Electric Sector Failure Scenarios Common Vulnerabilities and Mitigations Mapping

Version 1.0

June 2014

National Electric Sector Cybersecurity Organization Resource (NESCOR)

Technical Working Group 1

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, NOR ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THIS REPORT WAS PREPARED AS AN ACCOUNT OF WORK SPONSORED BY AN AGENCY OF THE UNITED STATES GOVERNMENT. NEITHER THE UNITED STATES GOVERNMENT NOR ANY AGENCY THEREOF, NOR ANY OF THEIR EMPLOYEES, MAKES ANY WARRANTY, EXPRESS OR IMPLIED, OR ASSUMES ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, APPARATUS, PRODUCT, OR PROCESS DISCLOSED, OR REPRESENTS THAT ITS USE WOULD NOT INFRINGE PRIVATELY OWNED RIGHTS. REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY THE UNITED STATES GOVERNMENT OR ANY AGENCY THEREOF. THE VIEWS AND OPINIONS OF AUTHORS EXPRESSED HEREIN DO NOT NECESSARILY STATE OR REFLECT THOSE OF THE UNITED STATES GOVERNMENT OR ANY AGENCY THEREOF.

THE FOLLOWING ORGANIZATION PREPARED THIS REPORT:

Electric Power Research Institute (EPRI

CONTENTS

LIST OF TABLES

1
INTRODUCTION

This document serves as a further reference for the National Electric Sector Cybersecurity Organization Resource (NESCOR) *Electric Sector Failure Scenarios and Impact Analyses version 2.0*, which was produced by the Electric Power Research Institute (EPRI) for the U.S. Department of Energy (DOE). That report, referred to hereafter as the Failure Scenarios, documents 113 different cybersecurity attack scenarios that could compromise Electric Sector systems. Each scenario includes a list of potential system vulnerabilities that could be exploited by an attacker, a list of impacts that could result from their exploitation, and a list of potential mitigations that could be used to prevent that exploitation.

Version 0.9 of the Failure Scenarios included the initial lists of vulnerabilities, impacts, and mitigations that were developed by Technical Working Group 1 (TWG1) of NESCOR. Those vulnerabilities and mitigations were written as unstructured English sentences. TWG1 recognized that consistency of terminology and structure within these lists would have several benefits, including improving document readability and enabling analyses of the Failure Scenarios. In particular, the team wanted to identify the *common vulnerabilities* and *common mitigations*. TWG1 devised a structured form for the vulnerabilities and mitigations that would support this goal, and used the same form for both lists:

Common vulnerability/mitigation followed by the vulnerability/mitigation context

That is, for each entry in the lists of vulnerabilities and mitigations, the common vulnerability or common mitigation appears first in italics, and is followed by the context in which it is used, in regular font. Structuring the vulnerabilities and mitigations in this way enabled TWG1 to identify which Failure Scenarios were subject to the same vulnerabilities and which Failure Scenarios could be mitigated in the same way.

Since version 0.9 of the Failure Scenarios, TWG1 has worked to normalize the list of vulnerabilities and mitigations according to this new form. The team identified and documented normalized mitigations in version 1.0 of the Failure Scenarios, and identified and documented normalized vulnerabilities in version 2.0. In addition, TWG1 grouped common vulnerabilities and common mitigations into larger classes to further support analysis of the failure scenarios. The common vulnerabilities were mapped to the Vulnerability Classes documented in the National Institute of Standards and Technology Interagency Report (NISTIR) Draft NISTIR 7628 Revision 1, *Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References*, while the common mitigations were mapped into larger classes defined by TWG1. The process and the analytical results are documented in more detail in the Failure Scenarios version 2.0.

This document is structured as follows:

- Appendix A includes the grouping of common vulnerabilities into NISTIR 7628 Vulnerability Classes,

- Appendix B includes the mapping of the original vulnerabilities in Failure Scenarios version 1.0 to common vulnerabilities in version 2.0,
- Appendix C includes the grouping of common mitigations into mitigation classes called mitigation action groups, defined by TWG1, and,
- Appendix D includes the mapping of the original mitigations in Failure Scenarios version 0.9 to common mitigations in version 1.0.

A
COMMON VULNERABILITIES AND VULNERABILITY CLASSES

The following table lists the common vulnerabilities appearing in version 2.0 of the Failure Scenarios, grouped into the Vulnerability Classes from the NISTIR 7628 Volume 3, along with the frequency of occurrence of that common vulnerability in all failure scenarios. In the first column, the number in parentheses following each Vulnerability Class name refers to the section number in NISTIR 7628 Volume 3 where the Vulnerability Class is described.

Table 1. Common Vulnerabilities by Class

Vulnerability Class	Common Vulnerability	Frequency
API Abuse (6.3.2.1)	presence of features or functions that may be misused by users	1
Business Logic Vulnerability (6.3.1.8)	critical operations are not locked out during maintenance	1
	inadequate criteria for determining which alarms deserve priority	1
	system assumes data inputs and resulting calculations are accurate	7
	system design limits opportunity for system recovery using reconfiguration	2
	system permits potentially harmful command sequences	3
	system takes action before confirming changes with user	3
Cryptographic Vulnerability (6.3.1.4)	cryptography used that employs algorithms that are breakable within a time period useful to the adversary	3
Error Handling Vulnerability (6.3.1.6)	system may become overwhelmed by traffic flooding or malformed traffic	1
	users lack visibility to the failure of the system to respond to commands	1
General Logic Error (6.3.1.7)	alarm management system does not support required processing for legitimate alarm conditions	1
	alarm processing capability is overwhelmed by unnecessary alarms	1
Inadequate Anomaly	users lack visibility of threat activity	9

Vulnerability Class	Common Vulnerability	Frequency
Tracking (6.4.4.1)	users lack visibility of unapproved access	5
Inadequate Change and Configuration Management (6.2.2.5)	configuration changes are not verified for correctness	4
	sensitive data remains on disposed equipment	1
	system permits unauthorized changes	39
	system permits unauthorized installation of software or firmware	5
	users lack visibility that unauthorized changes were made	9
	users lack visibility that unauthorized firmware has been installed	1
Inadequate Continuity of Operations or Disaster Recovery Plan (6.2.3.3)	emergency response policy, procedures, emergency response procedures unintentionally omit security controls"	1
	emergency situations may not have the appropriate replacement equipment, some of which require long lead times for repair or replacement	1
	inadequate continuity and recovery security architecture	1
Inadequate Incident Response Process (6.2.3.5)	speed of incident response process is not appropriate for incident	1
Inadequate Malware Protection (6.4.2.3)	system permits installation of malware	10
	the list of signatures used for detection of attacks is no longer current	2
Inadequate Network Segregation (6.5.1.2)	communication channels are shared between different system owners	1
	Internet connection may be misused by adversary	1
	network interconnections provide users and hardware/software entities with access unnecessary for their roles	3
	network interfaces permit unnecessary traffic flows	6
	network is connected to untrusted networks	2
	network services are shared between different system owners	1
	publicly accessible and/or third party controlled links used	5
Inadequate Patch Management Process (6.2.2.4)	software patches are not checked regularly to ensure that they are current	7

Vulnerability Class	Common Vulnerability	Frequency
	software patches may be applied without verifying continued system operation	1
Inadequate Periodic Security Audits (6.2.3.1)	adherence to policies and procedures degrades over time	1
	human error in adherence to policies and procedures	1
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	3
Insufficiently Trained Personnel (6.2.1.1)	workforce may be unaware of recommended precautions	3
	workforce not trained in proper procedures	1
Insufficient Redundancy (6.5.1.5)	critical components exhibit single point of failure	2
Physical Access to the Device (6.5.1.6)	enabled but unused ports	1
	physical access may be obtained by unauthorized individuals	18
	physical access to a serial port may enable logical access by unauthorized entities	1
	physical access to mobile devices may enable logical access to business functions by unauthorized individuals	3
Sensitive Data Protection Vulnerability (6.3.1.15)	system makes private data accessible to unauthorized individuals	5
Unnecessary System Access (6.2.2.6)	back doors for access are left in place	1
	default configuration allows access that is unnecessary after the system is operational	1
	design permits unnecessary privileges	2
	remote access may be obtained by unauthorized individuals	5
	system permits bypass of physical access controls	1
	system permits networking components to be accessed by unauthorized individuals	1
	system permits wireless access by unauthorized parties	2
	unnecessary access is permitted to critical functions	2
	unnecessary access is permitted to networking components	1
	unnecessary access is permitted to system functions	8

Vulnerability Class	Common Vulnerability	Frequency
	unnecessary access is permitted to the communications channel	4
	unnecessary access is permitted to the database	5
	unnecessary access is permitted to the operating system	3
	unnecessary network access is permitted	13
	users and hardware/software entities are given access unnecessary for their roles	2
Unneeded Services Running (6.4.3.2)	unnecessary system services are configured to run	4
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	1
	critical functions are not isolated from those that require fewer protections to operate	1
	design, implementation, security design does not consider the system lifecycle"	1
	system permits bypass of access control mechanisms	2
	system permits device identifier to be misused	4
	weaker security architecture at backup sites	1
Use of Insecure Protocols (6.3.1.21)	a copy of a prior alarm is difficult or infeasible to distinguish from a new legitimate alarm	1
	a copy of a prior message or command is difficult or infeasible to distinguish from a new legitimate message or command	5
	commands or other messages may be inserted on the network by unauthorized individuals	3
	message modified by an adversary is either difficult or infeasible to distinguish from a valid message	14
	spoofed signal is either difficult or infeasible to distinguish from a legitimate signal	1
	system makes messages accessible to unauthorized individuals	9
	system permits messages to be modified by unauthorized individuals	11
	system relies on communications that are easy to jam	2
Weaknesses in Authentication Process or	credentials are accessible in the clear	1
	default password is not changed	1
	encryption keys are shared	3

Vulnerability Class	Common Vulnerability	Frequency
Authentication Keys (6.5.1.4)	inadequate binding of meter with energy users authorized to charge to that meter	1
	secret key is stored or transmitted in the clear	3
	shared credentials are used for access	2
	system relies on credentials that are easy to obtain for access	46

B
MAPPING OF ORIGINAL VULNERABILITIES TO COMMON VULNERABILITIES

The following table documents how each failure scenario vulnerability was rewritten in the new common vulnerabilities form. The first column ("Failure Scenario") lists the Failure Scenario number. The second column ("Original Vulnerability") contains the vulnerability as written in version 1.0 of the Failure Scenarios. The third column ("Common Vulnerability") and the fourth column ("Vulnerability Context") comprise the revised vulnerability as presented in version 2.0 of the Failure Scenarios. For example, in AMI.1, "Inadequate system and process checks for disconnect commands" was replaced with "System permits potentially harmful command sequences such as a sufficiently large number of disconnects that may threaten system balance." The fifth column ("Vulnerability Class") repeats information provided in Appendix A, as a convenience.

Table 2. Mapping of Original Vulnerabilities to Common Vulnerabilities

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
ami.1	Inadequate system and process checks for disconnect commands.	system permits potentially harmful command sequences	such as a sufficiently large number of disconnects that may threaten system balance.	Business Logic Vulnerability (6.3.1.8)
ami.2	Inadequate controls on software installation, configuration, and integrity,	system permits unauthorized changes	to Meter Data Management System (MDMS) user billing data,	Inadequate Change and Configuration Management (6.2.2.5)
ami.2	Inadequate auditing for financial discrepancies.	system assumes data inputs and resulting calculations are accurate	for customer energy billing calculations in the Meter Data Management System (MDMS),	Business Logic Vulnerability (6.3.1.8)
ami.2	Inadequate controls on software installation, configuration, and integrity,	system permits installation of malware	on the MDMS	Inadequate Malware Protection (6.4.2.3)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
ami.3	Inadequate controls on software installation and integrity,	system permits installation of malware	on the utility enterprise network or AMI implementation,	Inadequate Malware Protection (6.4.2.3)
ami.3	Inadequately protected Internet access to 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,	Inadequate Network Segregation (6.5.1.2)
ami.3	Inadequate identity and access control management (physical and logical).	physical access may be obtained by unauthorized individuals	to the utility enterprise network or AMI implementation.	Physical Access to the Device (6.5.1.6)
ami.3	Inadequate identity and access control management (physical and logical).	system relies on credentials that are easy to obtain for access	to the utility enterprise network or AMI implementation.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.4	Weak or no cryptography on the internal bus,	secret key is stored or transmitted in the clear	while in transit on the internal bus of a meter,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.4	Wide use of the same symmetric key.	encryption keys are shared	by multiple meters in an AMI implementation.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.5	Wide use of the same symmetric key,	encryption keys are shared	by multiple meters in an AMI implementation.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
ami.5	Insecure key storage on the meter,	secret key is stored or transmitted in the clear	on the meter.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.5	Inadequate protection of keys during distribution.	secret key is stored or transmitted in the clear	during transit to the meter during key distribution.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.6	Weak or no authentication or authorization controls for privilege to install firmware or software,	system relies on credentials that are easy to obtain for access	for privileges to install firmware or software on a smart meter,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.6	No capability to detect installation of unauthorized firmware or software in a meter.	system permits unauthorized installation of software or firmware	on a smart meter.	Inadequate Change and Configuration Management (6.2.2.5)
ami.7	Unsecured access to interfaces on the device that permit modifying device functionality,	physical access may be obtained by unauthorized individuals	via the smart meter interfaces which can permit modifying device functionality,	Physical Access to the Device (6.5.1.6)
ami.7	Presence of features and functions that may be used in a manner not intended by the designers of the device.	presence of features or functions that may be misused by users	in a manner not intended by the designers of the smart meter.	API Abuse (6.3.2.1)
ami.8	Insufficient integrity protection for the path used for receipt of tamper alarms (allowing modification and insertion of messages to create or replay alarms),	a copy of a prior alarm is difficult or infeasible to distinguish from a new legitimate alarm	along the path used for receipt of tamper alarms,	Use of Insecure Protocols (6.3.1.21)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
ami.8	Legitimate alarm management is not appropriate for handling the maximum number of possible alarms,	alarm management system does not support required processing for legitimate alarm conditions	in the AMI system,	General Logic Error (6.3.1.7)
ami.8	Alarms are sent too often or are not appropriately aggregated.	alarm processing capability is overwhelmed by unnecessary alarms	in the alarm management component of the AMI system	General Logic Error (6.3.1.7)
ami.8	Alarms are sent too often or are not appropriately aggregated.	inadequate criteria for determining which alarms deserve priority	in the alarm management component of the AMI system	Business Logic Vulnerability (6.3.1.8)
ami.9	Use of credentials that are easy to social engineer,	system relies on credentials that are easy to obtain for access	(via social engineering) in the AMI system,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.9	Workforce unaware of social engineering techniques,	workforce may be unaware of recommended precautions	to prevent social engineering attacks,	Insufficiently Trained Personnel (6.2.1.1)
ami.9	Single-factor authentication for disconnect,	system relies on credentials that are easy to obtain for access	for a meter disconnect command (single-factor authentication),	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.9	Inadequate network segmentation and perimeter protection.	network interconnections provide users and hardware/software entities with access unnecessary for their roles	from remote networks to network containing the AMI system	Inadequate Network Segregation (6.5.1.2)
ami.10	Inadequate protection of enterprise boundary,	network interconnections provide users and hardware/software entities with access unnecessary for their roles	at the enterprise boundary	Inadequate Network Segregation (6.5.1.2)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
ami.10	Weak authentication for access to pricing change functions,	system relies on credentials that are easy to obtain for access	to pricing change functions,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.10	Inadequate control of credentials, privileges or accounts required to make TOU pricing changes,	system permits unauthorized changes	to accounts required to make TOU pricing changes,	Inadequate Change and Configuration Management (6.2.2.5)
ami.10	Lack of review for major price changes.	configuration changes are not verified for correctness	in pricing data (e.g., TOU pricing).	Inadequate Change and Configuration Management (6.2.2.5)
ami.11	Insufficient integrity protection of the path used to receive last gasp messages (able to insert, modify, and/or replay messages).	system permits messages to be modified by unauthorized individuals	in the path used to receive last gasp messages	Use of Insecure Protocols (6.3.1.21)
ami.11	Insufficient integrity protection of the path used to receive last gasp messages (able to insert, modify, and/or replay 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	Use of Insecure Protocols (6.3.1.21)
ami.11	Insufficient integrity protection of the path used to receive last gasp messages (able to insert, modify, and/or replay 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	Use of Insecure Protocols (6.3.1.21)
ami.12	Inadequate controls on firewall changes,	system permits unauthorized changes	to the firewall	Inadequate Change and Configuration Management (6.2.2.5)
ami.12	Weak application/system authentication,	system relies on credentials that are easy to obtain for access	to the database	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
ami.12	Weak database security configuration,	default configuration allows access that is unnecessary after the system is operational	This allows unnecessary access to the database	Unnecessary System Access (6.2.2.6)
ami.12	Lack of protection mechanisms and situational awareness (security information and event management (SIEM), intrusion detection system (IDS), firewalls, logging, and monitoring).	users lack visibility of threat activity	in the AMI system	Inadequate Anomaly Tracking (6.4.4.1)
ami.13	Poor user interface design/feedback and authentication,	system permits bypass of access control mechanisms	when the user has physical access to the console	Use of Inadequate Security Architectures and Designs (6.4.1.1)
ami.13	Inadequate physical security,	physical access may be obtained by unauthorized individuals	at an unattended user console	Physical Access to the Device (6.5.1.6)
ami.13	Unattended live console due to inadequate security procedure or training.	workforce may be unaware of recommended precautions	when leaving consoles unattended and unlocked	Insufficiently Trained Personnel (6.2.1.1)
ami.14	Inadequate separation of private leased networks (commercial mobile, utility leased),	publicly accessible and/or third party controlled links used	(e.g., commercial mobile, utility leased)	Inadequate Network Segregation (6.5.1.2)
ami.14	Weak or no cryptography,	cryptography used that employs algorithms that are breakable within a time period useful to the adversary		Cryptographic Vulnerability (6.3.1.4)
ami.14	Replay ability for commands.	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	Use of Insecure Protocols (6.3.1.21)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
ami.15	Inadequate cyber security mitigations implemented in backup sites and in business continuity and disaster recovery planning and procedures.	weaker security architecture at backup sites		Use of Inadequate Security Architectures and Designs (6.4.1.1)
ami.15	Inadequate cyber security mitigations implemented in backup sites and in business continuity and disaster recovery planning and procedures.	inadequate continuity and recovery security architecture	used in business continuity and disaster recovery planning and procedures.	Inadequate Continuity of Operations or Disaster Recovery Plan (6.2.3.3)
ami.16	Inadequate protections in the key generation and/or distribution process,	cryptography used that employs algorithms that are breakable within a time period useful to the adversary	for protection of the private CA key,	Cryptographic Vulnerability (6.3.1.4)
ami.16	Lack of full lifecycle security design at the headend.	security design does not consider the system lifecycle	in the headend.	Use of Inadequate Security Architectures and Designs (6.4.1.1)
ami.17	Insufficient integrity protection for routing mechanisms in the cellular network,	system permits unauthorized changes	in the routing mechanisms of the cellular network,	Inadequate Change and Configuration Management (6.2.2.5)
ami.17	Inadequate authentication to reconfigure the AMI network.	system relies on credentials that are easy to obtain for access	for reconfiguration of the AMI network.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.18	Weak or no authentication required for access to the HAN,	system relies on credentials that are easy to obtain for access	to the HAN,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.18	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	Inadequate Network Segregation (6.5.1.2)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
			center.	
ami.19	Using only time-stamping for replay attack protection,	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,	Use of Insecure Protocols (6.3.1.21)
ami.19	Poor time synchronization or time synchronization susceptible to tampering.	system permits unauthorized changes	to the time synchronization between meters and the AMI headend,	Inadequate Change and Configuration Management (6.2.2.5)
ami.19	Poor time synchronization or time synchronization susceptible to tampering.	system permits unauthorized changes	to timestamps on meter commands from the AMI headend.	Inadequate Change and Configuration Management (6.2.2.5)
ami.20	Inadequate checks in the TOU pricing implementation.	system permits unauthorized changes	to the TOU pricing implementation.	Inadequate Change and Configuration Management (6.2.2.5)
ami.21	Lack of physical controls and access controls for mobile platforms.	physical access to mobile devices may enable logical access to business functions by unauthorized individuals	to software components of the AMI infrastructure.	Physical Access to the Device (6.5.1.6)
ami.22	Wireless access to the public,	system permits wireless access by unauthorized parties	to the wireless network used to control an AMI device,	Unnecessary System Access (6.2.2.6)
ami.22	Weak or no authentication for privileged functionality.	system relies on credentials that are easy to obtain for access	to the web-based administration page used to control an AMI device.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
ami.23	Hardcoded passwords,	system relies on credentials that are easy to obtain for access	to AMI devices (hardcoded passwords),	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.23	Shared passwords and credentials.	shared credentials are used for access	to AMI devices.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.24	Implementation of weak or unapproved cryptography.	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.	Cryptographic Vulnerability (6.3.1.4)
ami.25	Improper or no change/configuration management for the timely deployment of patches and security updates.	software patches are not checked regularly to ensure that they are current	in the AMI devices and headend system.	Inadequate Patch Management Process (6.2.2.4)
ami.26	Lack of authentication between cards and a meter,	system assumes data inputs and resulting calculations are accurate	on smartcards inserted into a meter,	Business Logic Vulnerability (6.3.1.8)
ami.26	Lack of integrity protections on cards and meters for data and applications.	system permits unauthorized changes	to AMI billing information on smartcards.	Inadequate Change and Configuration Management (6.2.2.5)
ami.27	Back doors and unprotected interfaces (used during development for testing, development, monitoring or maintenance purposes)are deployed in production equipment.	design permits unnecessary privileges	such as unprotected interfaces used for development, testing, monitoring or maintenance purposes that remain in production equipment.	Unnecessary System Access (6.2.2.6)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
ami.27	Back doors and unprotected interfaces (used during development for testing, development, monitoring or maintenance purposes)are deployed in production equipment.	back doors for access are left in place	for AMI equipment.	Unnecessary System Access (6.2.2.6)
ami.28	Inadequate testing in realistic environment for large footprint operation.	software patches may be applied without verifying continued system operation	in the realistic environment of a large footprint operation.	Inadequate Patch Management Process (6.2.2.4)
ami.29	Weak or no authentication required for HAN access.	system relies on credentials that are easy to obtain for access	to the HAN.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.30	Weak or no authentication or authorization controls for privilege to install firmware,	system relies on credentials that are easy to obtain for access	to install firmware on the meter,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.30	No capability to detect unauthorized firmware in a meter.	system permits installation of malware	on a meter.	Inadequate Malware Protection (6.4.2.3)
ami.31	Weak or no authentication or authorization controls for privilege to install firmware,	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,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.31	No capability to detect unauthorized firmware in a meter.	system permits unauthorized installation of software or firmware	such as the propagation of unauthorized firmware to meters by a compromised headend system	Inadequate Change and Configuration Management (6.2.2.5)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
ami.32	Inadequate background checks on employees to avoid insider threats,	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,	Insufficient Identity Validation or Background Checks (6.2.2.1)
ami.32	Weak credentials needed to change the meter settings,	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),	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
ami.32	Inadequate protection of the configuration that determines how power consumption is recorded,	system permits unauthorized changes	to the configuration that determines how power consumption is recorded,	Inadequate Change and Configuration Management (6.2.2.5)
ami.32	Inadequate protection of the password on field tool or third party installations of software that can reconfigure meters.	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.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.1	Lack of access control,	physical access may be obtained by unauthorized individuals	to DER settings through the DER system user interface	Physical Access to the Device (6.5.1.6)
der.1	Lack of mandatory change from default password,	default password is not changed	for the DER system	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
der.1	Poor configuration design of the DER system that permits unauthorized changes to anti-islanding protection,	system permits unauthorized changes	to anti-islanding protection in the DER system due to poor configuration design,	Inadequate Change and Configuration Management (6.2.2.5)
der.1	Insecure communication protocol between the user interface and the DER system that allows unauthenticated changes to sensitive parameters.	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.	Use of Insecure Protocols (6.3.1.21)
der.2	The DER system is connected to non-authorized networks,	network is connected to untrusted networks	specifically the DER operational network is connected to the company's wireless corporate network,	Inadequate Network Segregation (6.5.1.2)
der.2	Weak or absent authentication on the wireless network allows an unauthorized entity to gain control of DER system through the Internet,	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,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.2	The wireless network allows systems to join without appropriate authorization,	system permits wireless access by unauthorized parties	to the wireless network in the DER system,	Unnecessary System Access (6.2.2.6)
der.2	The DER system does not have adequate access control to prevent unauthorized access by threat agents,	unnecessary access is permitted to system functions	in the DER system,	Unnecessary System Access (6.2.2.6)
der.2	The utility commands do not indicate failure of the DER system to respond.	users lack visibility to the failure of the system to respond to commands	by the utility for the DER system.	Error Handling Vulnerability (6.3.1.6)
der.3	Inadequate personnel security control procedures in the vendor factory or during implementation,	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,	Insufficient Identity Validation or Background Checks (6.2.2.1)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
der.3	Inadequate validation of software/firmware,	system permits unauthorized installation of software or firmware	in DER equipment,	Inadequate Change and Configuration Management (6.2.2.5)
der.3	Inadequate authentication and access control to critical security functions,	system relies on credentials that are easy to obtain for access	to modify software or firmware on systems post-delivery,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.3	Inadequate testing of all DER functions.	system permits unauthorized installation of software or firmware	in the DER system.	Inadequate Change and Configuration Management (6.2.2.5)
der.4	The communication protocol does not provide adequate confidentiality,	system makes messages accessible to unauthorized individuals	in the communication protocol of the DER system,	Use of Insecure Protocols (6.3.1.21)
der.4	The communication protocol does not detect or alert when information has been intercepted.	system makes private data accessible to unauthorized individuals	in the communication protocol of the DER system.	Sensitive Data Protection Vulnerability (6.3.1.15)
der.5	The supply chain does not detect embedded malware.	system permits installation of malware	in the supply chain for the DER system	Inadequate Malware Protection (6.4.2.3)
der.6	Application-to-application messaging scheme does not protect against changing the sequence of commands,	system permits potentially harmful command sequences	in the application-to-application messaging scheme of the DER storage system,	Business Logic Vulnerability (6.3.1.8)
der.6	Communication protocol does not protect against replay attacks (either through no security or inadequate security).	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.	Use of Insecure Protocols (6.3.1.21)
der.7	The time synchronization communication protocol does not adequately authenticate messages or ensure their integrity,	system permits messages to be modified by unauthorized individuals	in the time synchronization communication protocol,	Use of Insecure Protocols (6.3.1.21)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
der.7	The time synchronization communication protocol does not adequately authenticate messages or ensure their integrity,	message modified by an adversary is either difficult or infeasible to distinguish from a valid message	in the time synchronization communication protocol,	Use of Insecure Protocols (6.3.1.21)
der.7	The DER system does not notify or request confirmation of changes from the utility DER management system before taking actions.	system takes action before confirming changes with user	in the DER management system.	Business Logic Vulnerability (6.3.1.8)
der.8	The communication protocol used to issue the curtailing command lacks non-repudiation.	system permits unauthorized changes	to instructions received from the utility regarding permitted charging operations.	Inadequate Change and Configuration Management (6.2.2.5)
der.9	Lack of message authentication.	system permits messages to be modified by unauthorized individuals		Use of Insecure Protocols (6.3.1.21)
der.9	Lack of message authentication.	message modified by an adversary is either difficult or infeasible to distinguish from a valid message		Use of Insecure Protocols (6.3.1.21)
der.10	Inadequate access control for critical settings in FDEMS,	system permits unauthorized changes	to critical settings in FDEMS,	Inadequate Change and Configuration Management (6.2.2.5)
der.10	Inadequate logical access control for the FDEMS network and operating system,	unnecessary network access is permitted	to the FDEMS network,	Unnecessary System Access (6.2.2.6)
der.10	Inadequate logical access control for the FDEMS network and operating system,	unnecessary access is permitted to the operating system	hosting the FDEMS applications,	Unnecessary System Access (6.2.2.6)
der.10	Inadequate physical access control to the FDEMS system.	physical access may be obtained by unauthorized individuals	to the FDEMS system.	Physical Access to the Device (6.5.1.6)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
der.10		system relies on credentials that are easy to obtain for access	to the FDEMS network,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.10		system relies on credentials that are easy to obtain for access	that allows modification of the FDEMS settings,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.11	Inadequate logical access control for the FDEMS network and operating system,	unnecessary network access is permitted	to the FDEMS network,	Unnecessary System Access (6.2.2.6)
der.11	Inadequate logical access control for the FDEMS network and operating system,	unnecessary access is permitted to the operating system	hosting the FDEMS applications,	Unnecessary System Access (6.2.2.6)
der.11	Inadequate physical access control for the FDEMS system,	physical access may be obtained by unauthorized individuals	to the FDEMS system,	Physical Access to the Device (6.5.1.6)
der.11	Inadequate protection in the FDEMS against shut downs of DER systems,	system takes action before confirming changes with user	to shutdown DER systems in the FDEMS,	Business Logic Vulnerability (6.3.1.8)
der.11		system relies on credentials that are easy to obtain for access	to the FDEMS network	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.11		system relies on credentials that are easy to obtain for access	that allows modification of the FDEMS software	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
der.12	Inadequate access control for critical settings in FDEMS,	unnecessary access is permitted to critical functions	that modify critical settings in the FDEMS,	Unnecessary System Access (6.2.2.6)
der.12	Inadequate logical access control for the FDEMS network and operating system,	unnecessary network access is permitted	for the FDEMS network,	Unnecessary System Access (6.2.2.6)
der.12	Inadequate logical access control for the FDEMS network and operating system,	unnecessary access is permitted to the operating system	hosting the FDEMS applications,	Unnecessary System Access (6.2.2.6)
der.12	Inadequate physical access control to the FDEMS system,	physical access may be obtained by unauthorized individuals	to the FDEMS system,	Physical Access to the Device (6.5.1.6)
der.12		system relies on credentials that are easy to obtain for access	to the FDEMS network	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.12		system relies on credentials that are easy to obtain for access	that allows modificatio of the FDEMS settings	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.13	Unauthorized personnel in the supply chain, installation organization or maintenance organization have physical access to embedded equipment and can install malware,	physical access may be obtained by unauthorized individuals	to embedded equipment in the supply chain, installation organization or maintenance organization,	Physical Access to the Device (6.5.1.6)
der.13	The FDEMS accesses (and is thereby accessible to) the Internet through uncontrolled interface(s), allowing for Internet-based malware delivery mechanisms.	network interfaces permit unnecessary traffic flows	between the FDEMS and the Internet, allowing for Internet-based malware delivery mechanisms,	Inadequate Network Segregation (6.5.1.2)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
der.13	Unauthorized personnel in the supply chain, installation organization or maintenance organization have physical access to embedded equipment and can install malware,	software patches are not checked regularly to ensure that they are current	permitting compromise of the FDEMS platform,	Inadequate Patch Management Process (6.2.2.4)
der.13		system relies on credentials that are easy to obtain for access	to install software on the FDEMS platform	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.14	Inadequate authentication mechanisms used by DER SCADA communication protocols,	system permits messages to be modified by unauthorized individuals	in the DER SCADA communication protocols,	Use of Insecure Protocols (6.3.1.21)
der.14	Inadequate authentication mechanisms used by 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,	Use of Insecure Protocols (6.3.1.21)
der.14	Inadequate network and system management to detect intrusions,	users lack visibility of threat activity	specifically messages sent to DER systems but not originated by the SCADA system,	Inadequate Anomaly Tracking (6.4.4.1)
der.14	Inadequate access control applied to the DER 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.	Unnecessary System Access (6.2.2.6)
der.15	Inadequate data source authentication employed by the DER SCADA communication protocols,	system permits unauthorized changes	to load value data in the DER SCADA communication protocols,	Inadequate Change and Configuration Management (6.2.2.5)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
der.15	Missing consistency checking between load value and meter values.	system assumes data inputs and resulting calculations are accurate	between load value and meter values.	Business Logic Vulnerability (6.3.1.8)
der.15		message modified by an adversary is either difficult or infeasible to distinguish from a valid message	in the DER SCADA communication protocols	Use of Insecure Protocols (6.3.1.21)
der.15		users lack visibility of threat activity	specifically adversary presence on the network capable of intercepting and modifying messages.	Inadequate Anomaly Tracking (6.4.4.1)
der.16	Inadequate authentication and access control mechanisms.	system permits potentially harmful command sequences	in particular issuance of commands with unknown impact on the DER systems,	Business Logic Vulnerability (6.3.1.8)
der.16		system permits unauthorized changes	to SCADA application data or software that allows the DER SCADA system to send invalid commands to DER systems,	Inadequate Change and Configuration Management (6.2.2.5)
der.16		system relies on credentials that are easy to obtain for access	to the SCADA DER system,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.17	Inadequate authentication and access control applied to the DERMS system,	system relies on credentials that are easy to obtain for access	to the DERMS system,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
der.17	Lack of adequate protection against manipulation of the software application and configuration data that provides DERMS power flow analysis functionality.	system assumes data inputs and resulting calculations are accurate	in the software application and configuration data that provides DERMS power flow analysis functionality.	Business Logic Vulnerability (6.3.1.8)
der.17		system permits unauthorized changes	to the DERMS system power flow analysis function	Inadequate Change and Configuration Management (6.2.2.5)
der.18	Inadequate access control applied to the DERMS system,	unnecessary access is permitted to system functions	in the DERMS system,	Unnecessary System Access (6.2.2.6)
der.18	Lack of protection against changes to utility permissions for microgrid disconnect,	system permits unauthorized changes	to utility permissions for microgrid disconnect,	Inadequate Change and Configuration Management (6.2.2.5)
der.18	Lack of message authentication and message integrity.	system permits messages to be modified by unauthorized individuals	to convey a command to modify utility permission for microgrid disconnect,	Use of Insecure Protocols (6.3.1.21)
der.18	Lack of message authentication and message integrity.	message modified by an adversary is either difficult or infeasible to distinguish from a valid message		Use of Insecure Protocols (6.3.1.21)
der.19	Inadequate authentication mechanisms used by the DERMS communication protocols to access the FDEMS	system relies on credentials that are easy to obtain for access	to modify the DERMS settings, when communicating using the FDEMS to DERMS protocol,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.19	Inadequate access control applied to the DERMS system,	unnecessary access is permitted to system functions	in the DERMS system that modify settings that impact individual DER systems,	Unnecessary System Access (6.2.2.6)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
der.19	Lack of message authentication and message integrity for the DERMS data accessed from remote locations,	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,	Use of Insecure Protocols (6.3.1.21)
der.19	Lack of message authentication and message integrity for the DERMS data accessed from remote locations,	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,	Use of Insecure Protocols (6.3.1.21)
der.19	Lack of detection for unauthorized changes to DERMS functions.	users lack visibility that unauthorized changes were made	to DERMS functions.	Inadequate Change and Configuration Management (6.2.2.5)
der.20	Inadequate authentication and access control applied to the DERMS system,	system relies on credentials that are easy to obtain for access	to the DERMS system,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.20	Lack of message authentication and message integrity protection for the DERMS data accessed from remote locations,	system permits messages to be modified by unauthorized individuals	for the DERMS data access from remote locations,	Use of Insecure Protocols (6.3.1.21)
der.20	Lack of message authentication and message integrity protection for the DERMS data accessed 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,	Use of Insecure Protocols (6.3.1.21)
der.20	Lack of detection of unauthorized changes to DERMS data.	users lack visibility that unauthorized changes were made	to DERMS data.	Inadequate Change and Configuration Management (6.2.2.5)
der.21	Inadequate access control applied to the DERMS system,	unnecessary access is permitted to system functions	in the DERMS system,	Unnecessary System Access (6.2.2.6)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
der.21	Lack of confidentiality protection for confidential data at rest.	system makes private data accessible to unauthorized individuals	while at rest.	Sensitive Data Protection Vulnerability (6.3.1.15)
der.21		system relies on credentials that are easy to obtain for access	to customer DER registration information	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.23	Lack of authentication and access control mechanisms in the DER system.	system relies on credentials that are easy to obtain for access	to the DER system	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.24	Inadequate storage of private information for customers	system makes private data accessible to unauthorized individuals	while in storage,	Sensitive Data Protection Vulnerability (6.3.1.15)
der.24	Inadequate authentication and access control mechanisms used by DERMS communication protocols to REP systems,	system relies on credentials that are easy to obtain for access	to read private DER data, when communicating using the REP to DERMS protocol	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
der.24	Inadequate authentication and access control mechanisms used by DERMS communication protocols to REP systems,	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,	Use of Insecure Protocols (6.3.1.21)
der.24	Inadequate access control mechanisms applied to the REPs.	unnecessary access is permitted to system functions	in the DERMS.	Unnecessary System Access (6.2.2.6)
der.25	Inadequate authentication and access control mechanisms to the DER management system,	system relies on credentials that are easy to obtain for access	to the DER management system,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
der.25	Lack of processes to validate the level of trustworthiness of the data from the REP.	system assumes data inputs and resulting calculations are accurate	in the data from the REP.	Business Logic Vulnerability (6.3.1.8)
der.26	Utility is unable to authenticate the source and content of status messages from the microgrid.	system permits messages to be modified by unauthorized individuals	(e.g., status messages from the microgrid).	Use of Insecure Protocols (6.3.1.21)
der.26	Utility is unable to authenticate the source and content of 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).	Use of Insecure Protocols (6.3.1.21)
wampac.1	Insufficient protection of network hosting the PTP server,	network interfaces permit unnecessary traffic flows	for the network hosting the PTP server,	Inadequate Network Segregation (6.5.1.2)
wampac.1	Inadequate PTP server configuration allowing unnecessary services to run on the PTP server,	unnecessary system services are configured to run	on the PTP server	Unneeded Services Running (6.4.3.2)
wampac.1	Inadequate robustness of the network stack, PTP implementation or required auxiliary services against flooding or malformed traffic,	system may become overwhelmed by traffic flooding or malformed traffic	because of deficiencies in the network stack, PTP implementation or required auxiliary services,	Error Handling Vulnerability (6.3.1.6)
wampac.1	Inadequate/lack of access control to the PTP service.	unnecessary access is permitted to critical functions	in the PTP service.	Unnecessary System Access (6.2.2.6)
wampac.2	Inadequate access control applied allowing unauthorized access to networking devices,	unnecessary access is permitted to networking components	for WAMPAC networking devices,	Unnecessary System Access (6.2.2.6)
wampac.2	Use of standard industry-wide WAMPAC protocols in an insecure fashion (such as IEEE C37.118 which has no built-in security capabilities),	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),	Use of Insecure Protocols (6.3.1.21)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
wampac.2	Use of standard industry-wide WAMPAC protocols in an insecure fashion (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),	Use of Insecure Protocols (6.3.1.21)
wampac.2	Use of standard industry-wide WAMPAC protocols in an insecure fashion (such as IEEE C37.118 which has no built-in security capabilities),	commands or other messages may be inserted on the network by unauthorized individuals	in the standard industry-wide WAMPAC protocols (such as IEEE C37.118 which has no built-in security capabilities),	Use of Insecure Protocols (6.3.1.21)
wampac.2	Lack of authentication mechanisms for the network components (e.g., routers, switches, etc.),	system permits networking components to be accessed by unauthorized individuals	(e.g., routers, switches, etc.),	Unnecessary System Access (6.2.2.6)
wampac.2	Lack of patch management on the network components (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.).	Inadequate Patch Management Process (6.2.2.4)
wampac.3	Firewalls nonexistent or improperly configured allowing access for an unauthorized insider to the PDC,	network interfaces permit unnecessary traffic flows	to the PDC,	Inadequate Network Segregation (6.5.1.2)
wampac.3	Weak network security architecture allowing access to the PDC,	design permits unnecessary privileges	to the PDC,	Unnecessary System Access (6.2.2.6)
wampac.3	No security monitoring on the WAMPAC network,	users lack visibility that unauthorized changes were made	to the PDC configuration,	Inadequate Change and Configuration Management (6.2.2.5)
wampac.3	Inadequate authentication and access control for configuration and programming software on the PDC,	system relies on credentials that are easy to obtain for access	to configuration and programming software on the PDC,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
wampac.3	Insecure remote access to the PDC,	remote access may be obtained by unauthorized individuals	to the PDC,	Unnecessary System Access (6.2.2.6)
wampac.4	Authentication database hosted on a poorly protected network,	unnecessary network access is permitted	on the network hosting the authentication database,	Unnecessary System Access (6.2.2.6)
wampac.4	Credentials not protected from disclosure while in transit or a rest,	credentials are accessible in the clear	while in transit or at rest,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
wampac.4	Access control enforcement mechanism that can be bypassed,	system permits bypass of access control mechanisms		Use of Inadequate Security Architectures and Designs (6.4.1.1)
wampac.4	Access and modification of the PDC/PMU configuration, which may include connection information	system permits unauthorized changes	to the PDC/PMU configuration, which may include connection information	Inadequate Change and Configuration Management (6.2.2.5)
wampac.5	Inadequate authentication and access control for configuration and programming software on the phasor gateway,	system relies on credentials that are easy to obtain for access	to configuration and programming software on the phase gateway,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
wampac.5	Inadequate testing of configuration changes without involving a verification and approval process,	configuration changes are not verified for correctness		Inadequate Change and Configuration Management (6.2.2.5)
wampac.5	Insecure remote access to the phasor gateway,	remote access may be obtained by unauthorized individuals	to the phasor gateway,	Unnecessary System Access (6.2.2.6)
wampac.5	Lack of redundancy for critical components such as phasor gateways.	critical components exhibit single point of failure	such as phasor gateways.	Insufficient Redundancy (6.5.1.5)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
wampac.6	Weak network security architecture allowing unauthorized access to the network components,	unnecessary network access is permitted	to network components	Unnecessary System Access (6.2.2.6)
wampac.6	No security monitoring on the WAMPAC network,	users lack visibility of threat activity	specifically unexpected access to network components or unusual traffic on the network	Inadequate Anomaly Tracking (6.4.4.1)
wampac.6	WAMPAC network accessible with weak or no credentials.	system relies on credentials that are easy to obtain for access	to the WAMPAC network.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
wampac.7	Firewalls nonexistent or improperly configured allowing access to the historian,	network interfaces permit unnecessary traffic flows	to the historian,	Inadequate Network Segregation (6.5.1.2)
wampac.7	Weak network security architecture allowing access to the historian,	unnecessary network access is permitted	allowing access to the historian,	Unnecessary System Access (6.2.2.6)
wampac.7	No security monitoring on the WAMPAC network,	users lack visibility of unapproved access	on the WAMPAC network,	Inadequate Anomaly Tracking (6.4.4.1)
wampac.7	No security monitoring of the WAMPAC historian database,	users lack visibility that unauthorized changes were made	to the WAMPAC historian database,	Inadequate Change and Configuration Management (6.2.2.5)
wampac.7	Inadequate authentication and access control for configuration and programming software on the historian,	system relies on credentials that are easy to obtain for access	to configuration and programming software on the historian,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
wampac.7	Insecure remote access to the historian.	remote access may be obtained by unauthorized individuals	to the historian from remote networks.	Unnecessary System Access (6.2.2.6)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
wampac.8	Inadequate security for configuration change management process by the manufacturer.	system permits unauthorized changes	at the manufacturer.	Inadequate Change and Configuration Management (6.2.2.5)
wampac.8	No integrity checks at the firmware level	users lack visibility that unauthorized firmware has been installed	before running it	Inadequate Change and Configuration Management (6.2.2.5)
wampac.8	Inadequate access control for firmware updates	system permits unauthorized installation of software or firmware		Inadequate Change and Configuration Management (6.2.2.5)
wampac.10	No security monitoring on the WAMPAC backend,	users lack visibility of unapproved access	on the WAMPAC backend,	Inadequate Anomaly Tracking (6.4.4.1)
wampac.10	Inadequate access control on the WAMPAC network,	unnecessary network access is permitted	to the WAMPAC backend network hosting the gateway metadata database,	Unnecessary System Access (6.2.2.6)
wampac.10	PMU configuration database accessible with weak or no credentials.	system relies on credentials that are easy to obtain for access	to the gateway metadata database.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
wampac.11	Weak network security architecture allowing unauthorized access to the network components,	unnecessary network access is permitted	to network components,	Unnecessary System Access (6.2.2.6)
wampac.11	No security monitoring on the WAMPAC network,	users lack visibility of threat activity	specifically unexpected access to network components or unusual traffic on the network,	Inadequate Anomaly Tracking (6.4.4.1)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
wampac.11	WAMPAC network accessible with weak or no credentials.	system relies on credentials that are easy to obtain for access	to the WAMPAC network.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
wampac.12	Inadequate integrity protection of the time signal.	spoofed signal is either difficult or infeasible to distinguish from a legitimate signal	that provides GPS-based time synchronization.	Use of Insecure Protocols (6.3.1.21)
et.1	Lack of fail-safe circuitry that shuts down the battery when its voltage is outside the safe range. This circuitry would prevent damage to the battery by overcharging or draining beyond limits,	design, implementation, or maintenance permits system to enter a hazardous state	by overcharging or draining the battery beyond limits,	Use of Inadequate Security Architectures and Designs (6.4.1.1)
et.1	Easily accessible interface for modifying EV firmware,	system permits unauthorized changes	to EV firmware using easily accessible interfaces,	Inadequate Change and Configuration Management (6.2.2.5)
et.1	Lack of integrity protections on EV firmware.	system permits unauthorized changes	to EV firmware.	Inadequate Change and Configuration Management (6.2.2.5)
et.2	Lack of integrity protection for the fast-charging station management system software and configuration,	system permits unauthorized changes	to the fast-charging station management system software and configuration,	Inadequate Change and Configuration Management (6.2.2.5)
et.2	Lack of circuit-breaker protection to prevent overloading of the distribution transformer.	design, implementation, or maintenance permits system to enter a hazardous state	by letting circuits become overloaded in the distribution transformer.	Use of Inadequate Security Architectures and Designs (6.4.1.1)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
et.3	Lack of EV factory and maintenance center change control processes that address the introduction of unauthorized code,	system permits installation of malware	in an EV, at the EV factory and maintenance center,	Inadequate Malware Protection (6.4.2.3)
et.3	Lack of virus checking in the public charging station system,	system permits installation of malware	in the public charging station system,	Inadequate Malware Protection (6.4.2.3)
et.3	Lack of isolation of signals for EV charging from conventional data transmission during charging,	critical communication paths are not isolated from communication paths that require fewer protections to operate	specifically, EV charging and conventional data transmission during charging,	Use of Inadequate Security Architectures and Designs (6.4.1.1)
et.3	Lack of complete checking for unnecessary data being transferred during charging,	system permits installation of malware	in the public charging station system or EV being charged, during charging,	Inadequate Malware Protection (6.4.2.3)
et.3	Lack of isolation of key functions for car safety in the EV from the more vulnerable battery-related functions.	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.	Use of Inadequate Security Architectures and Designs (6.4.1.1)
et.4	Weak firewall rules,	unnecessary access is permitted to the database	in the firewall protecting the EV database server	Unnecessary System Access (6.2.2.6)
et.4	Weak passwords,	system relies on credentials that are easy to obtain for access	to the EV database server	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
et.4	Improperly configured database server security,	unnecessary access is permitted to the database	in the database server,	Unnecessary System Access (6.2.2.6)
et.5	Inadequate integrity protections for code in the protocol translation module.	system permits unauthorized changes	to code in the protocol translation module.	Inadequate Change and Configuration Management (6.2.2.5)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
et.6	Smart meter accepting connections from sources without sufficient authentication,	inadequate binding of meter with energy users authorized to charge to that meter		Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
et.6	EVSE not protected against reconfiguration that changes its associated meter.	users lack visibility that unauthorized changes were made	in the association between an EVSE and its smart meter.	Inadequate Change and Configuration Management (6.2.2.5)
et.7	Inadequate confidentiality protection on the EV/EVSE communications channel.	system makes private data accessible to unauthorized individuals	in the EV/EVSE communications channel.	Sensitive Data Protection Vulnerability (6.3.1.15)
et.8	No method to validate that an item being charged is an EV, when charging takes place based upon an EV registration identifier.	system permits device identifier to be misused	to charge non-EV items when charging takes place based upon an EV registration identifier.	Use of Inadequate Security Architectures and Designs (6.4.1.1)
et.9	No method to authenticate the specific individual or EV associated with registration identifier when charging takes place based upon the identifier.	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.	Use of Inadequate Security Architectures and Designs (6.4.1.1)
et.10	No method to authenticate the specific EV or determine that it is a high priority EV that is being charged.	system permits device identifier to be misused	to masquerade as a high priority EV that is being charged.	Use of Inadequate Security Architectures and Designs (6.4.1.1)
et.11	Inadequate access control for utility networks or databases that store or transmit registration identities,	unnecessary network access is permitted	for utility networks or databases that store or transmit registration identities,	Unnecessary System Access (6.2.2.6)
et.11	Inadequate access control for utility networks or databases that store or transmit registration identities,	unnecessary access is permitted to the database	that stores registration identities,	Unnecessary System Access (6.2.2.6)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
et.11	Unencrypted storage of registration identities,	system makes private data accessible to unauthorized individuals	in the storage of registration identities,	Sensitive Data Protection Vulnerability (6.3.1.15)
et.11	The scenario occurs due to a design that makes a stolen EV registration ID useful to a person and/or EV other than for which it was issued. It is useful for another person if it either enables charging or a preferential rate, and if the user's identity is not verified at the point of use. It is useful for another EV if the EV is not authenticated when charging takes place.	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.	Use of Inadequate Security Architectures and Designs (6.4.1.1)
et.12	Lack of redundant communication paths or replicated databases for verifying registration identities between utilities.	critical components exhibit single point of failure	such as communication paths or databases used to verify registration identities between utilities.	Insufficient Redundancy (6.5.1.5)
et.13	Inadequate access control for utility networks or databases that store registration identities,	unnecessary network access is permitted	to utility networks or databases that store registration identities,	Unnecessary System Access (6.2.2.6)
et.13	Inadequate access control for utility networks or databases that store registration identities,	unnecessary access is permitted to the database	that stores registration identities,	Unnecessary System Access (6.2.2.6)
et.13	Lack of logging for transactions that impact the EV registration ID database.	users lack visibility that unauthorized changes were made	via transactions that impact the EV registration ID database.	Inadequate Change and Configuration Management (6.2.2.5)
et.14	Inadequate controls on software integrity,	system permits unauthorized changes	to software,	Inadequate Change and Configuration Management (6.2.2.5)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
et.15	Inadequate integrity protections for code in the charging station management system and protocol translation module,	system permits unauthorized changes	to code in the charging station management system and protocol translation module,	Inadequate Change and Configuration Management (6.2.2.5)
et.15	Lack of circuit-breaker protection to prevent overloading of the distribution transformer if many EVs are discharged,	design, implementation, or maintenance permits system to enter a hazardous state	by overloading of the distribution transformer if many EVs are discharged,	Use of Inadequate Security Architectures and Designs (6.4.1.1)
et.15	Lack of protection in EVs to prevent undesired discharge.	system takes action before confirming changes with user	causing EVs to be discharged without owner's consent.	Business Logic Vulnerability (6.3.1.8)
et.16	Incomplete checking for unnecessary data being transferred during charging between the EV and the EVSE (ET.3),	system permits installation of malware	in the EVSE during charging between the EV and the EVSE (ET.3),	Inadequate Malware Protection (6.4.2.3)
et.16	Incomplete checking for unnecessary data being transferred on the network hosting the EVSEs for the charging station,	system permits installation of malware	due to the malware spreading between EVSEs on the network hosting the EVSEs for the charging station,	Inadequate Malware Protection (6.4.2.3)
et.16	Incomplete integrity protections of the in-vehicle system,	system permits unauthorized changes	to the in-vehicle system,	Inadequate Change and Configuration Management (6.2.2.5)
et.16	Incomplete malware checking in public charging station systems,	system permits installation of malware	in public charging station systems,	Inadequate Malware Protection (6.4.2.3)
et.16	Inadequate use of the same credentials on the nearby EVSEs,	shared credentials are used for access	to nearby EVSEs,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
et.16	Inadequate circuit-breaker protection to prevent overloading of the distribution transformer.	design, implementation, or maintenance permits system to enter a hazardous state	by allowing overloading of the distribution transformer.	Use of Inadequate Security Architectures and Designs (6.4.1.1)
dr.1	Physical access to communications channel components or logical access to communications channel permitted for entities that do not require it,	physical access may be obtained by unauthorized individuals	to communications channel components,	Physical Access to the Device (6.5.1.6)
dr.1	Physical access to communications channel components or logical access to communications channel permitted for entities that do not require it,	unnecessary access is permitted to the communications channel		Unnecessary System Access (6.2.2.6)
dr.1	Lack of communications channel monitoring, including the case of publicly accessible and/or third party controlled links,	publicly accessible and/or third party controlled links used	in DRAS/customer communication channels,	Inadequate Network Segregation (6.5.1.2)
dr.1	Easy to jam wireless communications channels,	system relies on communications that are easy to jam	in wireless DRAS/customer communications channels,	Use of Insecure Protocols (6.3.1.21)
dr.1	Inadequate integrity protection for the messaging interface components of the DRAS,	system permits unauthorized changes	to the messaging interface components of the DRAS,	Inadequate Change and Configuration Management (6.2.2.5)
dr.1	Inadequate integrity protection for the messaging components of the customer systems.	system permits unauthorized changes	to the messaging components of the customer systems.	Inadequate Change and Configuration Management (6.2.2.5)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dr.1		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	Inadequate Anomaly Tracking (6.4.4.1)
dr.2	Physical access to communications channel components or logical access to communications channel permitted for entities that do not require it,	physical access may be obtained by unauthorized individuals	to communications channel components,	Physical Access to the Device (6.5.1.6)
dr.2	Physical access to communications channel components or logical access to communications channel permitted for entities that do not require it,	unnecessary access is permitted to the communications channel		Unnecessary System Access (6.2.2.6)
dr.2	Lack of communications channel monitoring, including the case of publicly accessible and/or third party controlled links,	publicly accessible and/or third party controlled links used	in DRAS/customer communications channels,	Inadequate Network Segregation (6.5.1.2)
dr.2	Wide use of the same cryptographic key,	encryption keys are shared	by multiple computers on the DRAS network,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
dr.2	Easy to tap wired/wireless communications channels.	system makes messages accessible to unauthorized individuals	(easy to tap) in wired/wireless communications channels in the DRAS network.	Use of Insecure Protocols (6.3.1.21)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dr.2		users lack visibility of threat activity	specifically the presence of unknown entities creating traffic on the DRAS/customer communication channel	Inadequate Anomaly Tracking (6.4.4.1)
dr.3	DRAS or customer DR component unable to verify source and validity of messages,	system permits messages to be modified by unauthorized individuals	between the DRAS and customer DR component,	Use of Insecure Protocols (6.3.1.21)
dr.3	DRAS or customer DR component unable to verify source and validity of messages,	message modified by an adversary is either difficult or infeasible to distinguish from a valid message	between the DRAS and customer DR component,	Use of Insecure Protocols (6.3.1.21)
dr.3	Physical access to communications channel components or logical access to communications channel permitted for entities that do not require it,	physical access may be obtained by unauthorized individuals	to communications channel components,	Physical Access to the Device (6.5.1.6)
dr.3	Physical access to communications channel components or logical access to communications channel permitted for entities that do not require it,	unnecessary access is permitted to the communications channel		Unnecessary System Access (6.2.2.6)
dr.3	Lack of communications channel monitoring, including the case of publicly accessible and/or third party controlled links.	publicly accessible and/or third party controlled links used		Inadequate Network Segregation (6.5.1.2)
dr.3		users lack visibility of threat activity	specifically the presence of unknown entities with access to the DRAS/customer communication channel	Inadequate Anomaly Tracking (6.4.4.1)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dr.4	Inadequate access control for DRAS configuration changes,	system permits unauthorized changes	to DRAS configuration,	Inadequate Change and Configuration Management (6.2.2.5)
dr.4	Lack of monitoring for unexpected or atypical DRAS configuration changes,	users lack visibility that unauthorized changes were made	in the DRAS configuration,	Inadequate Change and Configuration Management (6.2.2.5)
dr.4	Inadequate access control for the network on which the DRAS resides.	unnecessary network access is permitted	to the network on which the DRAS resides.	Unnecessary System Access (6.2.2.6)
dr.4		system relies on credentials that are easy to obtain for access	to the DRAS configuration	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
dr.5	Out-of-date patches and anti-virus signatures,	software patches are not checked regularly to ensure that they are current		Inadequate Patch Management Process (6.2.2.4)
dr.5	Out-of-date patches and anti-virus signatures,	the list of signatures used for detection of attacks is no longer current		Inadequate Malware Protection (6.4.2.3)
dr.5	Un-blocked or unnecessary opened ports that allow access,	unnecessary system services are configured to run	on un-blocked or unnecessary opened ports,	Unneeded Services Running (6.4.3.2)
dr.5	Inadequate controls for remote access to the customer system,	remote access may be obtained by unauthorized individuals	to the customer system from remote networks,	Unnecessary System Access (6.2.2.6)
dr.5	Easy physical access to the DRAS (e.g., to use a Universal Serial Bus (USB) device).	physical access may be obtained by unauthorized individuals	to the DRAS (e.g., to use a Universal Serial Bus (USB) device).	Physical Access to the Device (6.5.1.6)
dr.6	Inadequate access control for DRAS software changes,	system permits unauthorized changes	to software in the DRAS,	Inadequate Change and Configuration Management (6.2.2.5)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dr.6	Lack of monitoring for unexpected or atypical DRAS software changes,	users lack visibility that unauthorized changes were made	to the DRAS software,	Inadequate Change and Configuration Management (6.2.2.5)
dr.6	Un-blocked or unnecessary open ports and functions that allow DRAS system access,	unnecessary system services are configured to run	on un-blocked or unnecessary open ports,	Unneeded Services Running (6.4.3.2)
dr.6	Inadequate access control for the network on which the DRAS resides.	unnecessary network access is permitted	to the network on which the DRAS resides.	Unnecessary System Access (6.2.2.6)
dr.7	Out-of-date patches and anti-virus signatures,	software patches are not checked regularly to ensure that they are current	resulting in vulnerabilities that support the injection of custom malware	Inadequate Patch Management Process (6.2.2.4)
dr.7	Out-of-date patches and anti-virus signatures,	the list of signatures used for detection of attacks is no longer current	resulting in vulnerabilities that support the injection of custom malware	Inadequate Malware Protection (6.4.2.3)
dr.7	Un-blocked or unnecessary opened ports that allow access,	unnecessary system services are configured to run	on un-blocked or unnecessary open ports,	Unneeded Services Running (6.4.3.2)
dr.7	Inadequate access control for the customer DR program,	unnecessary access is permitted to system functions	in the customer DR program,	Unnecessary System Access (6.2.2.6)
dr.7	Inadequate customer energy usage verification solution.	system assumes data inputs and resulting calculations are accurate	in customer energy usage.	Business Logic Vulnerability (6.3.1.8)
dr.7		system permits unauthorized changes	to software in the customer DR system	Inadequate Change and Configuration Management (6.2.2.5)
dr.7		users lack visibility that unauthorized changes were made	to the customer DR software	Inadequate Change and Configuration Management (6.2.2.5)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dgm.1	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 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.	Use of Insecure Protocols (6.3.1.21)
dgm.1	Wireless radio signals propagate through the air and are naturally easier to intercept and influence.	system makes messages accessible to unauthorized individuals	in wireless radio signals.	Use of Insecure Protocols (6.3.1.21)
dgm.2	Since all communications have finite bandwidth, sharing a communications channel with other entities or functions can potentially reduce the availability and reliability of the channel. 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,	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.	Inadequate Network Segregation (6.5.1.2)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dgm.2	Sharing network services with others increases the attack surface of all systems. This requires a utility to put a certain level of trust in the systems sharing the communications channel and the entity that manages it.	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.	Inadequate Network Segregation (6.5.1.2)
dgm.3	Lack of access control and authentication mechanisms to engineering and console ports of substation equipment,	unnecessary access is permitted to system functions	via engineering and console ports of substation equipment,	Unnecessary System Access (6.2.2.6)
dgm.3	Lack of software and information integrity mechanisms,	system permits unauthorized changes	to software and information,	Inadequate Change and Configuration Management (6.2.2.5)
dgm.3	Physical security controls are inadequate and easily subverted,	physical access may be obtained by unauthorized individuals		Physical Access to the Device (6.5.1.6)
dgm.3	Unused engineering and console ports are not disabled.	enabled but unused ports	(unused engineering and console ports).	Physical Access to the Device (6.5.1.6)
dgm.4	Poor access controls on remote substation WAN communications,	unnecessary access is permitted to the communications channel	for remote substation WAN communications,	Unnecessary System Access (6.2.2.6)
dgm.4	Patch management on cyber and communication equipment is inadequate and slow to provide updates,	software patches are not checked regularly to ensure that they are current		Inadequate Patch Management Process (6.2.2.4)
dgm.4	Dialup LSS or wireless access negates any physical access controls.	system permits bypass of physical access controls	via dialup LSS or wireless access.	Unnecessary System Access (6.2.2.6)
dgm.5	Inadequate access controls for modifying software files,	system permits unauthorized changes	to software files,	Inadequate Change and Configuration Management (6.2.2.5)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dgm.5	Outdated security patches,	software patches are not checked regularly to ensure that they are current		Inadequate Patch Management Process (6.2.2.4)
dgm.5	Inadequate protections for remote access to DMS systems,	remote access may be obtained by unauthorized individuals	to DMS systems,	Unnecessary System Access (6.2.2.6)
dgm.5	Weak passwords.	system relies on credentials that are easy to obtain for access	to systems.	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
dgm.6	Communications between field devices and the DMS are not authenticated,	system permits messages to be modified by unauthorized individuals	in the communications between field devices and the DMS,	Use of Insecure Protocols (6.3.1.21)
dgm.6	Communications between field devices and the DMS are not authenticated,	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,	Use of Insecure Protocols (6.3.1.21)
dgm.6	Communications channels are unencrypted.	system makes messages accessible to unauthorized individuals		Use of Insecure Protocols (6.3.1.21)
dgm.7	QoS mechanisms that rely on devices to report their own classification can be spoofed,	system assumes data inputs and resulting calculations are accurate	for QoS mechanisms that rely on devices to report their own classification,	Business Logic Vulnerability (6.3.1.8)
dgm.7	Inadequate access control for connection to communication network.	network interfaces permit unnecessary traffic flows	to communication networks.	Inadequate Network Segregation (6.5.1.2)
dgm.8	Lack of development change control processes that address the introduction of unauthorized code,	system permits unauthorized changes	during software/firmware development,	Inadequate Change and Configuration Management (6.2.2.5)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dgm.8	Poor screening or lack of oversight of suppliers of equipment, maintenance, and transportation,	system permits unauthorized changes	to software/firmware at suppliers of equipment, maintenance, and transportation,	Inadequate Change and Configuration Management (6.2.2.5)
dgm.8	Inadequate controls on utility employees with access to modify field equipment.	system permits unauthorized changes	to software/firmware by utility employees with access to modify field equipment.	Inadequate Change and Configuration Management (6.2.2.5)
dgm.9	The disregard of security controls due to the objective to restore functionality and service as quickly as possible,	emergency response policy, procedures, or execution intentionally disregards security controls to speed recovery		Inadequate Continuity of Operations or Disaster Recovery Plan (6.2.3.3)
dgm.9	Oversights in security due to confusion or lack of proper policies and procedures for emergency response.	emergency response procedures unintentionally omit security controls	either in the procedures themselves or during their execution	Inadequate Continuity of Operations or Disaster Recovery Plan (6.2.3.3)
dgm.10	Utility personnel untrained on social engineering attacks, such as impersonating persons of authority, phishing and rogue USB devices,	workforce may be unaware of recommended precautions	to block social engineering attacks, such as impersonating persons of authority, phishing and rogue USB devices,	Insufficiently Trained Personnel (6.2.1.1)
dgm.10	Physical access to DMS is loosely controlled or physical security measures are easily subverted,	physical access may be obtained by unauthorized individuals	to DMS,	Physical Access to the Device (6.5.1.6)
dgm.10	More individuals than necessary have access to critical DMS functions,	users and hardware/software entities are given access unnecessary for their roles	to critical DMS functions,	Unnecessary System Access (6.2.2.6)
dgm.10	Inadequate screening of personnel with access 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.	Insufficient Identity Validation or Background Checks (6.2.2.1)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dgm.11	Inadequate protection of linemen and maintenance personnel company laptops used for remote connections from loss, theft, or abuse, and from misuse when not under control of authorized individuals,	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,	Physical Access to the Device (6.5.1.6)
dgm.11	Lack of strong authentication on company computer,	system relies on credentials that are easy to obtain for access	to company computers,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
dgm.11	Weak protection of proprietary utility documents and information,	physical access may be obtained by unauthorized individuals	to proprietary utility documents and information,	Physical Access to the Device (6.5.1.6)
dgm.11	Inadequate measures to prevent and detect human error in data center configuration (e.g., Ethernet cable plugged into wrong port),	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),	Inadequate Change and Configuration Management (6.2.2.5)
dgm.11	Allowing remote access for vendors to do application maintenance and troubleshooting,	system permits unauthorized changes	by allowing remote access for vendors to do application maintenance and troubleshooting,	Inadequate Change and Configuration Management (6.2.2.5)
dgm.11	Unencrypted distribution control communications,	system makes messages accessible to unauthorized individuals	in the distribution control communication channel,	Use of Insecure Protocols (6.3.1.21)
dgm.11	Distribution networks are more radial in nature than meshed, making network reconfiguration to restore power more difficult.	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.	Business Logic Vulnerability (6.3.1.8)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dgm.12	Poor or no authentication between the transformer and the substation controller,	system relies on credentials that are easy to obtain for access	between the transformer and the substation controller,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
dgm.12	Wireless communications are unencrypted,	system makes messages accessible to unauthorized individuals	in the wireless communication channel,	Use of Insecure Protocols (6.3.1.21)
dgm.12	Long lead times to repair or replace custom built transformers.	emergency situations may not have the appropriate replacement equipment, some of which require long lead times for repair or replacement	(custom built transformers).	Inadequate Continuity of Operations or Disaster Recovery Plan (6.2.3.3)
dgm.13	Inadequate enforcement of account management policy that ensures accounts are up to date, including checks in place for human error.	workforce not trained in proper procedures	to check for human error in account management	Insufficiently Trained Personnel (6.2.1.1)
dgm.13	Inadequate enforcement of account management policy that ensures accounts are up to date, including checks in place for human error.	adherence to policies and procedures degrades over time	introducing human error in account management	Inadequate Periodic Security Audits (6.2.3.1)
dgm.13	Inadequate enforcement of account management policy that ensures accounts are up to date, including checks in place for human error.	human error in adherence to policies and procedures	to check for human error in account management	Inadequate Periodic Security Audits (6.2.3.1)
dgm.14	Lack of authentication on serial communications to substations,	physical access to a serial port may enable logical access by unauthorized entities	to communications at substations,	Physical Access to the Device (6.5.1.6)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dgm.14	No passwords or default passwords on substation relays and RTU,	system relies on credentials that are easy to obtain for access	to substation relays and RTU (e.g., no passwords or default passwords),	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
dgm.14	Using public communication channels without authentication or encryption.	publicly accessible and/or third party controlled links used		Inadequate Network Segregation (6.5.1.2)
dgm.14	Using public communication channels without authentication or encryption.	system makes messages accessible to unauthorized individuals	using public communications channels without encryption.	Use of Insecure Protocols (6.3.1.21)
dgm.15	Controls to lockout automation system actions during maintenance are absent or insufficient,	critical operations are not locked out during maintenance	(automation system actions),	Business Logic Vulnerability (6.3.1.8)
dgm.15	Inadequate protection of linemen and maintenance personnel company laptops used for remote connections from loss, theft, or abuse, and from misuse when not under control of authorized individuals,	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,	Physical Access to the Device (6.5.1.6)
dgm.15	Lack of strong authentication on company computer,	system relies on credentials that are easy to obtain for access	to company computers,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
dgm.15	Weak protection of proprietary utility documents and information,	physical access may be obtained by unauthorized individuals	to proprietary utility documents and information,	Physical Access to the Device (6.5.1.6)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dgm.15	Inadequate measures to prevent and detect human error in data center configuration (e.g., Ethernet cable plugged into wrong port),	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),	Inadequate Change and Configuration Management (6.2.2.5)
dgm.15	Allowing remote access for vendors to do application maintenance and troubleshooting,	system permits unauthorized changes	by allowing remote access for vendors to do application maintenance and troubleshooting,	Inadequate Change and Configuration Management (6.2.2.5)
dgm.15	Unencrypted distribution control communications,	system makes messages accessible to unauthorized individuals	in distribution control communications,	Use of Insecure Protocols (6.3.1.21)
dgm.15	Distribution networks are more radial in nature than meshed, making network reconfiguration to restore power more difficult.	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.	Business Logic Vulnerability (6.3.1.8)
dgm.16	Physical security control procedures in the utility or Telco/CSP,	physical access may be obtained by unauthorized individuals	to the utility or Telco/ISP,	Physical Access to the Device (6.5.1.6)
dgm.16	Implementation permit access of threat agent to the demarc or within the service providers network CSU/DSU,	unnecessary network access is permitted	allowing access of threat agent to the demarc or within the service providers network CSU/DSU,	Unnecessary System Access (6.2.2.6)
dgm.16	Inadequate authentication and access control to substation gateway/RTU or SCADA FEP,	system relies on credentials that are easy to obtain for access	to substation gateway/RTU or SCADA FEP,	Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)
dgm.16	Inadequate or nonexistent tamper detection at the Demarc,	users lack visibility of unapproved access	to the demarc,	Inadequate Anomaly Tracking (6.4.4.1)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
dgm.16	The communication protocol does not detect or alert when information or commands come from an unauthorized source,	commands or other messages may be inserted on the network by unauthorized individuals	in the communication protocol,	Use of Insecure Protocols (6.3.1.21)
dgm.16	Serial link does not protect against capture and reading of messages by unauthorized individuals.	system makes messages accessible to unauthorized individuals	over the serial link.	Use of Insecure Protocols (6.3.1.21)
dgm.16		message modified by an adversary is either difficult or infeasible to distinguish from a valid message	in the communication protocol	Use of Insecure Protocols (6.3.1.21)
dgm.16		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	Use of Insecure Protocols (6.3.1.21)
generic.1	Inadequate or no separation of duties,	users and hardware/software entities are given access unnecessary for their roles	to perform duties that should be separated,	Unnecessary System Access (6.2.2.6)
generic.1	Security-relevant and operationally critical functionality is not monitored,	system permits unauthorized changes		Inadequate Change and Configuration Management (6.2.2.5)
generic.1	Lack of situational awareness when privileges are elevated for access to security-relevant or operationally critical functions,	users lack visibility of unapproved access	when privileges are elevated for access to security-relevant or operationally critical functions,	Inadequate Anomaly Tracking (6.4.4.1)
generic.1	Either inadequate, or lack of, incident response processes to decrease response time when incidents occur.	speed of incident response process is not appropriate for incident		Inadequate Incident Response Process (6.2.3.5)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
generic.2	Lack of or inadequate network segregation such as using virtual local area networks (VLANs) for security or using the same networks for business operations and control systems,	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,	Inadequate Network Segregation (6.5.1.2)
generic.2	Lack of situational awareness to show remote command and control of a business asset has been obtained. Situational awareness mechanisms include observing and responding to anti-virus, firewall, IDS, IPS, and system-level alerts,	users lack visibility of unapproved access	to show remote command and control of a business asset has been obtained,	Inadequate Anomaly Tracking (6.4.4.1)
generic.2	Inadequate monitoring of traffic to and from the business operations network to the Internet to notice when an incident is occurring,	users lack visibility of threat activity	between the business operations network and the Internet to notice when an incident is occurring,	Inadequate Anomaly Tracking (6.4.4.1)
generic.2	No security controls between the business and control systems network and treating the business network as a "trusted" entity.	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.	Inadequate Network Segregation (6.5.1.2)
generic.3	Unrestricted access to interfaces such as USB, Firewire, or serial ports that allows the unrestricted ability to load software or firmware to devices.	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.	Physical Access to the Device (6.5.1.6)

Failure Scenario	Original Vulnerability	Common Vulnerability	Vulnerability Context	Vulnerability Class
generic.4	Lack of adequate equipment disposal which allows a threat agent to acquire and reverse engineer equipment,	sensitive data remains on disposed equipment	and allows a threat agent to acquire and reverse engineer equipment,	Inadequate Change and Configuration Management (6.2.2.5)
generic.4	Inadequate supply chain control and/or inadequate quality control within a supply chain.	system permits unauthorized changes	in the supply chain.	Inadequate Change and Configuration Management (6.2.2.5)

C COMMON MITIGATION ACTIONS AND ACTION GROUPS

The following table lists the common actions in version 1.0 of the Failure Scenarios, arranged into mitigation action groups, along with the frequency of occurrence of that common action in all failure scenarios. This 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 a new *automatic* implementation. If the type is 'm', that implies that the action can typically be performed *manually* or by using an already available implementation.

Table 3. Common Mitigation Actions by Action Group

Action Group	Type	Common Action	Frequency
alert	a	generate alarms	12
	a	generate alerts	11
	a	prioritize alarms	1
	m	generate alarms	1
analyze	m	analyze anomalous events	2
	m	re-evaluate scheduled disconnects	1
	m	review recovery response	1
audit	a	create audit log	26
	a	protect audit logs	1
	m	create audit log	2
	m	perform audit	1
	m	perform financial audit	2
authenticate	a	authenticate data source	3
	a	authenticate devices	8
	a	authenticate messages	14
	a	authenticate users	24
	a	require authentication	2
	a	require multi-factor authentication	15
	a	require PIN	3
	a	require second-level authentication	1
	a	require single sign-on	1
	m	authenticate devices	1
	m	require multi-factor authentication	1
check integrity	a	check message integrity	9

Action Group	Type	Common Action	Frequency
	a	check OS integrity	1
	a	check software execution integrity	9
	a	check software file integrity	10
	a	protect against replay	4
	m	check software execution integrity	1
control access	a	enforce least privilege	9
	a	require credential revocation	1
	a	restrict access	1
	a	restrict network access	5
	a	restrict physical access	1
	a	use RBAC	17
	m	enforce restrictive firewall rules	4
	m	limit remote modification	1
	m	prevent modification	1
	m	require read-only access	1
	m	restrict access	1
	m	restrict application access	6
	m	restrict communication access	1
	m	restrict configuration access	1
	m	restrict database access	3
	m	restrict device access	2
	m	restrict file access	3
	m	restrict Internet access	4
	m	restrict network access	15
	m	restrict network service access	3
	m	restrict physical access	9
	m	restrict port access	1
	m	restrict remote access	15
	m	restrict system access	2
detect	a	detect abnormal behavior	4
	a	detect abnormal functionality	1
	a	detect anomalous commands	2
	a	detect physical intrusion	2
	a	detect unauthorized access	1
	a	detect unauthorized configuration changes	1
	a	detect unauthorized use	1
	a	detect unusual patterns	10
	m	detect abnormal behavior	1
	m	detect abnormal functionality	1
	m	detect abnormal output	5

Action Group	Type	Common Action	Frequency
	m	detect unauthorized access	10
	m	detect unauthorized configuration	2
	m	detect unauthorized connections	2
	m	detect unauthorized devices	1
	m	detect unusual patterns	1
	m	require intrusion detection and prevention	14
encrypt	a	encrypt application layer	1
	a	encrypt communication paths	12
	a	encrypt data at rest	6
	a	encrypt link layer	1
	m	encrypt communication paths	1
	m	require VPNs	3
enforce limits	a	enforce hardware limits	1
	a	enforce limits in hardware	1
	a	limit events	2
	a	protect from overcharge	1
	a	require circuit breaker	3
ensure availability	a	require fail-over	2
	a	require fail-safe rollback	1
	a	require redundancy	3
	a	require resiliency	1
	a	require synchronous functions	1
	m	require backup	1
	m	require redundancy	5
	m	require resiliency	1
	m	require spares	1
	m	require spread-spectrum radio	1
isolate	a	isolate functions	4
	a	isolate networks	1
	a	require unique keys	4
	m	isolate networks	7
	m	require separation of duty	1
learn	m	learn from others	2
plan	m	define contingency plan	1
	m	define incident response plan	1
	m	define policy	7
	m	define procedure	7
	m	define SLA	1
	m	emphasize security management	1
	m	prioritize recovery activities	1

Action Group	Type	Common Action	Frequency
profile	a	profile equipment	1
sanitize	a	sanitize device	1
secure design and implementation	a	design for trust	1
	a	protect credentials	1
	a	require approved cryptographic algorithms	3
	a	require approved key management	4
	a	require secure key storage	1
	m	configure for least functionality	10
	m	design for security	3
	m	design for trust	4
	m	enforce changing default passwords	1
	m	minimize private information	1
	m	protect security configuration	1
	m	require approved cryptographic algorithms	6
	m	require approved key management	1
	m	require physical connection	1
	m	require secure factory settings	1
	m	restrict occurrence	1
secure operations	a	require application whitelisting	3
	a	require password rule enforcement	1
	a	require secure boot loader	2
	a	require secure remote firmware upgrade	1
	a	require tamper detection and response	1
	a	require video surveillance	4
	m	change default credentials	3
	m	configure for least functionality	1
	m	harden platforms	1
	m	lock workstations	3
	m	maintain anti-virus	6
	m	maintain latest firmware	1
	m	maintain patches	6
	m	require assured maintenance	1
	m	require lockout	3
	m	require password rule enforcement	1
	m	require safe mode	3
	m	require strong passwords	2
test	m	conduct code review	2
	m	conduct penetration testing	2
	m	perform hardware acceptance testing	1
	m	perform security testing	3

Action Group	Type	Common Action	Frequency
	m	require reconfiguration in test mode	1
	m	test after install	1
	m	test after maintenance	1
	m	test before install	7
	m	test for malware	1
	m	vulnerability scan before install	3
track	m	implement configuration management	11
	m	track asset	1
train	m	train personnel	14
user decision	m	choose own rate	1
	m	continue normal operations	1
verify	a	confirm action	3
	a	cross check	2
	a	require 2-person rule	8
	a	require acknowledgment	3
	a	require approval	1
	a	require failure messages	1
	a	require message verification	1
	a	require non-repudiation	2
	a	require on-going validation	1
	a	require read only access	1
	a	validate data	5
	a	validate inputs	3
	a	validate signal	1
	a	verify correct operation	2
	a	verify EV owner	1
	a	verify network changes	1
	m	confirm action	1
	m	cross check	8
	m	require periodic walk-downs	1
	m	require reliable external time source	1
	m	verify absence of hardcoded credentials	1
	m	verify correct operation	1
	m	verify load	1
	m	verify mode	1
	m	verify personnel	5
	m	verify settings	1
	m	verify time synchronization	1

D MAPPING OF ORIGINAL MITIGATIONS TO COMMON MITIGATIONS

The following table records how each failure scenario mitigation was rewritten into the new common mitigations form. The second column ("Original Mitigation") contains the mitigation as written in version 0.9 of the Failure Scenarios. The third column ("Type") indicates whether the mitigation represents an automatic ('a') or manual ('m') implementation. The fourth column ("Common Action") and fifth column ("Action Application") comprise the revised mitigation as presented in version 1.0 of the Failure Scenarios. For example, in AMI.1, "Protection schemes to detect anomalous disconnect and reconnect commands not stemming from the normal Customer Information System (CIS) system" was replaced with "Detect anomalous commands (disconnect and reconnect commands) not stemming from the normal Customer Information System (CIS) system." The sixth column ("Action Group") repeats information provided in Appendix C, as a convenience.

Table 4. Mapping of Original Mitigations to Common Mitigations

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.1	Protection schemes to detect anomalous disconnect and reconnect commands not stemming from the normal Customer Information System (CIS) system,	a	detect anomalous commands	(anomalous disconnect and reconnect commands) not stemming from the normal Customer Information System (CIS) system	detect
ami.1	Use Role-Based Access Control (RBAC) to limit who has access to sensitive functions,	a	use RBAC	to limit who has access to sensitive functions	control access
ami.1	Data validation to ensure reasonableness of changes,	a	validate data	to ensure reasonableness of changes	verify

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.1	Alarming of changes to sensitive data,	a	generate alarms	for changes to sensitive data	alert
ami.1	Audit logs to track who has made system configuration, software, or database additions or modifications,	a	create audit log	to track who has made system configuration, software, or database additions or modifications	audit
ami.1	Establish a two-person rule on single transactions that initiate mass disconnects (e.g., substation feeder, all meters listening to a given aggregation point, geographic region, etc.),	a	require 2-person rule	for single transactions that initiate mass disconnects (e.g., substation feeder, all meters listening to a given aggregation point, geographic region, etc.)	verify
ami.1	System does not allow greater than (n) number of disconnects (using any number of transactions) within a specified time period,	a	limit events	to no more than (n) number of disconnects (using any number of transactions) within a specified time period	enforce limits
ami.1	Greater than (n) number of disconnects within a specified time period should be subject to a two-person rule,	a	require 2-person rule	for greater than (n) number of disconnects within a specified time period	verify
ami.1	Perform a cross check with the billing system to ensure the customer has the appropriate status before the disconnect command is issued.	m	cross check	with the billing system to ensure the customer has the appropriate status before the disconnect command is issued	verify

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.2	Improve revenue protection methods to detect unusual patterns of energy usage (all utilities have some type of revenue protection scheme, but these may not be adequate),	a	detect unusual patterns	of energy usage (all utilities have some type of revenue protection scheme, but these may not be adequate)	detect
ami.2	Utilize RBAC to limit access to sensitive functions,	a	use RBAC	to limit access to sensitive functions	control access
ami.2	Use of data validation to ensure reasonableness for changes,	a	validate data	to ensure reasonableness for changes	verify
ami.2	Improve alarming to monitor and issue alerts for changes to sensitive data,	a	generate alarms	on changes to sensitive data	alert
ami.2	Audit logs to track who has made software or database modifications,	a	create audit log	of who has made software or database modifications	audit
ami.2	Conduct ongoing checks of live executables against correct versions using digital signatures or hashing techniques (that also must resist replacement),	a	check software execution integrity	since software may be compromised when loaded for execution	check integrity
ami.2	Monitor the billing and AMI system network traffic for unexpected data or destinations,	m	detect abnormal output	(unexpected data or destinations) in billing and AMI system network traffic	detect
ami.2	Implement a rigorous financial auditing program (checking for unexpected results),	m	perform financial audit	checking for unexpected results	audit

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.2	Implement a robust change/configuration management program,	m	implement configuration management		track
ami.2	Limit which system components can access the metering servers,	m	restrict network access	for system components to the metering servers	control access
ami.2	Improve physical security and training including the use of video surveillance and locking workstations when unattended and proper platform hardening.	m	restrict physical access		control access
ami.2		m	train personnel	regarding need to lock unattended workstations	train
ami.2		a	detect physical intrusion	with the use of video surveillance	detect
ami.2		m	lock workstations	when workstations are unattended	secure operations
ami.2		m	harden platforms		secure operations
ami.3	RBAC to limit who has access to the AMI system and the enterprise network,	a	use RBAC	to limit who has access to the AMI system and the enterprise network	control access
ami.3	Audit logs to track and alert who has made software additions or modifications,	a	create audit log	of who has made software additions or modifications	audit
ami.3		a	generate alerts	of who has made software additions or modifications	alert

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.3	Ongoing checks of live executables against correct versions using digital signatures or hashing techniques,	a	check software execution integrity	since software may be compromised when loaded for execution	check integrity
ami.3	Ensure physical access to the system(s) does not automatically grant logical access,	a	authenticate users	so that physical access to the system(s) does not automatically grant logical access	authenticate
ami.3	Limit physical access with good operational security (OPSEC) such as multi-factor authentication controls to gain access to sensitive systems,	a	require multi-factor authentication	to gain access to sensitive systems	authenticate
ami.3	Ensure adequate network segregation and deny controls systems networks access to or from the Internet,	m	isolate networks	serving critical functionality such as control systems from the Internet	isolate
ami.3		m	restrict Internet access	to deny controls systems networks access to or from the Internet	control access
ami.3	Live cameras and videos to document who enters the server room,	a	require video surveillance	to document who enters the server room	secure operations
ami.3	Limit who has access and can make configuration changes.	m	restrict configuration access	to limit who has access and can make configuration changes	control access

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.4	Use approved cryptographic algorithms and cryptographic modules to protect the confidentiality of the cryptographic keys,	m	require approved cryptographic algorithms	to protect the confidentiality of communications on the internal bus	secure design and implementation
ami.4		m	require approved key management	to protect the cryptographic keys	secure design and implementation
ami.4	Use unique symmetric keys for each deployed meter,	a	require unique keys	(symmetric keys) for each deployed meter	isolate
ami.4	Improve revenue protection methods to detect unusual reported patterns of energy usage on smart meters (all utilities have some type of revenue protection scheme, but these may not be adequate),	a	detect unusual patterns	of energy usage on smart meters (all utilities have some type of revenue protection scheme, but these may not be adequate)	detect
ami.4	Rigorous financial auditing program (checking for unexpected results).	m	perform financial audit	to check for unexpected results	audit
ami.5	Require a unique symmetric key for each meter,	a	require unique keys	(symmetric key) for each meter	isolate
ami.5	Use proven key management techniques,	a	require approved key management		secure design and implementation
ami.5	Use secure key storage methods on meters.	a	require secure key storage	on meters	secure design and implementation

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.6	Improve revenue protection methods to detect unusual patterns of energy usage on smart meters (all utilities have some type of revenue protection scheme, but these may not be sufficient),	a	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
ami.6	Require multi-factor authentication for firmware or software updates,	a	require multi-factor authentication	for firmware or software updates	authenticate
ami.6	Use of digital signature on code files to validate software or firmware updates before installation and/or during operation.	a	check software file integrity	(digital signatures or keyed hashes) to validate software or firmware updates before installation and/or during operation	check integrity
ami.7	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),	m	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)	test
ami.7	Capability to securely upgrade meter firmware remotely,	a	require secure remote firmware upgrade	on the meter	secure operations
ami.7	Use of a secure boot loader,	a	require secure boot loader		secure operations

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.7	Event or alarming capabilities that identify unusual or unexpected meter operations,	a	generate alarms	for unusual or unexpected meter operations	alert
ami.7	Monitor communications traffic between meters and the head end with the ability to identify network ports and services in use. Validate network ports and services against intended applications and generate alerts on any unapproved traffic. Security Information and Event Management (SIEM) systems can provide this visibility into network traffic.	m	detect abnormal functionality	to identify network ports and services in use and generate alerts on any unapproved traffic	detect
ami.7		m	cross check	network ports and services against intended applications	verify
ami.7		a	generate alerts	for unapproved traffic	alert
ami.8	Design the system to prioritize alarms by type, location, and other criteria so that high-profile alarms can be distinguished and highlighted,	a	prioritize alarms	by type, location, and other criteria so that high-profile alarms can be distinguished and highlighted	alert
ami.8	Path protection for receipt of tamper alarms (authentication, encryption, replay protection),	a	authenticate messages	for receipt of tamper alarms	authenticate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.8		a	encrypt communication paths	for receipt of tamper alarms	encrypt
ami.8		a	protect against replay	involving receipt of tamper alarms	check integrity
ami.8	Verify that tamper alarm is for a real meter,	m	cross check	that tamper alarm is for a real meter	verify
ami.8	Perform hardware acceptance testing that includes tamper alarms,	m	perform hardware acceptance testing	including tamper alarms	test
ami.8	Verify outage alerts with existing technology such as the customer service systems.	m	cross check	outage alerts with existing technology such as the customer service systems	verify
ami.9	Improve protection methods to detect unusual patterns of disconnects on smart meters,	a	detect unusual patterns	of disconnects on smart meters	detect
ami.9	May need to re-evaluate all scheduled disconnects,	m	re-evaluate scheduled disconnects		analyze
ami.9	Review and amend policy, procedures, and approval process for mass meter disconnect,	m	define policy	for mass meter disconnect	plan
ami.9		m	define procedures	for mass meter disconnect	plan
ami.9	Deploy multi-factor authentication for mass meter disconnect,	m	require multi-factor authentication	for mass meter disconnect	authenticate
ami.9	Workforce education and training,	m	train personnel	in the workforce	train

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.9	Implement strict Internet firewall rules and require use of a Virtual Private Network (VPN) for internal connections,	m	restrict Internet access	using firewall rules	control access
ami.9		m	require VPNs	for internal connections from the Internet	encrypt
ami.9	Monitoring of traffic between Internet and AMI head end to identify and mitigate unauthorized access,	m	detect unauthorized access	in network traffic between Internet and AMI head end	detect
ami.9		a	restrict network access	between Internet and AMI head end	control access
ami.9	Restrict the AMI head end system from connecting to the Internet and/or provide strong logical separation, authentication, and approved cryptographic methods as appropriate,	m	restrict Internet access	for the AMI head end system	control access
ami.9		m	isolate networks	for the AMI head end system from the Internet	isolate
ami.9		a	authenticate devices	connecting to the AMI head end system	authenticate
ami.9		m	require approved cryptographic algorithms	for the AMI head end system	secure design and implementation
ami.9	Limit MDMS access to a minimum number of systems and/or individuals.	a	enforce least privilege	to the minimum number of systems and/or individuals requiring MDMS access	control access

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.10	The price calculation system should have protections against a person overriding the calculated prices or entering inconsistent prices, as well as logging and alarming of overrides,	a	validate data	to detect a person overriding the calculated prices or entering inconsistent prices in the price calculation system	verify
ami.10		a	create audit log	when a person overrides the calculated prices or enters inconsistent prices in the price calculation system	audit
ami.10		a	generate alarms	when a person overrides the calculated prices or enters inconsistent prices in the price calculation system	alert
ami.10	Implement strict Internet firewall rules and require use of VPN for internal connections,	m	restrict Internet access	using firewall rules	control access
ami.10		m	require VPNs	for internal connections from the Internet	encrypt
ami.10	Monitoring of traffic between the Internet and AMI to identify and mitigate unauthorized access,	m	detect unauthorized access	between the Internet and AMI	detect
ami.10		a	restrict network access	between the Internet and AMI	control access
ami.10	Multi-factor authentication for price changes,	a	require multi-factor authentication	for price changes	authenticate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.10	Minimum set of personnel with access to perform price changes,	a	enforce least privilege	to minimize personnel with access to perform price changes	control access
ami.10	Two-person rule for execution of price changes.	a	require 2-person rule	for execution of price changes	verify
ami.11	Define an operating procedure to confirm an outage when receiving an AMI last gasp outage message,	m	define procedures	to confirm an outage when receiving an AMI last gasp outage message	plan
ami.11	Grid operator continues to follow normal operation procedures rather than responding to AMI last gasp outage messages,	m	continue normal operations	rather than responding to AMI last gasp outage messages	user decision
ami.11	Grid operator checks SCADA system including load verification at substation and line level to verify reduced demand,	m	verify load	at substation and line level to verify reduced demand	verify
ami.11	Protection of the path used for receipt of last gasp messages (authentication, encryption, replay protection, checks that a last gasp message is from a real meter),	a	authenticate messages	on receipt of last gasp messages	authenticate
ami.11		a	encrypt communication paths	for receipt of last gasp messages	encrypt
ami.11		a	protect against replay	on receipt of last gasp messages	check integrity

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.11		a	confirm action	on receipt of last gasp messages by checking that a last gasp message is from a real meter	verify
ami.11	Attempt communication with a meter after receiving its last gasp message.	m	confirm action	after receiving last gasp message from a meter	verify
ami.12	Monitoring of traffic between Internet and AMI consumer information to identify and mitigate unauthorized access,	m	detect unauthorized access	between Internet and AMI consumer information	detect
ami.12		a	restrict network access	between Internet and AMI consumer information	control access
ami.12	Implement a robust change/configuration management program to reduce the likelihood that a threat agent can compromise an entire system,	m	implement configuration management	to reduce the likelihood that a threat agent can compromise an entire system	track
ami.12	Require review and/or periodic penetration testing for changes to Internet-facing resources or high value targets,	m	conduct penetration testing	for changes to Internet-facing resources or high value targets	test
ami.12	Use strong authentication for system access, limiting database access to authorized applications and/or locally authenticated users,	a	authenticate users	for system access	authenticate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.12		a	enforce least privilege	to limit database access to authorized applications and/or locally authenticated users	control access
ami.12	Require strong database authentication be used.	a	authenticate users	to the database	authenticate
ami.13	Improve physical security and training including the use of video surveillance and locking workstations when unattended,	m	restrict physical access		control access
ami.13		m	train personnel	regarding need to lock unattended workstations	train
ami.13		a	require video surveillance		secure operations
ami.13		m	lock workstations	when unattended	secure operations
ami.13	Improve user interface design including confirmation for actions,	a	confirm action	in the user interface design	verify
ami.13	Inactivity logout for non-safety-critical consoles,	m	lock workstations	for inactivity on non-safety-critical consoles	secure operations

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.13	Integrate 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.	m	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	verify
ami.13	Implement second level authentication to the application interface to initiate customer disconnect.	a	require second-level authentication	to the application interface to initiate customer disconnect	authenticate
ami.14	Implement separate networks using different encryption keys to prevent a breach in one network from affecting another network,	m	isolate networks	using different encryption keys to prevent a breach in one network from affecting another network	isolate
ami.14	Use approved link layer cryptography on the AMI network to prevent a threat agent from being able to affect the confidentiality and integrity of the AMI network if a breach should occur,	a	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	secure design and implementation
ami.14	Use time-stamping, or other methods, to prevent replay attacks.	a	protect against replay	using time-stamping or other methods	check integrity

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.15	Provide backup sites with equivalent physical and logical security as normal operational sites, including video surveillance and continuous monitoring,	m	restrict physical access	for backup sites comparable to normal operational sites	control access
ami.15		a	require video surveillance	for backup sites comparable to normal operational sites	secure operations
ami.15		a	detect physical intrusion	for backup sites comparable to normal operational sites	detect
ami.15	Include and emphasize security management in business continuity and disaster recovery planning, procedures and execution,	m	emphasize security management	in business continuity and disaster recovery planning, procedures and execution	plan
ami.15	Include risk and vulnerability assessments in business continuity and disaster recovery testing.	m	define policy	to include risk and vulnerability assessments in business continuity and disaster recovery testing	plan
ami.16	Design and implement a trustworthy key management process, including secure generation, distribution, storage, and update of cryptographic keys.	a	require approved key management	including secure generation, distribution, storage, and update of cryptographic keys	secure design and implementation
ami.17	Ensure GSM-based communications for AMI operate only in 3G mode,	m	verify mode	of GSM-based communications in the AMI to operate only in 3G mode	verify

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.17	Provide a capability for cellular-based functions fail over to an alternative non-wireless technology such as power line carrier (PLC).	a	require fail-over	for cellular-based functions to an alternative non-wireless technology such as power line carrier (PLC)	ensure availability
ami.18	Strengthen access, authorization, and authentication controls for devices that will authenticate to a HAN network.	m	restrict device access	to the HAN network	control access
ami.18		a	authenticate devices	accessing the HAN network	authenticate
ami.19	Implement a reliable external time source and do not use the meter's internal clock for time-stamping functionality,	m	require reliable external time source	for the meter's time-stamping functionality	verify
ami.19	Provide periodic checks of time synchronization, and integrity and availability protections for the time synchronization protocol.	m	cross check	periodically, the results of the time synchronization protocol	verify
ami.19		a	check software execution integrity	of the time synchronization protocol, since software may be compromised when loaded for execution	check integrity
ami.19		m	verify time synchronization	in the time synchronization protocol	verify

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.20	Logging and auditing of TOU pricing changes,	a	create audit log	records for TOU pricing changes	audit
ami.20	Two-person rule for major changes,	a	require 2-person rule	for major changes	verify
ami.20	Implement a robust change/configuration management program to reduce the likelihood that one person can implement a change that impacts the entire system.	m	implement configuration management	to reduce the likelihood that one person can implement a change that impacts the entire system	track
ami.21	Minimize the functionality available on the field service laptop,	m	configure for least functionality	on the field service laptop	secure design and implementation
ami.21	Require laptop encryption and asset tracking (phone home) for field service equipment,	a	encrypt data at rest	on the field service equipment laptop	encrypt
ami.21		m	track asset	(phone home) for the field service equipment laptop	track
ami.21	Ensure credentials for laptops can be revoked,	a	require credential revocation	for laptops	control access
ami.21	Implement remote wipe capability for lost field assets,	a	sanitize device	with remote wipe capability for lost field assets	sanitize
ami.22	Require multi-factor authentication for privileged functionality,	a	require multi-factor authentication	for privileged functionality	authenticate
ami.22	Disable or restrict access to web-based administration if feasible.	m	restrict application access	to web-based administration	control access

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.23	Implement multi-factor authentication for privileged functionality,	a	require multi-factor authentication	for privileged functionality	authenticate
ami.23	Test AMI equipment to ensure it does not utilize hardcoded credentials.	m	verify absence of hardcoded credentials	on AMI equipment	verify
ami.24	Use approved cryptographic algorithms,	m	require approved cryptographic algorithms		secure design and implementation
ami.24	Implement upgrade procedures in change and configuration management policies and procedures to allow future cryptographic changes,	m	define procedures	in configuration management policies and procedures to allow future cryptographic changes	plan
ami.24	Standardize the purchasing process to include security, including cryptography,	m	define procedures	to include security, including cryptography, in the purchasing process	plan
ami.24	Include security controls in system acceptance testing.	m	perform security testing	of security controls during system acceptance testing	test
ami.25	Implement a change and configuration (patch) management plan which includes a severity rating (critical, important, moderate, low) and timeframes for patching vulnerabilities based on severity,	m	implement configuration management	including a severity rating (critical, important, moderate, low) and timeframes for patching vulnerabilities based on severity	track

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.25	Monitor network traffic to the AMI head end servers to identify, alarm and mitigate unauthorized access,	m	detect unauthorized access	in network traffic to the AMI head end servers	detect
ami.25		m	generate alarms	for unauthorized access to the AMI head end servers	alert
ami.25		m	restrict network access	to the AMI head end servers	control access
ami.25	Standardize the purchasing process to include security,	m	define procedures	to include security in the purchasing process	plan
ami.25	Make security controls part of system acceptance testing.	m	perform security testing	on security controls during system acceptance testing	test
ami.26	Security analysis of the payment system during its design,	m	design for security	in the payment system	secure design and implementation
ami.26	Implement integrity features such as digital signatures to the card contents,	a	check software file integrity	(digital signatures or keyed hashes) to the card contents	check integrity
ami.26	Include security testing as a part of system acceptance testing.	m	perform security testing	as part of system acceptance testing	test
ami.27	Security analysis of the device design to identify and remove unsecure development features and nonstandard" interfaces from production devices	m	design for security	to identify and remove unsecure development features and nonstandard" interfaces from production devices"	secure design and implementation

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.27	Develop 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,	m	design for security	in equipment such that knowledge alone should not allow a threat agent to access a device without knowledge of keys and other credentials in equipment design	secure design and implementation
ami.27	Remove unnecessary interfaces and labeling from production devices.	m	configure for least functionality	by removing unnecessary interfaces and labeling from production devices	secure design and implementation
ami.28	Provide fail-safe rollback capability for the patching process,	a	require fail-safe rollback	for the patching process	ensure availability
ami.28	Apply patches to a test (non-production) set of meters and troubleshoot problems prior to applying patches to production units.	m	test before install	to troubleshoot problems by testing a (non-production) set of meters prior to applying patches to production units	test
ami.29	Strengthen access control to the HAN,	m	restrict network access	to the HAN	control access
ami.29	Minimize the use of PII in HAN systems and devices.	m	minimize PII	in HAN systems and devices	secure design and implementation
ami.30	Improve revenue protection methods to detect unusual patterns of energy usage on smart meters (all utilities have some type of revenue protection scheme, but these may not be sufficient),	a	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

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
ami.30	Require multi-factor authentication for firmware updates,	a	require multi-factor authentication	for firmware updates	authenticate
ami.30	Use of digital signature on code files to validate firmware updates before installation.	a	check software file integrity	(using digital signature or keyed hash) code files to validate firmware updates before installation	check integrity
ami.31	Protection schemes to detect anomalous disconnect and reconnect commands not stemming from the normal Customer Information System (CIS) system,	a	detect anomalous commands	(disconnect and reconnect commands) not stemming from the normal Customer Information System (CIS) system	detect
ami.31	Require multi-factor authentication for firmware updates,	a	require multi-factor authentication	for firmware updates	authenticate
ami.31	Use of digital signature on code files to validate firmware updates before installation.	a	check software file integrity	(digital signature or keyed hash) on code files to validate firmware updates before installation	check integrity
ami.31	Audit logs to track who has made system configuration, software, or database additions or modifications,	a	create audit log	to track who has made system configuration, software, or database additions or modifications	audit
ami.31	Perform a cross check with the billing system to ensure the customer has the appropriate status before the disconnect command can is issued.	m	cross check	with the billing system to ensure the customer has the appropriate status before the disconnect command can is issued	verify

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.1	Implement username/password access protection for all user interface interactions,	a	authenticate users	for all user interface interactions	authenticate
der.1	Require users to change factory default access passwords after installation,	m	change default credentials	after installation	secure operations
der.1	Hardwire safe setting limits to ensure that no setting changes can damage equipment,	a	enforce limits in hardware	to ensure that no setting changes can damage equipment	enforce limits
der.1	Instruct DER owners on secure networking requirements so they will understand why they should not bypass security settings.	m	train personnel	on secure networking requirements so that DER owners will understand the impact of bypassing security settings	train
der.1	Require second level approval for any security settings	a	require approval	of next level management for critical security settings	verify
der.2	All network changes must be authenticated and any new connections must contain only authorized equipment,	a	verify network changes		verify
der.2		a	authenticate devices	so that any new connections support only authorized equipment	authenticate
der.2	Detect unauthorized configuration changes to the DER system,	a	detect unauthorized configuration changes	to the DER system	detect

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.2	Take preventive measures such as limiting the types of traffic, shut down certain ports, etc.,	m	configure for least functionality	by limiting the types of traffic, shutting down certain ports, etc.	secure design and implementation
der.2	Communication protocols used between DER system components are required to authenticate all messages, including their source and destinations,	a	authenticate messages	, including their source and destinations, in communication protocols used between DER system components	authenticate
der.2	Communication protocols used for critical commands are required to send acknowledgements and failure messages,	a	require acknowledgment	in communication protocols used for critical commands	verify
der.2		a	require failure messages	in communication protocols used for critical commands	verify
der.2	DER system installers are trained to ensure that the recommended access control security settings are enabled,	m	train personnel	(DER system installers) to ensure that the recommended access control security settings are enabled	train
der.2	Vendors enable secure configuration and network settings by default, and allow modifications only by authenticated users,	m	require secure factory settings	for configuration and network parameters	secure design and implementation
der.2		a	authenticate users	who make modifications to secure configuration and network settings	authenticate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.2	The DER system is constrained in what functional and security settings can be changed remotely.	m	limit remote modification	of functional and security settings for the DER system	control access
der.3	Validation of software/firmware before installation by comparing with a known good version (a gold disk")	m	cross check	software/firmware before installation by comparing with a known good version (a gold disk")"	verify
der.3	Periodic re-validation of software/firmware,	a	require on-going validation	of software/firmware	verify
der.3	Authentication for critical security functions,	a	authenticate users	for access to modify software/firmware	authenticate
der.3	More complete testing of DER systems.	m	test for malware	in DER systems	test
der.4	Communication protocols used for confidential or private information must ensure confidentiality of information in transit.	a	encrypt communication paths	used for confidential or private information	encrypt
der.5	Test all DER systems before installation for malware,	m	test before install	for malware in all DER systems	test
der.5	Test all DER systems after installation for malware,	m	test after install	for malware in all DER systems	test
der.5	The utility requires (or recommends) that maintenance be performed by security-certified maintenance organizations that can be trusted not to install malware,	m	require assured maintenance	by security-certified maintenance organizations that can be trusted not to install malware	secure operations

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.5	Test all DER systems after maintenance for malware,	m	test after maintenance	for malware in all DER systems	test
der.5	Audit logs capture all changes to software and firmware, linking the updates to roles,	a	create audit log	of all changes to software and firmware, linking the updates to roles	audit
der.5	Audit logs prevent deletion of records without notifying a security entity,	a	protect audit logs	from deletion of records unless a security authority is notified	audit
der.5	Backdoor vendor/maintenance ports are disabled.	m	configure for least functionality	by disabling backdoor vendor/maintenance ports	secure design and implementation
der.6	Communication protocols used to manage DER systems must validate the integrity of the data in transit, including protection against replay,	a	check message integrity	in communication protocols used to manage DER systems	check integrity
der.6		a	protect against replay	in communication protocols used to manage DER systems	check integrity
der.6		a	create audit log	of out-of-sequence data	audit
der.6		a	generate alarms	for system owners when out-of-sequence data is detected	alert
der.7	The time synchronization communication protocol authenticates messages and ensures their integrity,	a	authenticate messages	in the time synchronization communication protocol	authenticate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.7		a	check message integrity	in the time synchronization communication protocol	check integrity
der.7	The DER system confirms operationally critical actions with the utility DER management system before acting,	a	cross check	operationally critical actions with the utility DER management system before acting	verify
der.8	Time synchronization ensures that the timestamps of audit logs capture a series of events with adequate accuracy and resolution,	a	require read only access	to timestamp for stored copies of commands received from utility	verify
der.8	Communication protocols require non-repudiation interactions between the utility and the customer system for all critical commands.	a	require non-repudiation	for all critical commands in communication protocols between the utility and the customer system	verify
der.9	Ensure all communication protocols include message authentication,	a	authenticate messages	in all communication protocols	authenticate
der.9	Ensure DER systems validate the data received in messages as reasonable and within the DER intrinsic capabilities,	a	validate data	in DER systems messages as reasonable and within the DER intrinsic capabilities	verify
der.9	Ensure that messages that fail message authentication cause alarms that notify the appropriate personnel,	a	generate alarms	for messages that fail message authentication	alert

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.9	Ensure that messages that fail message authentication are logged for forensic analysis.	a	create audit log	of messages that fail message authentication	audit
der.10	Require access control and authentication for all FDEMS user interface interactions,	m	restrict application access	for all FDEMS user interface interactions	control access
der.10		a	authenticate users	for all FDEMS user interface interactions	authenticate
der.10	FDEMS requires users to reset factory-set default access passwords after installation,	m	change default credentials	for FDEMS after installation	secure operations
der.10	Implement strong role based access control (RBAC) for the FDEMS system,	a	use RBAC	in the FDEMS system	control access
der.10	Limit privileges to access the FDEMS operating system and physical host,	a	enforce least privilege	to access the FDEMS operating system and physical host	control access
der.10	Protect the FDEMS network with firewalls and require strong authentication for remote access to the FDEMS,	m	enforce restrictive firewall rules	for access to the FDEMS network	control access
der.10		a	require multi-factor authentication	for users requesting remote access to the FDEMS network	authenticate
der.10	The utility provides instruction to FDEMS owners on secure networking requirements	m	train personnel	including the FDEMS owners and administrators, on secure networking requirements	train

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.11	Limit privileges to access the FDEMS operating system and physical host,	a	enforce least privilege	to access the FDEMS operating system and physical host	control access
der.11	Protect the FDEMS network with firewalls and require strong authentication for remote access to the FDEMS,	m	enforce restrictive firewall rules	for access to the FDEMS network	control access
der.11		a	require multi-factor authentication	for users requesting remote access to the FDEMS	authenticate
der.11	FDEMS monitors for shutdown conditions and sends alerts,	a	detect conditions	indicating a shutdown of site DER systems	detect
der.11		a	generate alerts	upon shutdown of site DER systems	alert
der.11	The utility provides instruction to FDEMS owners on secure networking requirements,	m	train personnel	including FDEMS owners and administrators on secure networking requirements	train
der.12	Require access control and authentication for all FDEMS user interface interactions,	m	restrict application access	for all FDEMS user interface interactions	control access
der.12		a	authenticate users	for all FDEMS user interface interactions	authenticate
der.12	FDEMS requires users to reset factory-set default access passwords after installation,	m	enforce changing default passwords	as a system enforced step during installation	secure design and implementation

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.12	Implement strong role based access control (RBAC) for the FDEMS system,	a	use RBAC	in the FDEMS system	control access
der.12	Limit privileges to access the FDEMS operating system and physical host,	a	enforce least privilege	for access to the FDEMS operating system and physical host	control access
der.12	Protect the FDEMS network with firewalls,	m	enforce restrictive firewall rules	for access to the FDEMS network	control access
der.12	Require strong authentication for remote access to the FDEMS.	a	require multi-factor authentication	for users requesting remote access to the FDEMS	authenticate
der.13	Implement secure boot mechanisms,	a	require secure boot loader		secure operations
der.13	Implement trusted code execution mechanisms,	a	check software execution integrity	since software may be compromised when loaded for execution	check integrity
der.13	Create a certification mechanism such that the software executables and images are signed,	a	check software file integrity	for software executables and images	check integrity
der.13	Implement operating system integrity mechanisms (e.g., virtual machine monitoring, rootkit detection, etc.),	a	check OS integrity	(e.g., virtual machine monitoring, rootkit detection, etc.)	check integrity
der.13	Implement auditing capabilities to capture commands.	a	create audit log	to capture commands	audit

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.14	Implement a system threshold that limits the number of shutdowns of DER systems within a specified time period,	a	limit events	specifically the number of shutdown events of DER systems within a specified time period	enforce limits
der.14	Implement RBAC for the DER SCADA,	a	use RBAC	in the DER SCADA	control access
der.14	Employ a data source authentication mechanism for the DER SCADA protocols,	a	authenticate data source	for the DER SCADA protocols	authenticate
der.14	Implement message authentication and information input validation for the DER SCADA control commands,	a	authenticate messages	that convey DER SCADA control commands	authenticate
der.14		a	validate inputs	(as a consistency check) for the DER SCADA control commands	verify
der.14	Deploy intrusion detection mechanisms as part of the DER SCADA network management.	m	require intrusion detection and prevention	as part of DER SCADA network management	detect
der.15	Implement RBAC for the DER SCADA,	a	use RBAC	for the DER SCADA	control access
der.15	Employ a data source authentication mechanism for the DER SCADA protocols,	a	authenticate data source	for the DER SCADA protocols	authenticate
der.15	Deploy intrusion detection mechanisms as part of the DER SCADA network management,	m	require intrusion detection and prevention	as part of DER SCADA network management	detect

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.16	Authentication mechanisms,	a	authenticate users	accessing the DER SCADA system	authenticate
der.16	Message integrity and authentication mechanisms.	a	check message integrity	or messages issued by the DER SCADA system	check integrity
der.16		a	authenticate messages	communicated in the DER SCADA network	authenticate
der.17	Implement RBAC for the utility's DERMS system to prevent unauthorized users from changing pricing signals,	a	use RBAC	in the utility's DERMS system to limit those users authorized to change pricing signals	control access
der.17	For operationally critical events, implement multi-factor authentication,	a	require multi-factor authentication	for operationally critical modifications	authenticate
der.17	Deploy mechanisms for intrusion detection, auditing and event notification as part of the DERMS network and system management capabilities.	m	require intrusion detection and prevention	as part of the DERMS network and system management capabilities	detect
der.17		a	create audit log	of changes to DERMS power flow analysis configuration data	audit
der.17		a	generate alerts	if DERMS power flow analysis configuration data is changed, or is changed at an unexpected time or to an unexpected value (based on the logging information)	alert

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.18	Implement RBAC for the utility's DERMS system to prevent unauthorized users from changing microgrid establishment permissions,	a	use RBAC	to limit those users authorized to change microgrid establishment permissions in the utility's DERMS system	control access
der.18	Deploy mechanisms for intrusion detection, auditing and event notification as part of the DERMS network and system management capabilities,	m	require intrusion detection and prevention	as part of DERMS network and system management capabilities	detect
der.18		a	create audit log	for changes to microgrid establishment permissions, via GUI or file/database interface, and of utility disconnections of microgrids	audit
der.18		a	generate alerts	if microgrid establishment permissions are changed, or are changed at an unexpected time or to an unexpected value, and communicate to microgrid, to assist it in protecting itself	alert

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.18	Secure communications between the utility and the microgrid management system, including immediate notification of anomalies that might allow the microgrid to protect itself,	a	require resiliency	of communications path between the utility and the microgrid management system, to support immediate transmission of such alerts, without additional infrastructure	ensure availability
der.18	Implement strong authentication for operationally critical functions, such as modifying configuration files,	a	require multi-factor authentication	for operationally critical functions, such as modifying configuration files	authenticate
der.18	Implement message authentication and message integrity mechanisms.	a	authenticate messages	containing alerts to microgrid	authenticate
der.18		a	check message integrity	for messages containing alerts to microgrid	check integrity
der.19	Implement RBAC for the utility's DERMS system,	a	use RBAC	in the utility's DERMS system	control access
der.19	Employ a data source authentication mechanism for the DERMS communication protocols,	a	authenticate data source	to access the DERMS	authenticate
der.19	Implement an information input validation mechanism for the DERMS control commands,	a	validate inputs	in the DERMS control commands	verify

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.19	Deploy message authentication and message integrity mechanisms.	a	authenticate messages	containing DER commands	authenticate
der.19		a	check message integrity	for messages containing DER commands	check integrity
der.20	Implement RBAC for the utility's DERMS system,	a	use RBAC	in the utility's DERMS system	control access
der.20	Implement a message authentication, information input validation, and message integrity mechanisms for the DERMS control commands.	a	authenticate messages	in the DERMS communication protocols	authenticate
der.20		a	validate inputs	(for consistency) in the DERMS control commands	verify
der.20		a	check message integrity	for the DERMS control commands	check integrity
der.21	Implement RBAC for the utility's DERMS system,	a	use RBAC	in the utility's DERMS system	control access
der.21	Implement confidentiality protection for data at rest	a	using approved cryptographic techniques	encrypt data at rest	specifically DER registration data
der.21		a	require approved cryptographic algorithms	for encrypting DER registration data	secure design and implementation

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.21	Deploy mechanisms for intrusion detection, auditing and event notification as part of the DERMS network and system management capabilities.	m	require intrusion detection and prevention	as part of the DERMS network and system management capabilities	detect
der.21		a	create audit log	that records accesses to the registration data files	audit
der.23	Implement authentication and access control mechanisms,	a	authenticate users		authenticate
der.23		m	restrict system access		control access
der.23	Implement an auditing mechanism.	a	create audit log	of interactions with the DERMS system that would have impact on the data ultimately sent to the utility	audit
der.24	Implement RBAC at the REP and the utility's DERMS system,	a	use RBAC	at the REP and in the utility's DERMS system	control access
der.24	Implement a message authentication mechanism for the DERMS protocols,	a	authenticate messages	in the DERMS protocols	authenticate
der.24	Provide non-repudiation capabilities for data communicated to the REP,	a	require non-repudiation	for data communicated to the REP	verify
der.24	Audit all accesses to confidential information in the DERMS system,	a	create audit log	of all accesses to confidential information in the DERMS system	audit

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
der.24	Deploy a notification mechanism for the DERMS, in the case of unauthorized access to confidential information.	a	generate alerts	in the case of unauthorized access to confidential information for the DERMS and send them to affected parties	alert
der.25	Implement access control and authentication mechanisms for the DER management system,	m	restrict application access	to the DER management system	control access
der.25		a	authenticate users	to the DER management system	authenticate
wampac.1	Access control mechanism for the PTP service,	m	restrict network service access	to the PTP service	control access
wampac.1	Implement separation between the PTP service and the auxiliary services running on the same server (resource prioritization),	a	isolate functions	between the PTP service and the auxiliary services running on the same server (e.g., resource prioritization)	isolate
wampac.1	Configure the PTP server for least functionality,	m	configure for least functionality	the PTP server	secure operations
wampac.1	Validate that the network stack, NTP and required auxiliary services running on the NTP server remain operational when subjected to erroneous traffic and large amounts of traffic,	m	verify correct operation	of the NTP server in order to remain operational when subjected to erroneous traffic and large amounts of traffic in the network stack, NTP and required auxiliary services	verify

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
wampac.1	Intrusion detection and prevention systems (IDS/IPS) may stop or prevent various types of attacks, including DoS attacks. IDS/IPS software must be tested prior to deployment to verify that it does not compromise normal operation of the system.	m	require intrusion detection and prevention		detect
wampac.1		m	test before install	to verify that the IDS/IPS solution does not compromise normal operation of the system	test
wampac.2	Link and application layer encryption on the WAMPAC network, digital signatures (or other strong authentication and integrity mechanisms) on commands and data received by the WAMPAC components,	a	encrypt link layer	on the WAMPAC network	encrypt
wampac.2		a	encrypt application layer	on the WAMPAC network	encrypt
wampac.2		a	check message integrity	(digital signatures) of commands and data received by the WAMPAC components	check integrity
wampac.2	Strong access control mechanism for the network and/or networking components,	m	restrict network access	to the network and/or networking components	control access

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
wampac.2	Monitoring the communication patterns between WAMPAC components to detect unauthorized devices and/or traffic.	m	detect unauthorized devices	in the WAMPAC network	detect
wampac.2		a	detect unusual patterns	in WAMPAC components traffic communications	detect
wampac.3		a	require redundancy	in PDCs using manufacturing diversity	ensure availability
wampac.3	Implement multi-layer security controls to prevent unauthorized individuals from gaining access to the PDC,	m	restrict network service access	at multiple layers to prevent unauthorized individuals from gaining access to the PDC	control access
wampac.3	Firewall traffic to the PDC,	m	restrict remote access	to the PDC	control access
wampac.3	Monitor the communication patterns to and from the PDC to detect unauthorized connections,	m	detect unauthorized connections	captured in the communication patterns to and from the PDC	detect
wampac.3	Using cryptography on the WAMPAC network for authentication and message integrity.	m	require approved cryptographic algorithms	for authentication and message integrity on the WAMPAC network	secure design and implementation
wampac.4	Strong authentication mechanisms for access to PDC,	a	authenticate users	for access to PDC	authenticate
wampac.4	Access control enforced at all interfaces to PDC,	m	restrict network service access	to all interfaces on the PDC	control access
wampac.4	Protection of credentials used to authenticate the PMU to the PDC,	a	protect credentials	used to authenticate the PMU to the PDC	secure design and implementation

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
wampac.4	Do not use known defaults, store and transmit credentials in encrypted format, protect cryptographic keys,	m	change default credentials		secure operations
wampac.4		a	encrypt data at rest	specifically credentials	encrypt
wampac.4		a	encrypt communication paths	used to transmit credentials	encrypt
wampac.4		a	require approved key management		secure design and implementation
wampac.4	Protect network hosting authentication database with firewalls, intrusion detection, network authentication and network monitoring,	m	restrict remote access	to the network hosting authentication database	control access
wampac.4		m	require intrusion detection and prevention	for the network hosting authentication database	detect
wampac.4		a	authenticate users	to the network hosting authentication database	authenticate
wampac.4		m	detect unauthorized access	to the network hosting authentication database	detect
wampac.4	Protection of security configuration data that lists the systems permitted to connect to the PDC.	m	protect security configuration	that lists the systems permitted to connect to the PDC	secure design and implementation

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
wampac.5	Reconfigurations place gateways in a test mode, which must be completed before the reconfiguration takes effect,	m	require reconfiguration in test mode	for gateways	test
wampac.5	The test results must be verified and approved by personnel/entities other than those that carried out the reconfiguration,	a	require 2-person rule	of test results that must be verified and approved by personnel/entities other than those that carried out the reconfiguration	verify
wampac.5	Monitoring for unexpected reconfigurations at the gateway level.	m	detect unauthorized configuration	at the gateway level	detect
wampac.6	Strong access control mechanism for the network and/or networking components,	m	restrict network access		control access
wampac.6	Monitor network traffic on the PMU/PDC communication links to detect and mitigate unauthorized traffic,	m	detect unauthorized access	in network traffic on the PMU/PDC communication links	detect
wampac.6	Monitor network traffic on the PMU/PDC communications links to detect and mitigate unauthorized traffic,	a	restrict network access	on the PMU/PDC communication links	control access
wampac.6	Implement traffic throttling mechanisms such as router access control lists (ACLs) and firewalls,	m	restrict network access	through traffic throttling mechanisms such as router access control lists (ACLs) and firewalls	control access

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
wampac.6	Use alternate stability analysis using SCADA data (using independent communication networks)	m	require redundancy	for the stability analysis using SCADA data (using independent communication networks)	ensure availability
wampac.6	IDS/IPS software may stop or prevent various types of attacks, including DoS attacks. IDS/IPS software must be tested prior to deployment to verify that it does not compromise normal operation of the system.	m	require intrusion detection and prevention		detect
wampac.6		m	test before install	of an IDS/IPS solution to verify that it does not compromise normal operation of the system	test
wampac.7	Firewall network traffic addressed to the historian,	m	restrict remote access	to the historian	control access
wampac.7	Implement multi-layer security controls to prevent unauthorized individuals from gaining access to the historian,	m	restrict application access	to prevent unauthorized individuals from gaining access to the historian	control access
wampac.7	Implement read-only access where possible for historian data,	m	require read-only access	to historian data	control access
wampac.7	Monitor the communication patterns to and from the historian to detect unauthorized connections,	m	detect unauthorized connections	in communications to and from the historian to detect unauthorized connections	detect

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
wampac.7	Monitor/alert unexpected activity on the measurement database,	m	detect abnormal behavior	on the measurement database	detect
wampac.7		a	generate alerts	for unexpected activity on the measurement database	alert
wampac.7	Use cryptography on the WAMPAC network for authentication and integrity.	a	check message integrity	(use cryptography) on the WAMPAC network	check integrity
wampac.8	Implement a configuration management process for controlling modifications to firmware to ensure that a PMU/PDC is protected against inadequate or improper modifications before, during, and after firmware manufacturing.	m	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	track
wampac.8	Use firmware with integrity checks	m	check software execution integrity	in firmware, since software may be compromised when loaded for execution	check integrity
wampac.8		m	restrict system access	for firmware install/updates	control access
wampac.10	Monitor configuration databases for changes or deletions,	m	detect unauthorized configuration	in the configuration databases	detect
wampac.10	Limit access to databases to either applications that require them, or local administrators that use multi factor authentication,	m	restrict database access	to applications that require access	control access

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
wampac.10		a	require multi-factor authentication	for local administrators that require access	authenticate
wampac.10	Encrypt the database contents related to the PMU configurations.	a	encrypt data at rest	for database contents related to the PMU configurations	encrypt
wampac.11	Strong access control mechanism for the network and/or networking components,	m	restrict network access		control access
wampac.11	Use redundant measurements at each substation end transmitted through an independent communication network to double-check the transmitted measurements	a	verify correct operation	by using redundant measurements at each substation end transmitted through an independent communication network to double-check the transmitted measurements	verify
wampac.11	Monitor network traffic on the substation communication links to detect and mitigate unauthorized traffic,	m	detect unauthorized access	on the substation communication links	detect
wampac.11		a	restrict network access	on the substation communication links	control access
wampac.11	Implement traffic throttling mechanisms such as router access control lists (ACLs) and firewalls,	m	restrict network access	to throttle network traffic, using solutions such as router access control lists (ACLs) and firewalls	control access

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
wampac.11	IDS/IPS software may stop or prevent various types of attacks, including DoS attacks. IDS/IPS software must be tested prior to deployment to verify that it does not compromise normal operation of the system.	m	require intrusion detection and prevention		detect
wampac.11		m	test before install	of IDS/IPS solution to verify that it does not compromise normal operation of the system	test
wampac.12	Employ a method to validate the GPS time signal using a redundant GPS signal transmitted through a communication network. Use a different synchronization mechanism for the synchrophasor signals (e.g., use NTP or PTP)	a	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)	verify
wampac.12	Use a different synchronization mechanism for the synchrophasor signals (e.g. use internal clocks rather than GPS for the time signal).	a	design for trust	in the synchronization mechanism for the synchrophasor signals (e.g. use internal clocks rather than GPS for the time signal)	secure design and implementation

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
wampac.12	Once the intrusion is detected, disconnect local GPS signal and either use GPS signal brought from another part of the grid through communication network or use internal clocks rather than GPS for the timing signal	a	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	ensure availability
et.1	Deploy fail-safe hardware in the battery that prevents overcharging, providing a physical prevention of such an attack,	a	protect from overcharge	by using a fail-safe battery hardware, providing a physical prevention of such an attack	enforce limits
et.1	Execute run time integrity checks on EV firmware,	a	check software execution integrity	in EV firmware, since software may be compromised when loaded for execution	check integrity
et.1	An authentication mechanism to permit firmware modification.	a	authenticate users	that modify firmware	authenticate
et.2	Strong authentication for access to configuration and software files for the fast-charging station management system,	a	authenticate users	for access to configuration and software files for the fast-charging station management system	authenticate
et.2	Monitor integrity of fast-charging station management software and configuration files,	a	check software file integrity	of fast-charging station management software and configuration files	check integrity

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.2	Design of management system to alarm on changes to settings such as the number of EVs allowed to charge simultaneously,	a	generate alarms	on changes to settings such as the number of EVs allowed to charge simultaneously in the design of the management system	alert
et.2	Circuit breaker to avoid overloading of distribution transformer.	a	require circuit breaker	to avoid overloading of distribution transformer	enforce limits
et.3	Rigorous change control processes for EV software at the factory and maintenance center, including employee background checks, code reviews, automated scans of the code base, logging of all code changes,	m	implement configuration management	of all code changes for EV software at the factory and maintenance center	track
et.3		m	verify personnel	at the factory and maintenance center	verify
et.3		m	conduct code review	of EV software at the factory and maintenance center	test
et.3		m	vulnerability scan before install	of EV software at the factory and maintenance center	test
et.3		m	create audit log	of all code changes to EV software at the factory and maintenance center	audit

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.3	Special anti-virus software in the public charging station system to check that system for any new, unauthorized software already present or detected in communications with the electric vehicles,	m	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	secure operations
et.3	Complete separation of communication interface for charging signals from that for other user data,	a	isolate networks	within the vehicle to separate the charging signals from other signals	isolate
et.3	Isolation of charging functions from safety-related functions within electric vehicles,	a	isolate functions	specifically charging functions from safety-related functions within electric vehicles	isolate
et.3	Run time integrity checking of EV software,	a	check software execution integrity	of EV software, since software may be compromised when loaded for execution	check integrity
et.3	Detection of any abnormal car functionality (e.g., break malfunctioning),	a	detect abnormal functionality	(e.g., break malfunctioning)	detect
et.3	Rapid assessment of any anomalous behavior of EVs to determine if it is caused by malicious code.	m	analyze anomalous events	to determine if any anomalous behavior is caused by malicious code of EVs	analyze
et.4	Continuous monitoring of enterprise perimeter protections,	a	detect abnormal behavior	in enterprise perimeter protections	detect
et.4	Automatic enforcement of password rules,	m	require password rule enforcement		secure operations

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.4	Encryption of database contents containing charging locations,	a	encrypt data at rest	for database contents containing charging locations	encrypt
et.4	Limit access to databases to either applications that require them, or local administrators that use strong authentication.	m	restrict database access	to applications that require them	control access
et.4		m	restrict database access	to local administrators that use strong authentication	control access
et.5	Manage the number of charging stations in a neighborhood based upon transformer capabilities,	m	restrict occurrence	of charging stations in a neighborhood based upon transformer capabilities	secure design and implementation
et.5	Integrity protections for translation modules.	a	check software file integrity	of translation modules	check integrity
et.6	Require strong authentication check between the EVSE and the smart meter,	m	authenticate devices	between the EVSE and the smart meter	authenticate
et.6	If possible, require a physical connection between the EVSE and smart meter along with some form of authentication,	m	require physical connection	specifically a wired connection between the EVSE and smart meter	secure design and implementation
et.6		a	authenticate devices	between the EVSE and smart meter	authenticate
et.6	Engineer the EVSE so that the definition of an associated meter is not changeable by customer.	m	prevent modification	of the EVSE so that the definition of an associated meter is not changeable by customer	control access

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.7	Encrypt data communications channels between an electric vehicle and the EVSE.	a	encrypt communication paths	between an electric vehicle and the EVSE	encrypt
et.8	Charging protocol that uses not easily forgeable data sent by the EV that allows the utility to determine it is an EV, (a) Currently, an EV does not exchange any data with the EVSE during charging. (b)Future EV systems are expected to have additional communications channels for data exchange with the EVSE usable for this purpose.	a	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, (a) Currently, an EV does not exchange any data with the EVSE during charging. (b)Future EV systems are expected to have additional communications channels for data exchange with the EVSE usable for this purpose.	authenticate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.8	Monitoring for 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,	a	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,	detect
et.9	Require entry of a verification code or personal identification number (PIN) with use of registration identity and include lockout functionality for multiple failed retries,	a	require PIN	(or verification code) with use of registration identity	authenticate
et.9		m	require lockout	for multiple failed retries	secure operations
et.9	Charging protocol that authenticates specific vehicles associated with a registration identity. This would require significant administration by the utility,	a	authenticate devices	with charging protocol that authenticates specific vehicles associated with a registration identity. This would require significant administration by the utility,	authenticate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.9	The EV ID could be tied to the owner of the EV (e.g., user ID or license ID) and all uses of the EV ID logged. Unauthorized use of the EV ID could be detected by the owner of the ID and anomalous uses centrally flagged for verification. This is parallel to a customer checking the usage history of his credit card on the web (or paper statement) today, and credit card company analysis and verification of unexpected card uses,	a	verify EV owner	association with the EV ID (e.g., user ID or license ID)	verify
et.9		a	create audit log	all uses of the EV ID	audit
et.9		a	detect unauthorized use	of the EV ID	detect
et.9	Other techniques used by credit card companies and ATMs that could be used for EVs: (a) Cancellation of ID and reissuance of a new one, (b) Refunds to customers for fraudulent charges,	m	learn from others	like credit card companies and ATMs for EVs: (a) Cancellation of ID and reissuance of a new one, (b) Refunds to customers for fraudulent charges,	learn
et.9	Complete separation of EV registration identity from payment method.	a	isolate functions	specifically EV registration identity from payment method	isolate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.10	Require entry of a verification code (VIN number) or PIN with use of the EV registration identity and include lockout functionality for multiple failed retries,	a	require PIN	or verification code (VIN number) with use of the EV registration identity	authenticate
et.10		m	require lockout	for multiple failed retries	secure operations
et.10	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,	a	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,	authenticate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.11	To make such a theft less attractive, design the registration identities to have less value to someone other than their owner: (a) Require entry of a verification code or PIN with use of registration identity with lockouts for multiple failed attempts, (b) Use a charging protocol that authenticates the specific EV being charged and that the EV is associated with the registration identity. This would require significant administration by the utility.	a	require PIN	or verification code with use of registration identity	authenticate
et.11		m	require lockout	for multiple failed attempts	secure operations
et.11		a	require authentication	using a charging protocol that authenticates the specific EV being charged and that the EV is associated with the registration identity	authenticate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.11	To make theft more difficult, improve access control for the utility network and database that stores registration identities by: (a) Applying least privilege principles to define the set of insiders authorized to access this data, (b) Ensuring that all methods of access to view the databases require the creation of an audit record of the individual viewing the data. Therefore, remote direct access to the database and access to applicable database files via the host operating system need to be strictly controlled.	a	enforce least privilege	by defining the set of insiders authorized to access registration identities	control access
et.11		a	create audit log	of the individual viewing registration identities	audit
et.11		m	restrict remote access	to the database	control access
et.11		m	restrict file access	to database files from the host operating system	control access
et.11	Limit access to the network hosting the database,	m	restrict network access	to the network hosting the database	control access
et.11	Encrypt database files and network traffic containing EV registration identities.	a	encrypt data at rest	for database files containing EV registration identities	encrypt

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.11		a	encrypt communication paths	of network traffic containing EV registration identities	encrypt
et.12	Design resilient communication paths for verifying registration identities,	m	require resiliency	in communication paths for verifying registration identities	ensure availability
et.12	Leverage credit card company concepts, using a central verification service that provides redundancy and resiliency,	m	learn from others	such as credit card company concepts like using a central verification service that provides redundancy and resiliency	learn
et.12	If individual charging stations determine their own rate regardless of the customers' utility membership (like existing gas stations), this scenario may not occur.	m	choose own rate	at individual charging stations, regardless of the customers' utility membership (like existing gas stations)	user decision
et.13	Log and alarm administrative activity that invalidates a registration identity using the customary user interface,	a	create audit log	of administrative activity that invalidates a registration identity using the customary user interface	audit
et.13		a	generate alarms	for administrative activity that invalidates a registration identity using the customary user interface	alert
et.13	Apply least privilege principles for individuals authorized to use this customary user interface,	a	enforce least privilege	for individuals authorized to use this customary user interface	control access

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.13	Ensure that all methods of access to view the databases require the creation of an audit record of the individual accessing the data. Therefore, remote direct access to the database and access to applicable database files via the host operating system need to be strictly controlled,	a	create audit log	of all methods of access to view the databases	audit
et.13		m	restrict remote access	to the database	control access
et.13		m	restrict file access	to applicable database files via the host operating system	control access
et.13	Ensure the validity of assumptions that in retail situations the customer with an invalid registration identity can pay with a credit card and that home charging is permitted (or defaults) at the standard rate.	m	validate assumption	that in retail situations the customer with an invalid registration identity can pay with a credit card	verify
et.13		m	validate assumption	that home charging is permitted at the standard rate	verify
et.14	Audit logs to track who has made software additions or modifications,	a	create audit log	of who has made software additions or modifications	audit

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.14	Conduct ongoing checks of live executables against correct versions using digital signatures or hashing techniques (that must resist replacement),	a	check software execution integrity	since software may be compromised when loaded for execution	check integrity
et.14	Other ways to verify the EV without directly accessing the EV registration system,	m	require redundancy	for ways to verify the EV without directly accessing the EV registration system	ensure availability
et.14	Separation of the vehicle charging process from the validation of EVs (such as a driver pumps gas in a gas station).	a	isolate functions	of the vehicle charging process from the validation of EVs (such as a driver pumps gas in a gas station)	isolate
et.15	Deploy circuit in EVs that stops discharging below a user-defined threshold,	a	enforce hardware limits	for circuit in EVs that stops discharging below a user-defined threshold	enforce limits
et.15	Charging station sends alarm to utility on detection of abnormal discharging behaviors,	a	generate alarms	for utility on detection of abnormal discharging behaviors in the charging station	alert
et.15	Circuit breaker to avoid reverse-directional overpower to the distribution transformer,	a	require circuit breaker	to avoid reverse-directional overpower to the distribution transformer	enforce limits
et.15	Strong authentication and authorization for access to software files for charging station management system,	a	authenticate users	seeking access to software files for charging station management system	authenticate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.15		m	restrict file access	to software files for charging station management system	control access
et.15	Monitor integrity of charging station management and protocol translation module software files.	a	check software file integrity	of charging station management and protocol translation module software files	check integrity
et.16	Apply strict access control and integrity monitoring to the charging station management system (ET.2),	m	restrict application access	to the charging station management system	control access
et.16		a	check software execution integrity	of the charging station management system, since software may be compromised when loaded for execution	check integrity
et.16	Strict monitoring of messages from EVs (ET.3) and EVSEs,	m	detect abnormal output	containing messages from EVs (ET.3) and EVSEs	detect
et.16	Assessment of anomalous behaviors of EVs to detect malicious code,	m	analyze anomalous events	in EVs to detect malicious code	analyze
et.16	Keep the charging station system up to date with security patches/anti-malware software,	m	maintain patches	in the charging station system	secure operations
et.16		m	maintain anti-virus	in the charging station system	secure operations
et.16	Use of cryptographic mechanisms to guarantee that each EVSE uses unique credentials,	a	require unique keys	in the EVSE	isolate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
et.16	Circuit breaker to avoid overloading of distribution transformer.	a	require circuit breaker	to avoid overloading the distribution transformer	enforce limits
dr.1	Ensure that default energy management settings are enabled if expected DR messages are not received within the appropriate time window,	m	require safe mode	in the energy management settings if expected DR messages are not received within the appropriate time window	secure operations
dr.1	Generate link status messages that require periodic acknowledgement and information returned on the health of the communications link. If no response, call the facility owner to restore availability,	a	require acknowledgment	of link status including information on the health of the communications link	verify
dr.1	Implement firewalls and network access control,	m	restrict remote access		control access
dr.1		m	restrict network access		control access
dr.1	Implement IDS and traffic monitoring,	m	require intrusion detection and prevention	where feasible along the communications channel	detect
dr.1		m	detect unauthorized access		detect
dr.1	Limit physical access to communications channel components,	m	restrict physical access	to communications channel components	control access
dr.1	Implement strong authentication for access to modify DRAS software,	a	authenticate users	seeking access to modify DRAS software	authenticate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dr.1	Implement strong authentication for remote access to modify customer DR software,	a	authenticate users	seeking remote access to modify customer DR software	authenticate
dr.1	Require responses from devices indicating what commands they received,	a	require acknowledgment	from devices indicating what commands they received	verify
dr.1	Perform random monitoring by non-DRAS (maybe supervisory control and data acquisition (SCADA)) systems of the results of DR commands to validate reasonability of load/generation results.	m	detect abnormal output	in the results of DR commands to validate reasonability of load/generation results by non-DRAS (maybe supervisory control and data acquisition (SCADA)) systems	detect
dr.2	Implement firewalls and network access control,	m	restrict remote access		control access
dr.2		m	restrict network access		control access
dr.2	Implement IDS and traffic monitoring,	m	require intrusion detection and prevention	where feasible along the communications channel	detect
dr.2		m	detect unauthorized access		detect
dr.2	Limit physical access to communications channel components,	m	restrict physical access	to communications channel components	control access
dr.2	Encrypt messages being transferred with unique keys per meter,	a	require unique keys	per meter for messages being transferred	isolate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dr.2	Use approved cryptographic algorithms and cryptographic modules to protect the confidentiality of communications.	m	require approved cryptographic algorithms	to protect the confidentiality of communications	secure design and implementation
dr.3	Customer equipment verifies authenticity and integrity of DR messages using digital signatures or message authentication codes,	a	check message integrity	(digital signatures or message authentication codes) to verify the authenticity and integrity of DR messages in customer equipment	check integrity
dr.3	Utility verifies authenticity of responses from customer DR systems,	a	authenticate messages	from customer DR systems	authenticate
dr.3	Use timestamps, sequence numbers, or cryptographic nonces on DR messages to detect replay attacks,	a	protect against replay	in DR messages using timestamps, sequence numbers, or cryptographic nonces	check integrity
dr.3	Use data validation to ensure the DR data is reasonable,	a	validate data	to ensure the DR data is reasonable	verify
dr.3	Implement network access control,	m	restrict network access	to the network hosting the DRAS system and the network on the customer side	control access
dr.3		m	require intrusion detection and prevention	where feasible along the communications channel	detect
dr.3		m	detect unauthorized access		detect

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dr.3	Implement anomaly detection algorithms on DRA to include a human in the decision loop when unexpected patterns or inputs are recognized,	a	detect unusual patterns	and include a human in the decision loop when unexpected patterns or inputs are recognized on DRA	detect
dr.3	Limit physical access to communications channel components,	m	restrict physical access	to communications channel components	control access
dr.3	Perform random monitoring by non-DRAS systems (such as SCADA) of the results of DR commands to validate reasonability of load/generation results.	m	detect abnormal output	in the results of DR commands to validate reasonability of load/generation results by non-DRAS systems (such as SCADA)	detect
dr.4	Limit which remote systems can access the DRAS systems,	m	restrict remote access	specifically to only those systems that are allowed remote access to the DRAS systems	control access
dr.4	Implement firewalls and network access control on the network hosting the DRAS,	m	restrict remote access	to the network hosting the DRAS	control access
dr.4		m	restrict network access	to the network hosting the DRAS	control access
dr.4	Utilize RBAC to limit access to the DRAS configuration,	a	use RBAC	to limit access to the DRAS configuration	control access
dr.4	Two-person rule on manual overrides or configuration changes in DRAS,	a	require 2-person rule	on manual overrides or configuration changes in the DRAS	verify
dr.4	Alerting on changes to the DRAS configuration,	a	generate alerts	on changes to the DRAS configuration	alert

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dr.4	Random monitoring of the results of DR commands by a non-DRAS (maybe SCADA) system to validate reasonability of load/generation results.	m	detect abnormal output	in the results of DR commands to validate reasonability of load/generation results by a non-DRAS (maybe SCADA) system	detect
dr.5	Keep DRAS and customer DR systems up to date with security patches/anti-malware software,	m	maintain patches	in the DRAS and customer DR systems	secure operations
dr.5		m	maintain anti-virus	in the DRAS and customer DR systems	secure operations
dr.5	Limit open ports and installed functions on DRAS and DR customer systems to those required,	m	configure for least functionality	by limiting open ports and installed functions in the DRAS and DR customer systems	secure design and implementation
dr.5	Limit physical access to DRAS or its input interfaces (e.g., Universal Serial Bus (USB), compact disk - read only memory (CD-ROM)),	m	restrict physical access	to DRAS or its input interfaces (e.g., Universal Serial Bus (USB), compact disk - read only memory (CD-ROM))	control access
dr.5	Implement strong authentication for remote access to a customer DR system,	a	authenticate users	for remote access to a customer DR system	authenticate
dr.6	Limit which remote systems can access the DRAS systems,	m	restrict remote access	to the DRAS systems	control access
dr.6	Implement firewalls and network access control on the networks hosting the DRAS systems,	m	restrict remote access	to the networks hosting the DRAS systems	control access

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dr.6		m	restrict network access	to the networks hosting the DRAS systems	control access
dr.6	Utilize RBAC to limit access to the DRAS software files,	a	use RBAC	to limit access to the DRAS software files	control access
dr.6	Make any unnecessary functions and ports unavailable on the DRAS systems.	m	configure for least functionality	by making unavailable any unnecessary functions and ports on the DRAS systems	secure design and implementation
dr.7	Keep the customer DR system up to date with security patches/anti-malware software,	m	maintain patches	on the customer DR system	secure operations
dr.7		m	maintain anti-virus	on the customer DR system	secure operations
dr.7	Implement strong authentication for remote access to a customer DR system,	a	authenticate users	seeking remote access to a customer DR system	authenticate
dr.7	Limit privileges to access the customer DR program,	a	enforce least privilege	for access to the customer DR program	control access
dr.7	Protect the customer network with firewalls,	m	restrict remote access	to the customer network	control access
dr.7	Implement a customer message verification solution.	a	require message verification	for customer messages	verify

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.1	Use of channel-hopping, spread-spectrum radios, and switching to alternate communication paths. Examples include: (a) Switching from licensed band(s) to unlicensed band(s), (b) Switching from unlicensed band(s) to licensed band(s), (c) Transition from RF to fiber or copper land-lines, (d) Transition from RF to dialup (possibly with degraded performance),	m	require spread-spectrum radio	with channel-hopping and switching to alternate communication paths. Examples include: (a) Switching from licensed band(s) to unlicensed band(s), (b) Switching from unlicensed band(s) to licensed band(s), (c) Transition from RF to fiber or copper land-lines, (d) Transition from RF to dialup (possibly with degraded performance)	ensure availability
dgm.1	Plan and use an alternate communications channel when the wireless channel is no longer available,	a	require redundancy	in communications channels when the wireless channel is no longer available	ensure availability
dgm.1	Ensure all feeder devices such as capacitor banks and voltage regulators have default states that rely on local electrical conditions if communications are lost,	m	require safe mode	in feeder devices such as capacitor banks and voltage regulators by having default states that rely on local electrical conditions if communications are lost	secure operations
dgm.2	Thoroughly vet service providers to ensure their services are secure and reliable,	m	verify personnel	(service providers) to ensure their services are secure and reliable	verify

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.2	Ensure customers sharing the network are reputable, security conscious and using network resources appropriately,	m	verify personnel	(customers) sharing the network to ensure they are reputable, security conscious and using network resources appropriately	verify
dgm.2	Ensure all feeder devices such as capacitor banks and voltage regulators have default states that rely on local electrical conditions if communications are lost,	m	require safe mode	in feeder devices such as capacitor banks and voltage regulators by having default states that rely on local electrical conditions if communications are lost	secure operations
dgm.3	Ensure strong access control of protective relays and other critical devices,	m	restrict device access	(both physical and logical) to protective relays and other critical devices	control access
dgm.3	Implement software and information integrity mechanisms,	a	check software execution integrity	of software in substation equipment, since software may be compromised when loaded for execution	check integrity
dgm.3	Disable unused console and engineering ports on intelligent electronic devices (IEDs),	m	configure for least functionality	by disabling unused console and engineering ports on intelligent electronic devices (IEDs)	secure design and implementation
dgm.3	Log all substation actions and alarm any serious anomalies, such as connection changes and device configuration changes,	a	create audit log	of substation actions	audit

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.3		a	generate alarms	for any serious anomalies, such as connection changes and device configuration changes in substations	alert
dgm.3	Enhance physical security access controls and surveillance or enhance engineering access controls or both,	m	restrict physical access	to substation using, for example, card swipes, pin codes, etc	control access
dgm.3		a	require video surveillance	of the human interfaces to the DGM equipment	secure operations
dgm.3		m	restrict access	to engineering functions	control access
dgm.3	Keep substation equipment updated to the latest firmware / patch level,	m	maintain latest firmware	for substation equipment	secure operations
dgm.3		m	maintain patches	for substation equipment	secure operations
dgm.3	Install software to restrict access to USB ports on substation equipment.	m	restrict port access	of USB ports on substation equipment	control access
dgm.4	Ensure strong access control of protective relays and other critical devices,	m	restrict remote access	to protective relays and other critical devices	control access
dgm.4	Log all substation actions and alarm any serious anomalies, such as connection changes and device configuration changes,	a	create audit log	of substation actions	audit

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.4		a	generate alarms	for any serious anomalies, such as connection changes and device configuration changes in substations	alert
dgm.4	Keep substation and communication updated to the latest firmware / patch level,	m	maintain patches	for all substation and communication equipment	secure operations
dgm.4		m	maintain latest firmware	for all substation and communication equipment	secure operations
dgm.4	Install antivirus software or application white listing software on substation equipment where feasible,	m	maintain anti-virus	on substation equipment	secure operations
dgm.4	Configure the substation network to use authentication (possibly two factor authentication) and encryption via VPNs.	a	authenticate users	in the substation network (possibly two factor authentication)	authenticate
dgm.4		m	require VPNs	in the substation network	encrypt
dgm.5	Validate all patches to programs and create a robust change control policy,	m	maintain patches		secure operations
dgm.5		m	implement configuration management		track

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.5	Log all program changes and updates through automated logging techniques,	a	create audit log	of all program changes and updates	audit
dgm.5	Monitor voltage on feeders via selected AMI meters or alternative devices that provide redundant information,	a	detect abnormal behavior	of voltage on feeders via selected AMI meters or alternative devices that provide redundant information	detect
dgm.5	Provide strong integrity mechanisms such as digital signatures for driver installation,	a	check software file integrity	(digital signatures) for driver installation	check integrity
dgm.5	Incorporate host-based intrusion detection on DMS,	m	require intrusion detection and prevention	on DMS hosts	detect
dgm.5	Configuration management of all software updates including patches and firmware updates,	m	implement configuration management	for all software updates including patches and firmware updates	track
dgm.5	Install antivirus software or application white listing software on DMS hosts,	m	maintain anti-virus	on DMS hosts	secure operations
dgm.5	Have a hot running backup DMS ready when primary DMS is inoperable.	m	require backup	when primary DMS is inoperable	ensure availability
dgm.6	Add authentication to communication from field devices to control centers,	a	authenticate devices	in communication from the field to control centers	authenticate
dgm.6	Increase communication security by adding encryption and stronger access controls.	m	restrict communication access		control access

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.6		a	encrypt communication paths		encrypt
dgm.7	Implement a mechanism that classifies end devices based on their profile of ports and traffic,	a	profile equipment	(end devices) based on their profile of ports and traffic	profile
dgm.7	Improved trust models,	m	design for trust		secure design and implementation
dgm.7	Implement strong access controls and account management practices to prevent unauthorized access to the network,	m	restrict network access	to the network	control access
dgm.7	Use encryption and authentication techniques to prevent spoofing.	m	encrypt communication paths	to prevent spoofing	encrypt
dgm.7		a	authenticate users	to prevent spoofing	authenticate
dgm.8	Stock spares of critical components,	m	require spares	for critical components	ensure availability
dgm.8	For developers of equipment, rigorous development change control processes including employee background checks, code reviews, automated scans of the code base and logging of all code changes,	m	implement configuration management	for developers of equipment	track
dgm.8		m	verify personnel	(developers of equipment) including employee background checks	verify

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.8		m	conduct code review		test
dgm.8		m	vulnerability scan before install	of the code base	test
dgm.8		m	create audit log	of all code changes	audit
dgm.8	Introduce the concept of devices of varying degrees of trust along with associated certifications for their associated supply chains,	m	design for trust	of devices including varying degrees of trust along with associated certifications for their associated supply chains	secure design and implementation
dgm.8	Conduct extensive background checks on utility employees and contract maintenance personnel, especially those that directly interact with field devices.	m	verify personnel	with extensive background checks on utility employees and contract maintenance personnel, especially those that directly interact with field devices	verify
dgm.9	Ensure good configuration management of the DGM before and after disasters,	m	implement configuration management	in the DGM before and after disasters	track
dgm.9	Create strong and up to date policies and procedures for emergency response that ensure security during a recovery effort,	m	define policy	for emergency response that ensures security during a recovery effort	plan
dgm.9		m	define procedures	for emergency response that ensures security during a recovery effort	plan

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.9	Prioritize physical security including personnel authentication and access control during the recovery effort,	m	prioritize recovery activities	for physical security including personnel authentication and access control during the recovery effort	plan
dgm.9	Review recovery response after the disaster to verify repairs, configurations, and changes are correct.	m	review recovery response	after the disaster to verify repairs, configurations, and changes are correct	analyze
dgm.10	Educate employees 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,	m	train personnel	on the threat of social engineering attacks and perform social engineering exercises (such as company generated phishing emails or rogue USB drives)	train
dgm.10	Implement synchronous closing control, surge arrestors, or pre-insertion resistors to minimize capacitor bank switching transients,	a	require synchronous functions	for closing control, surge arrestors, or pre-insertion resistors to minimize capacitor bank switching transients	ensure availability
dgm.10	Increase physical security of engineering consoles and HMIs and strictly control their access,	m	restrict physical access	to engineering consoles and HMIs	control access
dgm.10	Institute single sign-on practices.	a	require single sign-on		authenticate
dgm.11	Require strong passwords with complexity requirements on company devices and systems,	m	require strong passwords	for company devices and systems	secure operations

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.11	Protect company information and documents from unauthorized disclosure through training and implementing corporate policies on handling sensitive information. This includes one-lines, equipment information, communication architectures, protection schemes, load profiles, etc.,	m	train personnel	to protect company information and documents from unauthorized disclosure	train
dgm.11		m	define policy	on handling sensitive information. This includes substation one-line diagrams, equipment information, communication architectures, protection schemes, load profiles, etc.	plan

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.11	Train 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,	m	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	train
dgm.11	Log and alert all changes in HMI control actions,	a	create audit log	of all changes in HMI control actions	audit
dgm.11		a	generate alerts	for all changes in HMI control actions	alert
dgm.11	Prohibit or restrict remote vendor connections (e.g. physically disconnect remote connections when not in use),	m	restrict remote access	of remote vendor connections (e.g. physically disconnect remote connections when not in use)	control access
dgm.11	Encrypt distribution control communications,	a	encrypt communication paths	for distribution control communications	encrypt
dgm.11	Apply strict policy that requires two person verification of correct DMS configuration and keep configuration documents up to date,	a	require 2-person rule	for correct DMS configuration	verify
dgm.11		m	implement configuration management	for configuration documents	track

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.11	Provide defense in depth by segmenting distribution control network.	m	isolate networks	(distribution control networks)	isolate
dgm.12	Incorporate strong authentication and encryption techniques for wireless communications,	a	authenticate users	of wireless communications	authenticate
dgm.12		a	encrypt communication paths	for wireless communications	encrypt
dgm.12	Replace wireless communications with wired ones,	m	design for trust	by replacing wireless communications with wired ones	secure design and implementation
dgm.12	Log all changes in control functions and set points, and alert on unusual changes.	a	create audit log	of all changes in control functions and set points	audit
dgm.12		a	generate alerts	for unusual changes	alert
dgm.13	Incorporate and enforce a comprehensive account management policy that removes old or unused accounts in a timely manner,	m	configure for least functionality	by removing old or unused accounts in a timely manner	secure design and implementation
dgm.13	Install sensors at critical loads that alarm loss of power to ensure timely restoration of power.	a	generate alarms	for loss of power to ensure timely restoration of power	alert
dgm.14	Incorporate authentication and strong passwords on serial communications,	a	authenticate users	of serial communications using strong passwords	authenticate

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.14	Install low latency endpoint encryption devices to encrypt serial communications,	a	encrypt communication paths	for serial communications using low latency encryption devices	encrypt
dgm.14	Migrate serial communications to field devices from public phone lines to private communication channels.	m	design for trust	and migrate serial communications to field devices from public phone lines to private communication channels	secure design and implementation
dgm.15	Implement technical and procedural controls that disallow remote DMS control actions on lines and equipment that are under maintenance,	m	define procedures	that will disallow remote DMS control actions on lines and equipment that are under maintenance	plan
dgm.15	Require strong passwords with complexity requirements on company devices and systems,	m	require strong passwords	with complexity requirements on company devices and systems	secure operations
dgm.15	Protect company information and documents from unauthorized disclosure through training and implementing corporate policies on handling sensitive information. This includes one-lines, equipment information, communication architectures, protection schemes, load profiles, etc.,	m	train personnel	to protect company information and documents from unauthorized disclosure	train

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.15		m	define policy	on handling sensitive information. This includes one-lines, equipment information, communication architectures, protection schemes, load profiles, etc.	plan
dgm.15	Train 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,	m	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	train
dgm.15	Log and alert all changes in HMI control actions,	a	create audit log	of all changes in HMI control actions	audit
dgm.15		a	generate alerts	for all changes in HMI control actions	alert
dgm.15	Prohibit or restrict remote vendor connections (e.g. physically disconnect remote connections when not in use),	m	restrict remote access	using remote vendor connections (e.g. physically disconnect remote connections when not in use)	control access
dgm.15	Encrypt distribution control communications,	a	encrypt communication paths	for distribution control communications	encrypt

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
dgm.15	Apply strict policy that requires two person verification of correct DMS configuration and keep configuration documents up to date,	a	require 2-person rule	for DMS configuration	verify
dgm.15		m	implement configuration management	of DMS configuration documents	track
dgm.15	Provide defense in depth by segmenting distribution control network.	m	isolate networks	(distribution control networks)	isolate
generic.1	Implement strict separation of duties,	m	require separation of duty		isolate
generic.1	Use RBAC to limit access,	a	use RBAC	to limit access	control access
generic.1	Implement protection mechanisms and situational awareness (SIEM, IDS, firewalls, logging, and monitoring) of control networks to detect abnormal and/or out-of-policy behavior by authorized users,	a	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)	detect
generic.1	Increased situational awareness initiatives should include adequate policies, procedures, guidelines, and accompanying technical controls concerning access to security-relevant and operationally critical functionality,	m	define procedures	concerning access to security-relevant and operationally critical functionality	plan

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
generic.2	Segregate business and controls systems networks using air-gapped equipment at the network and host level,	m	isolate networks	that host business systems from those that host control systems	isolate
generic.2	Properly implement a secure SIEM and monitor alerts according to the risks associated,	a	generate alerts	using a SEIM and monitor alerts according to the risks associated	alert
generic.2	Create a defensible, defense in depth, network architecture which includes a demilitarized zone (DMZ), firewalls, IDS etc.,	m	isolate networks	with a defensible, defense in depth, network architecture that includes a demilitarized zone (DMZ), firewalls, IDS etc.	isolate
generic.2		m	enforce restrictive firewall rules		control access
generic.2		m	require intrusion detection and prevention		detect
generic.2	Train personnel to monitor traffic to and from the Internet to recognize when an incident is occurring,	m	train personnel	to monitor traffic to and from the Internet to recognize when an incident is occurring	train

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
generic.2	Develop a comprehensive incident response process to reduce response time when incident do occur. Develop a contingency plan as part of the incident response process to maintain adequate resiliency in high-priority control systems.	m	define incident response plan	to reduce response time when incidents do occur	plan
generic.2		m	define contingency plan	as part of the incident response plan to maintain adequate resiliency in high-priority control systems	plan
generic.3	Restrict access by permanently physically disabling the interfaces with epoxy or other methods or using software controls to restrict access to interfaces on equipment,	m	configure for least functionality	by permanently physically disabling unnecessary interfaces with epoxy or other methods or physically removing them	secure design and implementation
generic.3	Remove or disable unnecessary interfaces from equipment,	m	configure for least functionality	by using software controls or other non-physical methods to disable unnecessary interfaces on equipment	secure design and implementation
generic.3	Verify the settings on equipment before the equipment is installed in the field,	m	verify settings	on equipment before the equipment is installed in the field	verify

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
generic.3	If possible, test equipment before it is installed in the field,	m	test before install	of equipment in the field	test
generic.3	Perform vulnerability or port scans on equipment before it is installed in the field,	m	vulnerability scan before install		test
generic.3	Perform periodic walk-downs of equipment to help ensure there are not any new unauthorized devices connected,	m	require periodic walk-downs	of equipment to help ensure there are not any new unauthorized devices connected	verify
generic.3	Implement strict policies outlining acceptable and unacceptable use of portable computing devices in a business/corporate local area network (LAN) environment and a control LAN environment,	m	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	plan
generic.3	Implement a user awareness training program that includes portable media guidelines.	m	train personnel	under a user awareness training program that includes portable media guidelines	train
generic.4	Develop a procurement service level agreement (SLA) which verifies the manufacture and origin of equipment from a known good and reputable source,	m	define SLA	for procurement which verifies the manufacture and origin of equipment from a known good and reputable source	plan

Failure Scenario	Original Mitigation	Type	Common Action	Action Application	Action Group
generic.4	Develop disposal policy and procedures which prevent the acquisition of sensitive parts from excessed or disposed devices,	m	define policy	addressing disposal which prevents the acquisition of sensitive parts from excessed or disposed devices	plan
generic.4	Use approved cryptography to prevent a threat agent from reverse engineering devices which are acquired outside of the legitimate supply chain,	m	require approved cryptographic algorithms	to prevent a threat agent from reverse engineering devices which are acquired outside of the legitimate supply chain	secure design and implementation
generic.4	Periodic audits of supply chain to ensure adequate quality control,	m	perform audit	of the supply chain periodically to ensure adequate quality control	audit
generic.4	Implement and maintain a system of continuous monitoring of the system network to detect unauthorized communications or behavior by deployed devices,	a	detect abnormal behavior	that may indicate supply chain issues, such as unauthorized communications or behavior by deployed devices in the system network	detect