabilities into the NISTIR 7628 vulnerability classes, and counting the occurrence of these classes among the relevant vulnerabilities identified in the failure scenarios. The task showed that along with authentication and access control vulnerabilities, Change Control and Configuration Management and Use of Insecure Protocols are the most frequently occurring classes.

7
Common Mitigation Analysis

In previous working drafts of this document, the mitigations recommended within each short failure scenario were described inconsistently within and across the domains (AMI, DER, etc.). This challenged efforts to identify those mitigations with the greatest potential for the utilities. Section 5 above of this document presents those mitigations normalized to a common form. This form consists of a common action (highlighted in italics within each mitigation listed in Section 5) along with an action application. The mapping from the old form to the new form is described fully in the separate document "Electric Sector Failure Scenarios Common Vulnerabilities and Mitigations Mapping". These changes enabled automated analysis of the mitigations, especially counting the frequency of each mitigation to identify the ones recommended most often. Frequency is not the only ranking that should be considered (the risk associated with the mitigated threat is also important), but it provides a useful rough estimate.

This process identified twenty-two common mitigations for the short failure scenarios documented in Section 5. Following the conversion to common mitigations, the mitigation recommended most frequently was controlling access (107 occurrences), followed by authentication (73 occurrences), better detection (59 occurrences), and verifying settings or conditions (57 occurrences). Controlling access, better detection and verifying settings were recommended by every domain (AMI, DER, etc.). The remainder of this section describes the process and its results in more detail.

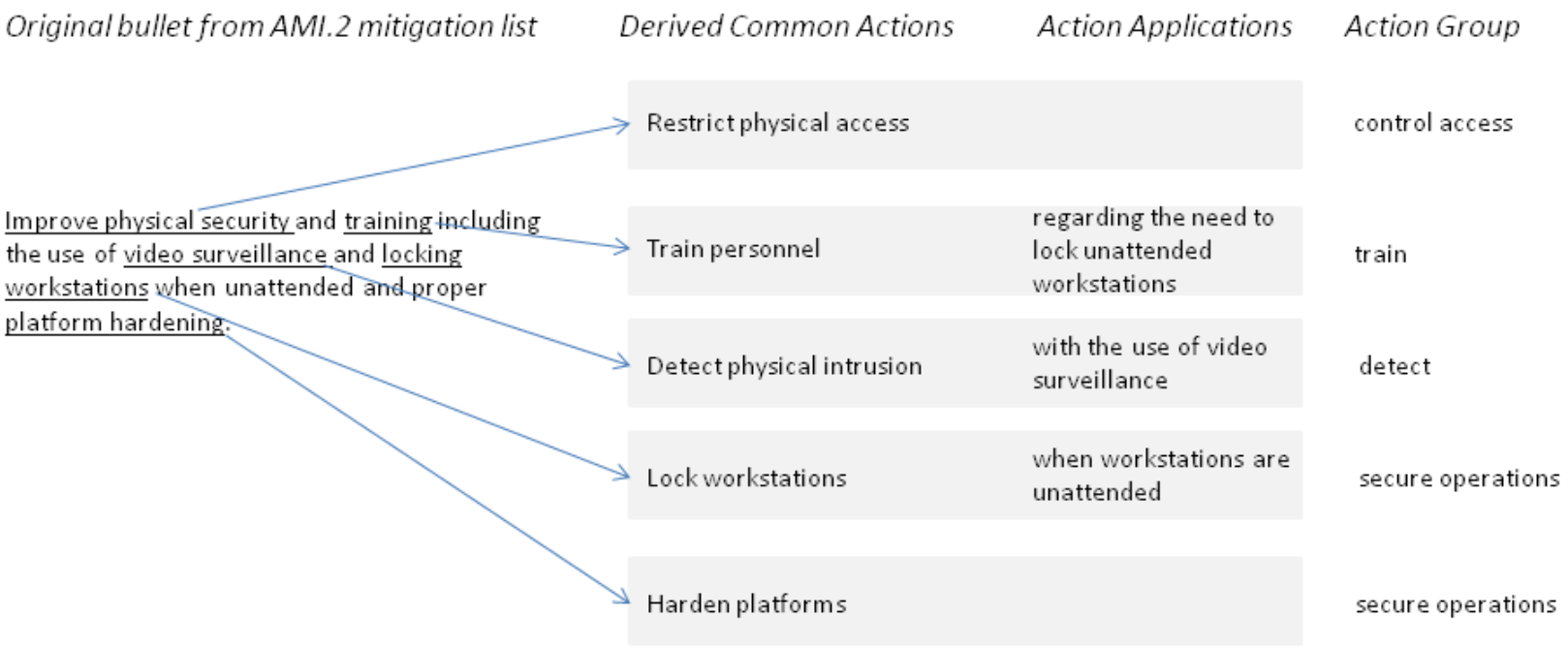
7.1 Process

The recommended mitigations within each short failure scenario are expressed as simple English sentences or phrases. After reviewing many examples, it became apparent that the majority of mitigations could be restated as a *common action* followed by an *action application* that provides context for the common action. For example, the following bullet from the mitigation list of scenario AMI.1: “Data validation to ensure reasonableness of changes” was restated as “Validate data to ensure reasonableness of changes”, where “validate data” is the common action and the remainder is the action application.

Converting each mitigation to this new form required many iterations through the failure scenarios because there were several challenges. One challenge was trying to identify the minimum set of common actions without losing valuable context. For example, the

common actions “use RBAC” and “restrict network access” could both be stated as “control access”, but doing so would obscure the distinctions between them. Changing “use RBAC” to “control access” would lose the context that RBAC was specifically recommended by the mitigation, while changing “restrict network access” to “control access” would lose the context that access should be enforced at the network layer. Another challenge is that different failure scenario authors tended to emphasize different mitigations, e.g., ET authors were unique in their focus on secure charging protocols. Another challenge is that a single bullet in the prior mitigation list might imply several common actions, so it was necessary to carefully associate each mitigation bullet with its derived common actions, as demonstrated in the following figure.

Figure 3. Sample Translation from Mitigation Bullet to Common Actions and Action Groups



When completed, the first task yielded a set of common actions that correlated closely with the mitigation bullets from which they were derived. This was intentional to simplify the process of validating each common action against its mitigation bullet. Though the original mitigation bullets were reduced to a set of common actions about the third of the size, the members of TWG1 believed that there were still too many common actions to support practical analysis. This insight motivated a second task to collect the common actions into larger groups.

Many common actions differed only in subtle ways. The first task, for example, identified the common actions “enforce least privilege,” “use RBAC,” “require read-only access,” “restrict network access,” and “restrict physical access.” Though they differ in technique, they are all means of controlling access. At a high level, “control access” seemed sufficient to distinguish these common actions from other common actions, such as audit or authenticate. A second task, then, focused on collecting related common actions into larger *action groups*. This task reduced the number of items to consider by an order of magnitude.

With the common actions and action groups identified, the third task counted the occurrences of each common action and action group across all failure scenarios. While these counts provide a useful yet general impression of the potential mitigations, they do not fully answer the question of which mitigations offer the most potential for improving the utility’s risk posture because other factors must be considered in that assessment. For example, each common action should be weighted according to the failure scenario’s listed impacts. If the impacts are large, then the return on investment for implementing the mitigation may be large also.

7.2 Results

The initial analysis was based on working draft version 0.9 of the NESCOR Failure Scenarios, dated July 25, 2013. That document contained 111 short failure scenarios distributed across seven application domains (AMI, DER, DGM, DR, ET, GENERIC, and WAMPAC). These scenarios collectively expressed 445 unique, bulleted mitigations. The first task defined 158 common actions, and the second task defined 22 action groups. The assignment of common actions to action groups is documented in Appendix D. Since the original analysis was performed, the failure scenarios have been updated and generation has been added.

Figure 4 displays the top six action groups and the frequency of their occurrence by application domain for Version 3 of this document. The top six were selected as the most common identified across the scenarios.

Each common action was annotated to indicate whether the mitigation is typically implemented as an automated control (typically a technical solution) or a manual control (policy or procedure). This assignment is also documented in Appendix D and is based on version 3 of this document. Of the 162 common actions, 105 were identified as automated and 57 were identified as manual.

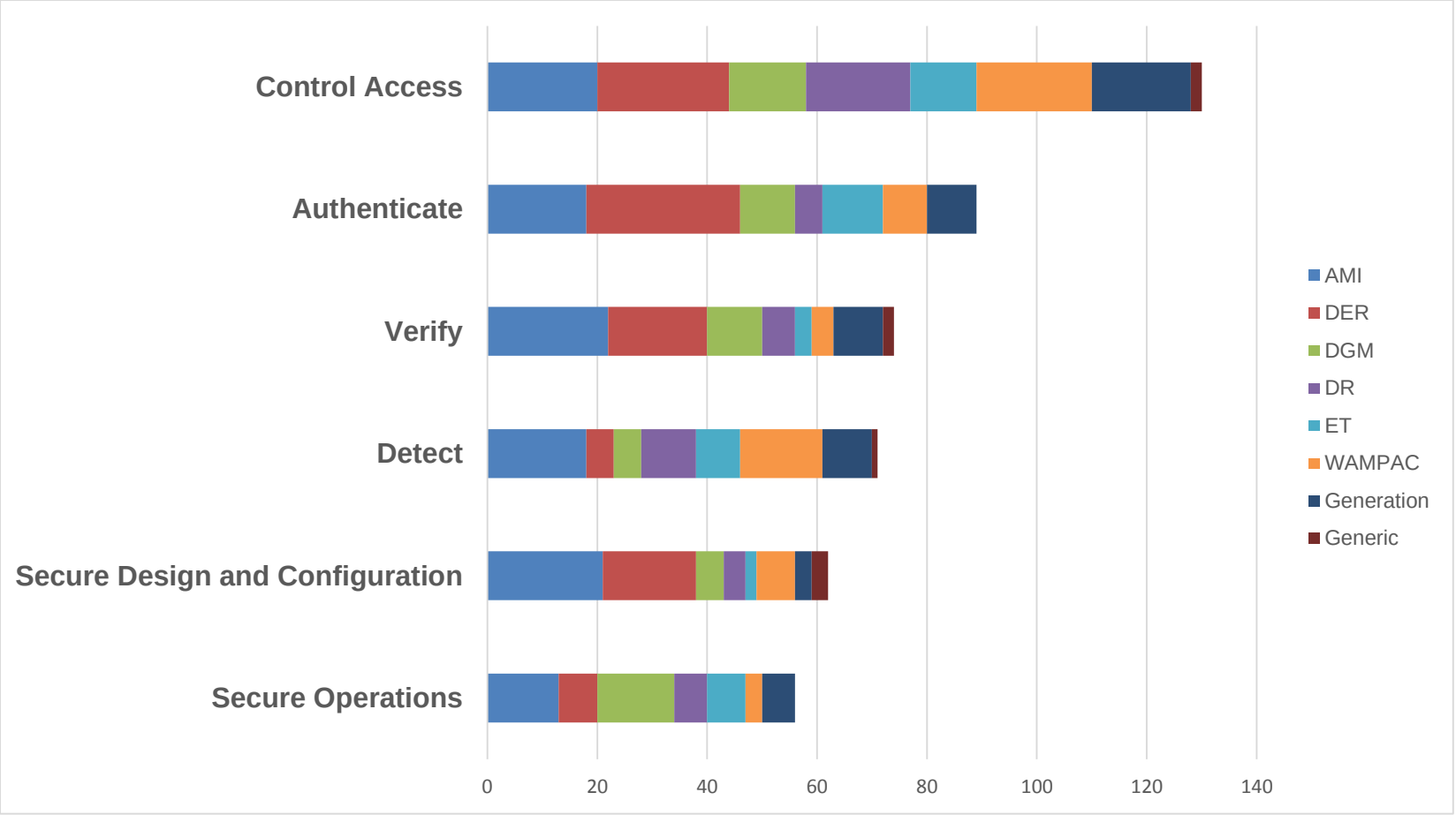


Figure 4. Observed Frequency of Mitigation Action Groups in Failure Scenarios v3.0

7.3 Summary

This section provides the results of the investigation into common mitigations. This task first identified common actions, then grouped related actions into action groups, and counted the occurrence of both within the list of potential mitigations provided in the short failure scenarios. The task revealed a heavy emphasis on access control, authentication, verifying correct operation, and detection. Other common actions, such as encryption, may also yield a good return, but they were not mentioned as often within the failure scenarios.

8

ACRONYMS

ACL	Access Control List
ADR	Automated Demand Response
AMI	Advanced Metering Infrastructure
APN	Access Point Name
AVR	Automatic Voltage Regulator
CA	Certificate Authority
CAPEC	Common Attack Pattern Enumeration and Classification Schema
CCTV	Closed-Circuit Television
CD-ROM	Compact Disk - Read Only Memory
CF	Compact Flash
CIS	Customer Information System
CPP	Critical Peak Pricing
CSP	Commercial Service Provider
DER	Distributed Energy Resources
DERMS	Distributed Energy Resources Management System
DGM	Distribution Grid Management
DHS	Department of Homeland Security
DMS	Distribution Management System
DMZ	Demilitarized Zone
DOE	Department of Energy
DoS	Denial-of-Service
DR	Demand Response
DRAS	Demand Response Automation Server
ET	Electronic Transportation
EV	Electric Vehicle
EVSE	Electric Vehicle Service Equipment
FDEMS	Field DER Energy Management System
FEP	Front End Processor
GPS	Global Positioning System

GSM	Group Special Mobile
HAN	Home Area Network
HMI	Human-Machine Interface
IDS	Intrusion Detection System
ICMP	Internet Control Message Protocol
IED	Intelligent Electronic Device
IPS	Intrusion Prevention System
JTAG	Joint Test Action Group
LAN	Local Area Network
LSS	Line Sharing Switch
LTC	Load Tap Charger
MDMS	Meter Data Management System
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NESCOR	National Electric Sector Cybersecurity Organization Resource
NTP	Network Time Protocol
OC	Optical Carrier
OpenADR	Open Automated Demand Response
OPSEC	Operational Security
PCC	Point of Common Coupling
PDC	Phasor Data Concentrator
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLC	Power Line Carrier
PMU	Phasor Measurement Unit
PWM	Pulse-Width Modulation
QoS	Quality of Service

RBAC	Role-Based Access Control
REP	Retail Energy Provider
RF	Radio Frequency
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SD	Secure Digital
SEP	Smart Energy Profile
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SVC	Static VAR Compensators
TOU	Time-of-Use
TPM	Trusted Platform Module
TWG	Technical Working Group
USB	Universal Serial Bus
V2I	Vehicle-to-Infrastructure
V2G	Vehicle-to-Grid
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAMPAC	Wide Area Monitoring, Protection, and Control
WAN	Wide Area Network

Appendix A Reference Threat Models

A.1 Introduction

This Appendix provides further background related to the threat model presented in Section 3. The following example threat models from other domains were instructive in developing the threat model for the electric sector cyber security domain. The domains addressed by the examples are: the mission for specific individual organizations that provide critical infrastructure in Minnesota (MN) (Table 7), the energy infrastructure in Europe (Table 8 and Table 9), and safety in general, where the cause of failure is due to human error (Table 10). These domains are not the same as the electric sector cyber security domain, but share some common characteristics.

For each example, the ideas that are adopted from that domain for the electric sector cyber security domain threat model are discussed, as well as aspects of the model that did not fit the electric sector cyber security domain.

A.2 Adventium Threat Model

Table 7 shows a threat model developed by Adventium and the Minnesota Red Team in support of several public and private sector organizations in Minnesota.

Table 7 - Adventium Threat Model

Threat Agent	Example Members
Criminal Organizations	Russian Mafia, Sicilian Mafia, Tongs, Yakuza
Eco and Cause Driven	PETA, ALF, Earth First, Greenpeace
Religious Radical Extremists	Al Qaeda, Taliban, 5 Percenters
Lone Extremists	Columbine, Washington Sniper, Hackers
Strategic Political	State Sponsored: China, North Korea, Cuba
Tactical Political	Chechnya Rebels, Hamas, PLO, IRA

Threat Agent	Example Members
US National Separatist	Montana Freemen, US Militia, Aryan Nations, KKK, Folk Nation, People Nation
Natural Hazards	Tornados, Pandemics, Floods

The content adopted and aspects of this model not applicable for the electric sector cyber security domain are:

- Content adopted
  - As laid out in Table 7, threat agents are human as well as non-human.
  - All of the threat agents listed have members that impact the electric sector. Human threat agents may have criminal, political, religious or other cause-driven motivations, and may be groups or loners.
- Aspects not applicable
  - Criminal threat agents in the electric sector cyber security domain behave differently if motivated by money or simply by malevolence, so more granularity is needed.
  - This threat model does not include the possibility for accidental causes or non-malicious human error.
  - Many of the examples given in this threat model do not appear relevant for the electric sector cyber security domain, such as PETA or KKK.

A.3 European Energy Infrastructure Model

As a second example, a threat model to address all causes for failure of the energy infrastructure was developed for the European Commission.[8] The model is not focused specifically on cyber security since it covers all causes for energy infrastructure failure. The criminal threat agents in this model are shown in Table 8 below.

[8]Extracted from **A Reference Security Management Plan for Energy Infrastructure,** Prepared by the Harnser Group for the European Commission, Summer 2010

Table 8 - European Union Threat Agents (Criminal)

Ref	Category/Sub-Category	Ref	Category/Sub-Category
A: Terrorists		**B: Economic Criminals**	
A1	State Sponsored Terrorists	B1	Transnational Criminal Organization
A2	Religious Extremists	B2	Organized Crime Groups
A3	Radical Revolutionaries	B3	Sophisticated Individuals
A4	Guerrillas	B4	Opportunistic Individuals
A5	Amateur Terrorists	B5	Other – Specify
C: Violent Criminals		**D: Subversives**	
C1	Workforce	D1	Political and Industrial Spies
C2	Contractors, Visitors	D2	Activist Groups
C3	Deranged Persons	D3	Disgruntled Persons
C4	Sexual Attackers	D4	Hackers
C5	Muggers	D5	Others
C6		Other – Specify	
E: Petty Criminals			
E1		Vandals	
E2		Petty Thieves	
E3		Other – Specify	

The content adopted and aspects of this model not applicable for the electric sector cyber security domain are:

- Content adopted
    - This model has in common threat agents A1, A2, A3, B1, D2 and D4 with the Adventium model – and all of these are applicable to the electric sector cyber security domain.
    - This model separates economic criminals from other types of criminals, which is appropriate for the electric sector.
    - The model distinguishes between organized crime and individual criminals, which have different motivations and tactics.
    - The model points out the insider threat as well as the threat from deranged persons under C (and this threat extends beyond violent crime).
    - The model points out under D4 the threat of spies and disgruntled persons.

- Aspects not applicable
  - Non-economic criminals in the cyber world are not necessarily violent.
  - The breakdown for economic criminals does not appear to fully separate these entities along the lines of attack methods and mitigations. For example, insiders that are economic criminals and customers that are economic criminals will use different methods than each other and external entities with this same motivation. These three threat agents may require different mitigations.
  - A4, C4, and C5 do not apply to the electric sector.
  - For simplicity of the model, amateur terrorists and petty criminals were not separately identified. This is because in cases where these threat agents cause significant impact, this same impact also could have been achieved by more skilled adversaries. Likewise, the mitigations against those more skilled adversaries would also work against those less skilled.

The following table from the same source covers non-criminal threat agents.

Table 9 - European Union Threat Model (Non-criminal)

Ref	Category/ Subcategory	Ref	Category/ Subcategory	Ref	Category/ Subcategory
A: Natural Hazards		B: Accidental Hazards		C: Consequential Hazards	
A1	Flood	B1	Fire	C1	Loss of Suppliers
A2	Cyclonic Storms	B2	Explosion	C2	Loss of Customers
A3	Tornados	B3	Containment Failure	C3	Loss of Employees
A4	Earthquake	B4	Structural Collapse	C4	Outage – Essential Services
A5	Tsunami	B5	Electrocution	C5	Loss of Transportation
A6	Wildfire			C6	Proximity Hazards
A7	Blizzard/Ice Storm				

The concepts adopted and aspects of this model not applicable to the electric sector cyber security domain are:

- Concepts adopted
  - This model distinguishes between natural and accidental causes, which are important since they require different mitigations.

  - Related to column C, loss of employees that detect or respond to failure situations, and outages of outsourced communications or networking services would fit under this set of hazards, and are applicable in the electric sector cyber security domain.

- Aspects not applicable
  - The distinction between many types of natural and accidental hazards in columns A and B is not as important for cyber security failures, as the impact of any of these causes will be to take out processing, control or communication facilities, resulting in the need to implement back-up operations.

  - However, the focus on cyber security will require some additional types of accidental hazards to be considered, in particular non-malicious human error.

  - Except as noted under “concepts adopted,” the consequential hazards in Column C do not apply to cyber security related failures.

A.4 Safety and Human Error

To address the topic of non-malicious human error, TWG1 reviewed models used in the safety-related industry, which has done extensive study of human- in- the-loop system failures. The UK Health and Safety Executive (HSE) organization[9] summarizes critical topics to be addressed in avoiding human errors as shown in the left column of Table 10. This list of topics was not developed specifically as a threat model, but provided a useful starting point.

TWG1 considered whether the safety-related evidence would generalize to cyber security related events, by reviewing a range of such events where human error was involved in the underlying cause. The events ranged from configuration of systems, to operation centers, to large-scale system failure. The conclusion from the review was that the human error descriptions and analysis from the safety-related events did

[9] http://www.hse.gov.uk/humanfactors The Health and Safety Executive (HSE) is a UK national independent watchdog for work-related health, safety and illness. HSE is independent regulator and acts in the public interest to reduce work-related death and serious injury across Great Britain’s workplaces.

appear to describe the underlying topics important for human errors in cyber events. Thus this is likely to hold true more specifically for cyber security related events.

The topics related to human error are summarized as shown in the left column of Table 10 into the following five vulnerabilities related to human error in the electric sector cyber security domain.

(1) Poor human-system design

(2) Configuration or data entry errors

(3) Inadequate or non-existence of policy, process, procedures, and training

(4) Non-compliance (not following policy and procedures)

(5) Inadequate auditing, maintenance and testing

These concepts are more specific to cyber security and provide more guidance on potential mitigations than some of the HSE topics. For example, human failures have been mapped to configuration or data entry errors, which is specific to cyber security. As a second example, organizational change is probably not preventable, but addressing policy, procedures, training and compliance serve to mitigate its negative effects.

Table 10 - HSE Topics Mapped to Electric Sector Cyber Security Threat Agents

HSE Human Errors and Safety Topics	Vulnerabilities Human Errors Electric Sector Cyber Security Domain
Human failures, staffing	(2) Configuration or data entry errors (4) Non-compliance (not following policy and procedures)
Fatigue and shift work	(1) Poor human-system design (2) Configuration or data entry errors (4) Non-compliance (not following policy and procedures)
Safety critical communication	(3) Inadequate or non-existence of policy, process, procedures, and training
Human factors in design	(1) Poor human-system design
Procedures	(3) Inadequate or non-existence of policy, process, procedures, and training (3) Inadequate or non-existence of policy, process, procedures, and training
Competence	(3) Inadequate or non-existence of policy, process, procedures, and training

HSE Human Errors and Safety Topics	Vulnerabilities Human Errors Electric Sector Cyber Security Domain
Training	(3) Inadequate or non-existence of policy, process, procedures, and training
Organizational change	(3) Inadequate or non-existence of policy, process, procedures, and training (4) Non-compliance (not following policy and procedures)
Organizational culture	(3) Inadequate or non-existence of policy, process, procedures, and training (4) Non-compliance (not following policy and procedures)
Maintenance, inspection and testing	(5) Inadequate auditing, maintenance and testing
Action errors for skills-related tasks, where familiarity brought errors of omission or commission	(1) Poor human-system design (2) Configuration or data entry errors (3) Inadequate or non-existence of policy, process, procedures, and training (4) Non-compliance (not following policy and procedures)
Thinking errors including decision making and judgment	(1) Poor human-system design (3) Inadequate or non-existence of policy, process, procedures, and training (4) Non-compliance (not following policy and procedures)
Non-compliance including deviation from the rules either on purpose or accidental.	(4) Non-compliance (not following policy and procedures)

Appendix B Additional Information on Failure Scenario Ranking

This appendix provides additional information regarding the failure scenario ranking methodology described in Section 4.

B.1 Scoring Guidance

The most effective process for the scoring of criteria for each failure scenario is to have a group of experts meet to agree on consensus scores. A second option is to have experts independently score each of the criteria and then average the scores. Team members that have done similar exercises agreed that the exchange of observations and assumptions in a discussion setting contributes to a better quality result.

To understand how the ranking process would work in practice, TWG1 walked through the scoring of an example failure scenario. To achieve repeatable and objective rankings, it is clear that specific guidelines for scoring are required. Two points of confusion in the trial scoring exercise were:

- The descriptions for the various scores were not mutually exclusive,
- There were failure scenarios for which the scoring descriptions did not seem to apply.

An attempt to make the definitions provided for each score mutually exclusive from the other scores appeared to complicate them unnecessarily. It was also clear that the score definitions could not feasibly envision a method of scaling that would fit exactly for all scenarios. Hence to resolve the issues above, the following guidelines were developed, leveraging guidelines used by TWG1 members for similar tasks.

Guidance	Rationale/Example
1) Indicate score as discrete values 0, 1, 3, or 9. 2) Do not use other values	When assigning numbers to represent H, M, L, and NA, whole numbers should be used for simplicity, rather than values between 0 and 1. Using a wide and unevenly spaced range of numbers generates deeper thought and better results than a scheme such as 0, 1, 2, 3. In the latter case, 2 is too often an easy default score.
3) For impact criteria: a) If more than one of the scoring descriptions applies, select the	As an example of 3a), If both “3: any possible injury”, and “9: any possible

Guidance	Rationale/Example
highest one. b) If none of them apply, select the highest score impact that is closest in seriousness to an impact that could occur.	death" might apply for a scenario, select 9. As an example of 3b), suppose a failure scenario causes a flood of customer service calls for a week. The possible scores for the criterion "Critical back office operations are impacted" are: 0: None 1: isolated errors in customer bills 3: 2 week delay in billing customers, widespread errors in bills 9: customer service or power usage data collection off-line more than one day The impact in question seems more serious than isolated errors in customer bills, but less serious than customer service off-line for more than a day. Hence this scenario would be scored as 3 for this criterion.

Guidance	Rationale/Example
4) For effects on likelihood and opportunity criteria: a) If more than one of the scoring descriptions applies, select the highest one. b) If none of them apply, select the highest scored item that most closely resembles the effect on the likelihood and opportunity for the failure scenario.	As an example of 4a), the “common vulnerability among others” criterion has possible scores: 0: Isolated occurrence 1: More than one utility 3: Half or more of the power infrastructure 9: Nearly all utilities If score 3 applies to a scenario, score 1 also applies. However, in this case, score the scenario as 3. As an example of 4b), the “accessibility (physical)” criterion has possible scores: 0: Inaccessible 1: Guarded, monitored 3: Fence, standard locks 9: Publicly accessible A scenario in which a portable system is in a tamperproof case does not match any of these, but may closely resemble the description for score 1 in terms of effect on the likelihood and opportunity for the occurrence of scenario.

B.2 Refinements to the Ranking Process

The following sections discuss refinements to the ranking process described in Section 4.

B.2.1 Impact of Utility Characteristics on Scores

TWG1 believed that some of the criteria would be scored differently, depending upon the characteristics of the utility. This is taken into account when a utility scores a failure scenario for its own purposes, but there was a question of how TWG1 should address this when scoring the failure scenarios in the context of the overall industry.

TWG1 members proposed that it would be useful to develop three different reference models for utilities – one for small utilities (including munis and coops), a second for medium size utilities (including munis and coops), and a third for large utilities (including munis and coops). The ranking process would then provide three scores per failure scenario, one for each reference model utility. If this approach was pursued, it was suggested that the models be built "bottom-up" by analyzing the characteristics that would impact the rank of each scenario, rather than attempting to create these models up front and then ranking the scenarios for each model. This is because models created up front would themselves take considerable effort, and then are unlikely to adequately support the next step to differentiate scenario rankings for each model.

An alternative approach would be to produce just one score per scenario that would apply to a utility with reasonably common characteristics. The resulting ranking would apply to a large number of utilities, though not all utilities. In this case one would document the characteristics of the utility assumed when determining this score.

The first approach could be more accurate and more directly useful to individual utilities, but will take considerably more effort to execute. The second approach would be less detailed, but more streamlined and may be sufficient to meet a goal such as that of TWG1 for the failure scenario ranking process. In general, feedback on the ranking method has been that documentation of assumptions made during the process is critical to its success.

B.2.2 Correcting for Equation Bias

The implicit assumption in the ranking approach is that all the ranking criteria for impact, and for likelihood, have the same importance, since the method adds their scores to get composite impact and likelihood scores. If subsequent experience with the ranking method yields intuitively incorrect results due to a failure of this assumption, adjustment of the criteria or application of weights to them can be considered, or the conservative approach discussed in the next paragraph.

To take a conservative approach, all failure scenarios could be ranked as High (with non-negligible probability/likelihood) if they had impacts that exceed some defined threshold. An example of a possible threshold is: There is at least one criterion where the failure scenario impact is "High" or at least three criteria where the scenario impact is "Medium." Using this threshold-based or rule-based evaluation procedure for identifying failure scenarios as High priority might mitigate biases that could be present in an equation-based evaluation where scoring is dependent on the values chosen for the equation weights. This rule could be applied as a post-processing operation to an addition-based method, and would result in some failure scenarios being added to the High list.

B.2.3 Identify "Low Hanging Fruit"

Consideration should be given to raising the priority for, or otherwise flagging failure scenarios that might be mitigated by policies, procedures, and training. Mitigation of these failure scenarios is likely to have a good return on investment for a utility. Hence the identification of such failure scenarios would be a useful output from the analysis of the set of scenarios. A significant step has been taken in this analysis by the assignment of mitigations as manual or automatic as part of the common mitigation analysis described in Section 7.

B.3 Other Ranking Methods Considered

TWG1 discussed the following type of equations to combine the types of criteria, in addition to the impact/cost ratio described in **Error! Reference source not found.** initially used by TWG1.

- **Weighted sum/product:** Create subtotals for each of the criteria types and combine them in a weighted sum/product. This basic idea is used by the Common Vulnerability Scoring System (CVSS) Version 2,[10] which is a recognized system used to rank software vulnerabilities and prioritize repairs. Example underlying weights used by CVSS are .6 for impact and .4 for exploitability. However, the CVSS equation expands considerably on the basic weighted sum idea. It is significantly more complex than a simple weighted sum, more so than would be appropriate for the purposes here.

The group was not generally in favor of such a method, since they believed that impact is usually multiplied by probability in order to obtain risk, these factors are not normally added together.

B.4 Additional Ranking Criteria for Utility-Specific Prioritization

This section lists additional proposed ranking criteria beyond those described in Section 4.2.2 that may be useful for an individual utility to apply for mitigation planning or incident response purposes.

The scoring notation used for these criteria differs from that used for the criteria in Section 4.2.2. This is because numerical scoring definitions have not been developed for these criteria.

B.4.1 Mitigation Criteria

Table 11 lists general mitigation strategies that are available for a utility to minimize the impacts listed in Table 2. If these mitigations are already implemented, this may lower

[10] See Section 3.2 of http://www.first.org/cvss/cvss-guide.pdf

the priority of further addressing a failure scenario from the point of view of a specific utility. These criteria could be assessed by a single utility for their situation or for a particular incident. They also might appear as characteristics of the various types of model utilities as discussed in Appendix B.2.1.

In the following discussion, these criteria are discussed and scored as shown in Table 11 for the example failure scenario used in Section 4, in which a widely deployed smart meter does not encrypt customer data.

Redundant systems: This criterion indicates whether using redundant systems can mitigate the expected consequences of this failure scenario. This would be scored by first assessing whether a redundant system exists for systems affected by the failure scenario, and then whether this system would mitigate the failure scenario. In many cases redundant systems *do not* address malicious cyber security attacks, because the threat agent can just as easily target both systems as one of them. For the example failure scenario, no redundant system would prevent the loss of privacy that occurs hence this score is *No*.

Backup systems available: Similar to the previous criterion, this criterion indicates whether using backup systems can mitigate the expected consequence of a failure scenario. This would be scored as discussed for the redundant systems criteria. For the example failure scenario, no backup system would prevent the loss of privacy that occurs hence this score is *No*.

Independent, standalone systems: The intent of this criterion is to address independent stand-alone systems that will typically have less impact than for more integrated parts of an overall “system of systems.” The example failure scenario was scored as *Fully Integrated* since the feed from the meter is transmitted over communications media that is connected to the upstream functions of the utility.

Able to be reconfigured or diverted during an attack: This criterion indicates whether reconfiguration or some method of diverting load from an under-attack element of the system can mitigate the expected consequence of a failure scenario. This would be scored in a similar manner as discussed for the redundant systems criterion. For the example failure scenario no such mitigation is available hence this score is *No*.

Table 11 - General Mitigations Criteria

Mitigation				
Redundant systems	**Negligible**	**Yes**	**Somewhat**	**No**
Backup systems available	**Negligible**	**Yes**	**Somewhat**	**No**
Independent, Standalone system	**Negligible**	**Isolated**	**Somewhat**	**Fully Integrated**
Able to be reconfigured or diverted during an attack	**Negligible**	**Yes**	**Somewhat**	**No**

B.4.2 Feedback

Table 12 lists criteria that assess the “feedback” to the utility that may result if a threat agent carries out a failure scenario. “Feedback” is a response from constituents including customers, regulators, or shareholders. Each utility may have a unique view on how the scoring of these criteria should impact the priority of a failure scenario from their point of view.

In the following discussion, these criteria are discussed and scored as shown in

Table 12, for the example failure scenario.

The criteria “Illustrates a gap in local, state, or national policies or standards” and “Exposes need for new regulations” are inherently subjective, hence a precise definition of how to score them would be challenging. Scoring for these is best accomplished by providing a few scored examples, then polling a number of experts in the subject matter and assessing the majority opinion.

For the example failure scenario, there may be additional standards and regulations applicable to the smart grid, particularly if widespread failure scenarios such as the example are encountered. Hence both of these criteria are scored as *Somewhat*.

Possible compliance prioritization issue: This criterion means that the occurrence of the failure scenario points to a possible non-compliance by the utility in some area of regulation. At this time, this would be scored as *No* for the example failure scenario.

Table 12 - Feedback Criteria

Feedback				
Illustrates a gap in local, state, or national policies or standards	**Negligible**	**No**	**Somewhat** 	**Yes**
Exposes need for new regulations	**Negligible**	**No**	**Somewhat** 	**Yes**
Possible compliance prioritization issue	**Negligible**	**No** 	**Somewhat**	**Yes**

Appendix C Mapping of Failure Scenarios to NISTIR 7628 Families

The following table lists the families included in the NISTIR 7628 and their codes. The codes are used in the next table.

Table 13 - Codes for NISTIR 7628 Smart Grid Requirements Families

Ref.	NIST Smart Grid Security Requirements Families
SG.AC	Access Control
SG.AT	Awareness and Training
SG.AU	Audit and Accountability
SG.CA	Security Assessment and Authorization
SG.CM	Configuration Management
SG.CP	Continuity of Operations
SG.IA	Identification and Authentication
SG.ID	Information and Document Management
SG.IR	Incident Response
SG.MA	Smart Grid system Development and Maintenance
SG.MP	Media Protection
SG.PE	Physical and Environmental Security
SG.PL	Strategic Planning
SG.PM	Security Program Management
SG.PS	Personnel Security
SG.RA	Risk Management and Assessment
SG.SA	Smart Grid system and Services Acquisition
SG.SC	Smart Grid System and Communication Protection
SG.SI	Smart Grid System and Information Integrity

Table 14 - Mapping of Failure Scenarios to NISTIR 7628 Smart Grid Requirements Families

	SG.AC	SG.AT	SG.AU	SG.CA	SG.CM	SG.CP	SG.IA	SG.ID	SG.IR	SG.MA	SG.MP	SG.PE	SG.PL	SG.PM	SG.PS	SG.RA	SG.SA	SG.SC	SG.SI
AMI.1	x		x		x													x	
AMI.2	x	x	x		x							x						x	
AMI.3	x		x		x							x							x
AMI.4																	x	x	
AMI.5																		x	
AMI.6	x																		x
AMI.7			x	x	x												x	x	
AMI.8							x											x	x
AMI.9	x	x	x		x		x											x	x
AMI.10	x		x				x												x
AMI.11																		x	
AMI.12	x			x	x													x	
AMI.13		x					x					x					x		
AMI.14																		x	
AMI.15						x						x				x			
AMI.16																		x	
AMI.17																x			
AMI.18	x						x												
AMI.19			x																x
AMI.20	x		x		x														
AMI.21	x				x						x							x	
AMI.22	x						x												
AMI.23					x		x												

	SG.AC	SG.AT	SG.AU	SG.CA	SG.CM	SG.CP	SG.IA	SG.ID	SG.IR	SG.MA	SG.MP	SG.PE	SG.PL	SG.PM	SG.PS	SG.RA	SG.SA	SG.SC	SG.SI
AMI.24					x												x	x	
AMI.25	x		x		x												x		
AMI.26																	x	x	
AMI.27					x												x		
AMI.28					x												x		x
AMI.29					x														
AMI.30							x												x
AMI.31			x				x											x	x
AMI.32	x						x												x
DER.1		x			x		x												
DER.2		x			x		x											x	x
DER.3							x									x		x	x
DER.4																		x	
DER.5			x		x											x			
DER.6			x															x	
DER.7					x													x	
DER.8	x		x															x	
DER.9			x																
DER.10	x	x			x		x												
DER.11	x	x	x		x		x												
DER.12	x				x		x												
DER.13			x																x
DER.14					x		x											x	x
DER.15							x											x	x

	SG.AC	SG.AT	SG.AU	SG.CA	SG.CM	SG.CP	SG.IA	SG.ID	SG.IR	SG.MA	SG.MP	SG.PE	SG.PL	SG.PM	SG.PS	SG.RA	SG.SA	SG.SC	SG.SI
DER.16							x											x	
DER.17			x		x		x												x
DER.18	x		x		x		x							x				x	x
DER.19	x																	x	
DER.20	x																	x	
DER.21	x		x															x	x
DER.22 (deleted)																			
DER.23	x		x																
DER.24	x		x															x	
DER.25	x				x														
WAMPAC.1	x		x		x													x	x
WAMPAC.2	x				x													x	
WAMPAC.3	x				x													x	
WAMPAC.4	x				x		x											x	x
WAMPAC.5	x				x														
WAMPAC.6	x				x														x
WAMPAC.7	x		x		x													x	
WAMPAC.8	x				x														x
WAMPAC.9 (deleted)																			
WAMPAC.10	x				x		x											x	
WAMPAC.11	x				x														x
WAMPAC.12																	x		
ET.1							x												x

	SG.AC	SG.AT	SG.AU	SG.CA	SG.CM	SG.CP	SG.IA	SG.ID	SG.IR	SG.MA	SG.MP	SG.PE	SG.PL	SG.PM	SG.PS	SG.RA	SG.SA	SG.SC	SG.SI
ET.2				x								x							x
ET.3			x		x					x		x			x	x	x		x
ET.4	x				x													x	
ET.5																			x
ET.6	x						x												
ET.7																		x	
ET.8							x												
ET.9			x		x		x												
ET.10	x						x												
ET.11	x		x				x												
ET.12						x							x				x		
ET.13	x		x																
ET.14			x											x					
ET.15	x		x										x						x
ET.16	x		x															x	x
DR.1	x		x		x		x												x
DR.2	x											x						x	x
DR.3	x											x		x				x	x
DR.4	x		x									x							
DR.5					x		x					x							x
DR.6	x				x														
DGM.1						x						x							
DGM.2												x			x				
DGM.3	x		x		x							x							x

	SG.AC	SG.AT	SG.AU	SG.CA	SG.CM	SG.CP	SG.IA	SG.ID	SG.IR	SG.MA	SG.MP	SG.PE	SG.PL	SG.PM	SG.PS	SG.RA	SG.SA	SG.SC	SG.SI
DGM.4	x		x		x		x												x
DGM.5			x		x									x				x	x
DGM.6	x						x											x	
DGM.7	x				x		x										x	x	
DGM.8			x		x										x	x	x		
DGM.9					x	x			x							x			
DGM.10	x	x										x							
DGM.11	x	x	x					x										x	
DGM.12			x				x							x				x	
DGM.13					x														
DGM.14							x							x				x	
DGM.15	x	x	x		x			x										x	
DGM.16	x						x					x						x	
GEN.1			x		x		x					x							
GEN.2			x		x													x	x
GEN.3			x		x												x		
GEN.4		x	x		x		x												
GEN.5	x				x							x							x
GEN.6		x	x		x														x
GEN.7																			x
GEN.8	x	x					x												x
GEN.9	x	x			x														
GEN.10	x											x						x	
GEN.11		x			x													x	x

	SG.AC	SG.AT	SG.AU	SG.CA	SG.CM	SG.CP	SG.IA	SG.ID	SG.IR	SG.MA	SG.MP	SG.PE	SG.PL	SG.PM	SG.PS	SG.RA	SG.SA	SG.SC	SG.SI
GEN.12	x				x	x													
GEN.13	x																		x
GEN.14						x	x											x	x
GEN.15	x	x	x		x		x												x
GEN.16					x							x							x
GENERIC.1	x		x																x
GENERIC.2		x	x		x	x			x					x					x
GENERIC.3	x	x		x	x											x			
GENERIC.4			x	x	x												x	x	

Appendix D Common Vulnerabilities List

The table in this appendix presents the common vulnerabilities as discussed in Section 6, and their organization into the vulnerability classes from NISTIR 7628 Volume 3.

The separate document "Electric Sector Failure Scenarios Common Vulnerabilities and Mitigations Mapping" contains the full mapping of the prior vulnerabilities listed for each failure scenario to the *common vulnerability*, *context* form used in this document version.

Table 15 - Common Vulnerabilities and Vulnerability Classes

Vulnerability Class	Common Vulnerability
API Abuse (6.3.2.1)	presence of features or functions that may be misused by users
Business Logic Vulnerability (6.3.1.8)	critical operations are not locked out during maintenance
	inadequate criteria for determining which alarms deserve priority
	system assumes data inputs and resulting calculations are accurate
	system design limits opportunity for system recovery using reconfiguration
	system permits potentially harmful command sequences
	system takes action before confirming changes with user
Cryptographic Vulnerability (6.3.1.4)	cryptography used that employs algorithms that are breakable within a time period useful to the adversary
Error Handling Vulnerability (6.3.1.6)	system may become overwhelmed by traffic flooding or malformed traffic
	users lack visibility to the failure of the system to respond to commands
General Logic Error (6.3.1.7)	alarm management system does not support required processing for legitimate alarm conditions
	alarm processing capability is overwhelmed by unnecessary alarms
Inadequate Anomaly Tracking (6.4.4.1)	users lack visibility of threat activity
	users lack visibility of unapproved access
	configuration changes are not verified for correctness
	sensitive data remains on disposed equipment

Vulnerability Class	Common Vulnerability
Inadequate Change and Configuration Management (6.2.2.5)	system permits unauthorized changes
	system permits unauthorized installation of software or firmware
	users lack visibility that unauthorized changes were made
	users lack visibility that unauthorized firmware has been installed
Inadequate Continuity of Operations or Disaster Recovery Plan (6.2.3.3)	emergency response procedures unintentionally omit security controls
	emergency situations may not have the appropriate replacement equipment
	inadequate continuity and recovery security architecture
Inadequate Incident Response Process (6.2.3.5)	speed of incident response process is not appropriate for incident
Inadequate Malware Protection (6.4.2.3)	system permits installation of malware
	the list of signatures used for detection of attacks is no longer current
Inadequate Network Segregation (6.5.1.2)	communication channels are shared between different system owners
	Internet connection may be misused by adversary
	network interconnections provide users and hardware/software entities with access unnecessary for their roles
	network interfaces permit unnecessary traffic flows
	network is connected to untrusted networks
	network services are shared between different system owners
	publicly accessible and/or third party controlled links used
Inadequate Patch Management Process (6.2.2.4)	software patches are not checked regularly to ensure that they are current
	software patches may be applied without verifying continued system operation
Inadequate Periodic Security Audits (6.2.3.1)	adherence to policies and procedures degrades over time
	human error in adherence to policies and procedures
Insufficient Identity Validation or Background Checks (6.2.2.1)	insiders with high potential for criminal or malicious behavior have access to critical functions or sensitive data

Vulnerability Class	Common Vulnerability
Insufficiently Trained Personnel (6.2.1.1)	workforce may be unaware of recommended precautions
	workforce not trained in proper procedures
Insufficient Redundancy (6.5.1.5)	critical components exhibit single point of failure
Physical Access to the Device (6.5.1.6)	enabled but unused ports
	physical access may be obtained by unauthorized individuals
	physical access to a serial port may enable logical access by unauthorized entities
	physical access to mobile devices may enable logical access to business functions by unauthorized individuals
Sensitive Data Protection Vulnerability (6.3.1.15)	system makes private data accessible to unauthorized individuals
Unnecessary System Access (6.2.2.6)	back doors for access are left in place
	default configuration allows access that is unnecessary after the system is operational
	design permits unnecessary privileges
	remote access may be obtained by unauthorized individuals
	system permits bypass of physical access controls
	system permits networking components to be accessed by unauthorized individuals
	system permits wireless access by unauthorized parties
	unnecessary access is permitted to critical functions
	unnecessary access is permitted to networking components
	unnecessary access is permitted to system functions
	unnecessary access is permitted to the communications channel
	unnecessary access is permitted to the database
	unnecessary access is permitted to the operating system
	unnecessary network access is permitted

Vulnerability Class	Common Vulnerability
	users and hardware/software entities are given access unnecessary for their roles
Unneeded Services Running (6.4.3.2)	unnecessary system services are configured to run
Use of Inadequate Security Architectures and Designs (6.4.1.1)	critical communication paths are not isolated from communication paths that require fewer protections to operate
	critical functions are not isolated from those that require fewer protections to operate
	security design does not consider the system lifecycle
	system permits bypass of access control mechanisms
	system permits device identifier to be misused
	weaker security architecture at backup sites
Use of Insecure Protocols (6.3.1.21)	a copy of a prior message or command is difficult or infeasible to distinguish from a new legitimate message or command
	commands or other messages may be inserted on the network by unauthorized individuals
	message modified by an adversary is either difficult or infeasible to distinguish from a valid message
	spoofed signal is either difficult or infeasible to distinguish from a legitimate signal
	system makes messages accessible to unauthorized individuals
	system permits messages to be modified by unauthorized individuals
	system relies on communications that are easy to jam
	credentials are accessible in the clear
Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)	default password is not changed
	encryption keys are shared
	inadequate binding of meter with energy users authorized to charge to that meter
	secret key is stored or transmitted in the clear
	shared credentials are used for access
	system relies on credentials that are easy to obtain for access

Appendix E Common Mitigations List

The table in this appendix presents the common actions and their organization into action groups as discussed in Section 7. The table also notes the implementation type that was assigned to each common action. If the type is ‘a’, that implies that performing the action will typically require an *automatic* implementation. If the type is ‘m’, that implies that the action is typically performed *manually*.

The separate document "Electric Sector Failure Scenarios Common Vulnerabilities and Mitigations Mapping" contains the full mapping of the prior mitigations listed for each failure scenario to the *common action*, *action application* form.

Table 16 - Action Groups and Common Actions

Action Group	Type	Common Action
alert	a	generate alarms
	a	generate alerts
	a	prioritize alarms
analyze	m	analyze anomalous events
	m	re-evaluate scheduled disconnects
	m	review recovery response
audit	a	create audit log
	a	protect audit logs
	m	perform audit
	m	perform financial audit
authenticate	a	authenticate data source
	a	authenticate devices
	a	authenticate messages
	a	authenticate users
	a	require authentication
	a	require multi-factor authentication
	a	require PIN
	a	require second-level authentication
	a	require single sign-on
check integrity	a	check message integrity
	a	check OS integrity
	a	check software execution integrity
	a	check software file integrity
	a	protect against replay
control access	a	enforce least privilege
	a	require credential revocation
	a	restrict access

Action Group	Type	Common Action
	a	restrict network access
	a	restrict physical access
	a	use RBAC
	a	enforce restrictive firewall rules
	a	limit remote modification
	a	Prevent remote modification
	a	prevent modification
	a	require read-only access
	a	restrict application access
	a	restrict communication access
	a	restrict configuration access
	a	restrict database access
	a	restrict device access
	a	restrict file access
	a	restrict Internet access
	a	restrict remote access
	a	restrict system access
	m	restrict network service access
	m	restrict physical access
	m	restrict port access
detect	a	detect abnormal behavior
	a	detect abnormal functionality
	a	detect anomalous commands
	a	detect physical intrusion
	a	detect unauthorized access
	a	detect unauthorized configuration changes
	a	detect unauthorized use
	a	detect unusual patterns
	a	detect abnormal output
	a	detect unauthorized configuration
	a	detect unauthorized connections
	a	detect unauthorized devices
	a	require intrusion detection and prevention
	m	detect abnormal functionality
encrypt	a	encrypt application layer
	a	encrypt communication paths
	a	encrypt data at rest
	a	encrypt link layer
	a	require VPNs
enforce limits	a	enforce hardware limits

Action Group	Type	Common Action
	a	enforce limits in hardware
	a	limit events
	a	protect from overcharge
	a	require circuit breaker
ensure availability	a	require fail-over
	a	require fail-safe rollback
	a	require redundancy
	a	require synchronous functions
	m	require backup
	m	require redundancy
	m	require resiliency
	m	require spares
	m	require spread-spectrum radio
isolate	a	isolate functions
	a	isolate networks
	a	require unique keys
	a	require separation of duty
	m	isolate networks
learn	m	learn from others
plan	m	define contingency plan
	m	define incident response plan
	m	define policy
	m	define procedure
	m	emphasize security management
	m	prioritize recovery activities
profile	m	profile equipment
sanitize	a	sanitize device
secure design and implementation	a	configure for least functionality
	a	protect credentials
	a	protect security configuration
	a	require secure key storage
	m	design for security
	m	design for trust
	m	minimize private information
	m	require approved cryptographic algorithms
	m	require approved key management
	m	require physical connection
	m	require secure factory settings
	m	restrict occurrence

Action Group	Type	Common Action
secure operations	a	maintain anti-virus
	a	maintain latest firmware
	a	maintain patches
	a	require application whitelisting
	a	require lockout
	a	require safe mode
	a	require strong passwords
	a	require secure boot loader
	a	require secure remote firmware upgrade
	a	require tamper detection and response
	a	require video surveillance
	m	change default credentials
	m	lock workstations
	m	require assured maintenance
	m	require password rule enforcement
test	m	conduct code review
	a	conduct penetration testing
	a	perform hardware acceptance testing
	a	perform security testing
	a	require reconfiguration in test mode
	a	test after installation
	a	test after maintenance
	a	test before installation
	a	test for malware
	a	vulnerability scan before installation
track	m	implement configuration management
	m	track asset
train	m	train personnel
user decision	m	choose own rate
	m	continue normal operations
verify	a	confirm action
	a	cross check
	a	require two-person rule
	a	require acknowledgment
	a	require failure messages

Action Group	Type	Common Action
	a	require message verification
	a	require non-repudiation
	a	require on-going validation
	a	validate data
	a	validate inputs
	a	validate signal
	a	verify absence of hardcoded credentials
	a	verify correct operation
	a	verify EV owner
	a	verify mode
	a	verify network changes
	a	verify settings
	a	verify time synchronization
	m	confirm action
	m	cross check
	m	require approval
	m	Require periodic physical surveillance
	m	require periodic walk-downs
	m	require reliable external time source
	m	verify load
	m	verify personnel

Appendix F Supplementary Information for Selected Common Vulnerabilities

The table in this appendix contains additional information regarding selected common vulnerabilities. In particular it lists important (though not exhaustive) sub cases for some of the common vulnerabilities, where the vulnerability is stated more broadly in the failure scenarios. These sub cases should be considered when determining whether the vulnerability exists in a particular situation. They are provided here to avoid being repetitive or implying completeness by listing the sub cases in every scenario in place of the broader vulnerability. Also, the table notes cases when a common vulnerability is an important sub case of another more general common vulnerability, and provides rationale for a few of the less transparent common vulnerabilities to explain why they are considered vulnerabilities.

Table 17 - Supplemental Information on Selected Common Vulnerabilities

Vulnerability Class and NISTIR 7628 Reference	Common Vulnerability	Supplemental Information
General Logic Error (6.3.1.7)	*alarm management system does not support required processing for legitimate alarm conditions*	Sub cases: • Inability to handle a legitimate high rate of alarms • Inability to handle certain types of important alarms due to incomplete upgrade • Inability to handle certain types of important alarms due to configuration change
Inadequate Anomaly Tracking (6.4.4.1)	*users lack visibility of unapproved access*	Sub case of: *Users lack visibility of threat activity*
Inadequate Change and Configuration Management (6.2.2.5)	*system permits unauthorized installation of software or firmware*	Sub cases: • system does not enforce authorization for installing software or firmware • easy to obtain new credentials that provide authorization for a specific function • method exists to bypass authentication/authorization process in place for installation of software or firmware

Vulnerability Class and NISTIR 7628 Reference	Common Vulnerability	Supplemental Information
	unauthorized firmware may be installed without detection	Sub case of: *system permits unauthorized changes*
Inadequate Malware Protection (6.4.2.3)	*system permits installation of malware*	Sub case of: *system permits unauthorized installation of software or firmware*
Inadequate Network Segregation (6.5.1.2)	*Internet connection may be misused by adversary*	Sub cases, connection may be used to: • exfiltrate information off the target network • to perform command and control of malware that has been placed on that network • to scan the target network for vulnerabilities.
Physical Access to the Device (6.5.1.6)	*physical access to mobile devices may enable logical access to business functions by unauthorized individuals*	Sub cases: • mobile device does not enforce authorization for logical access once physical access is obtained • method exists to bypass authentication/authorization process in place on the mobile device • theft of "logged in" device provides access
Unnecessary System Access (6.2.2.6)	*design permits unnecessary privileges*	Sub cases: • Any user login provides access to all available functions • Test ports, maintenance ports or monitoring ports on equipment always active, and/or usable by anyone (no authorization needed) • These ports support unnecessary functionality

Vulnerability Class and NISTIR 7628 Reference	Common Vulnerability	Supplemental Information
	remote access may be obtained by unauthorized individuals	Sub cases: • system does not enforce authorization for remote access • easy to obtain new credentials that provide authorization for remote access • method exists to bypass authentication/authorization process in place for remote access
	system permits networking components to be accessed by unauthorized individuals	Sub cases: • system does not enforce authorization for access to networking components • easy to obtain new credentials that provide authorization access to networking components • easy to obtain new credentials that provide authorization access to networking components • method exists to bypass authentication/authorization process in place for access to networking components

Vulnerability Class and NISTIR 7628 Reference	Common Vulnerability	Supplemental Information
	system permits wireless access by unauthorized parties	Sub cases: • system does not enforce authorization for wireless access • easy to obtain new or existing credentials that provide authorization for wireless access (for existing credentials, particularly due to weak cryptography used) • method exists to bypass authentication/authorization process in place for wireless access • theft of device provides wireless access
Use of Inadequate Security Architectures and Designs (6.4.1.1)	*system permits bypass of access control mechanisms*	Sub cases: • Via back doors • By using leftover default passwords • By using another layer (so application has good access control but not the database or the file system or the printer) • By finding same data where not protected as in backup or archive storage
	critical communication paths are not isolated from communication paths that require fewer protections to operate	Rationale: Isolation of critical communication paths permits independent design of appropriate protections for different communication paths. Less critical communication paths may support desired functionality, such as access to the Internet

Vulnerability Class and NISTIR 7628 Reference	Common Vulnerability	Supplemental Information
	critical functions are not isolated from those that require fewer protections to operate	Rationale: Isolation of critical functions permits independent design of appropriate protections for different functions, and stops the attacker from gaining access to more critical functions leveraging their access to less critical functions
Use of Insecure Protocols (6.3.1.21)	*commands or other messages may be inserted on the network by unauthorized individuals*	Rationale: An entity with logical access to the network may not have this vulnerability, because there could be an additional layer that creates a point to point secure link between the sender of messages and the receiver

Appendix G Additional Figures

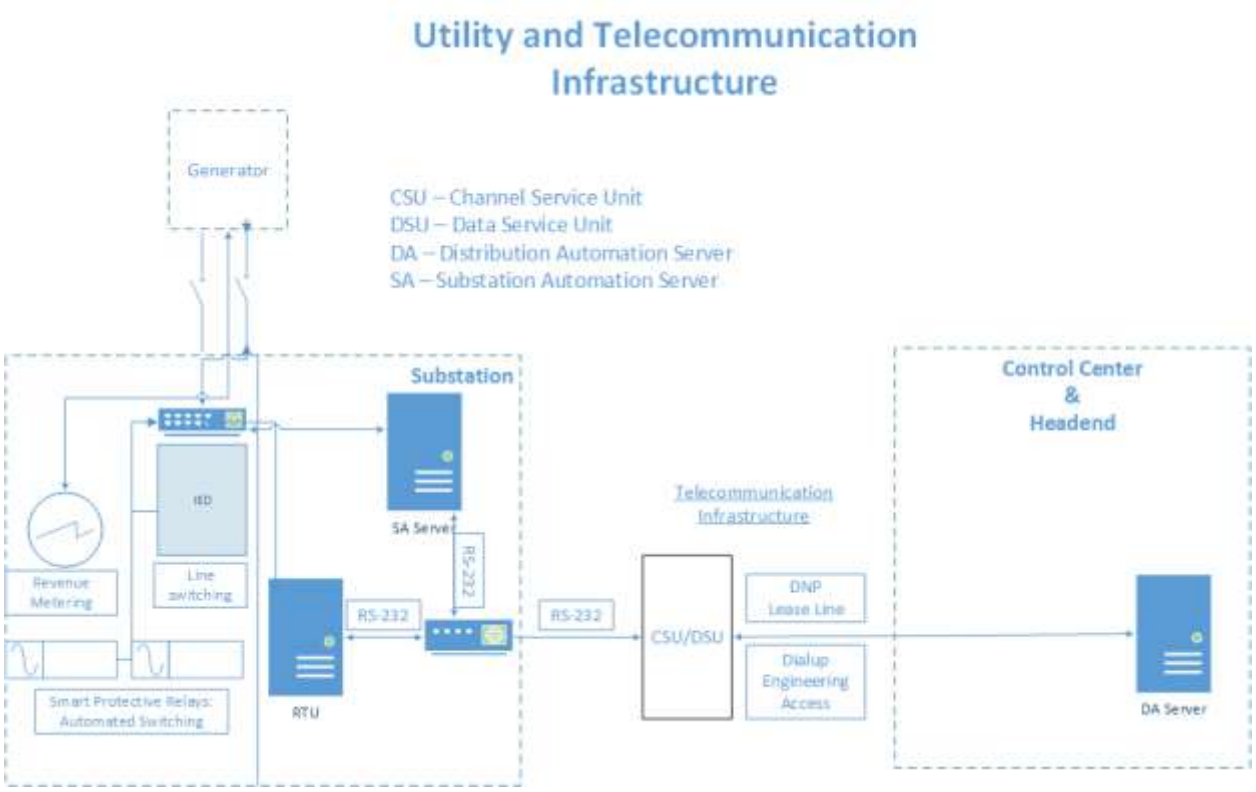


Figure 5. Threat agent compromises serial control link to substation (DGM.16)