DRAFT NISTIR 7628 Revision 1

Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References

The Smart Grid Interoperability Panel
– Smart Grid Cybersecurity Committee

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

DRAFT NISTIR 7628 Revision 1

Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References

The Smart Grid Interoperability Panel –Smart Grid Cybersecurity Committee

October 2013

U. S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Interagency Report 7628 Rev. 1, vol. 3
235 pages (October 2013)

Comments on this publication may be submitted to: NISTIR.7628.Rev1@nist.gov
Public comment period: October 25 – December 24, 2013

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: NISTIR.7628.Rev1@nist.gov
Comment form available at: http://csrc.nist.gov/publications/drafts/nistir-7628-r1/nistir7628_r1_vol3_comments_template.xlsx

Reports on computer systems technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

This three-volume report, *Guidelines for Smart Grid Cybersecurity*, presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of Smart Grid stakeholders—from utilities to providers of energy management services to manufacturers of electric vehicles and charging stations—can use the methods and supporting information presented in this report as guidance for assessing risk and identifying and applying appropriate security requirements. This approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment. Each organization's cybersecurity requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify.

Keywords

advanced metering infrastructure; architecture; cryptography; cybersecurity; electric grid; privacy; security requirements; smart grid

ACKNOWLEDGMENTS

This revision to the NISTIR was developed by members of the Smart Grid Interoperability Panel (SGIP) Smart Grid Cybersecurity Committee (SGCC) (formerly the Cyber Security Working Group (CSWG)), which is chaired by Marianne Swanson (NIST). Dave Dalva (Stroz Friedberg), Akhlesh Kaushiva (Department of Energy), and Scott Saunders (Sacramento Municipal Utility District) are the vice chairs and Mark Enstrom (Neustar) and Amanda Stallings (Ohio PUC) have served as the secretary. Tanya Brewer of NIST is the lead editor of this report. A special note of thanks goes to the subgroup leads, Frances Cleveland (Xanthus Consulting International), Victoria Pillitteri and Nelson Hastings (NIST), Rebecca Herold (Rebecca Herold & Associates, LLC), Elizabeth Sisley (Calm Sunrise Consulting, LLC), and Doug McGinnis (Exelon) who along with their subgroup team members contributed significantly to this revision. The dedication and commitment of all the individuals in developing the original document and now this revision is significant. In addition, appreciation is extended to the various organizations that have committed these resources to supporting this endeavor. Past and current members of the CSWG are listed in Appendix J of this report.

Acknowledgement is also extended to the NIST Smart Grid Team and to Liz Lennon (NIST) for her superb technical editing of this report. Thanks is also extended to Bruce McMillin (Missouri University of Science and Technology), and to Harold Booth and Quynh Dang (NIST) for assistance in updating specific sections in the document. Finally, acknowledgment is extended to all the other individuals who have contributed their time and knowledge to ensure this report addresses the security needs of the Smart Grid.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

[This page intentionally left blank.]

OVERVIEW AND REPORT ORGANIZATION

REPORT OVERVIEW

This document (the original NISTIR and Revision 1) is the product of a participatory public process that, starting in March 2009, included workshops as well as weekly and bi-weekly teleconferences, all of which were open to all interested parties. Drafts of the three volumes will have undergone at least one round of formal public review before final publication. The public review cycle will be announced in The Federal Register in advance.

AUDIENCE

This report is intended for a variety of organizations that may have overlapping and different perspectives and objectives for the Smart Grid. For example—

- *Utilities/asset owners/service providers* may use this report as guidance for a specific Smart Grid information system implementation;
- *Industry/Smart Grid vendors* may base product design and development, and implementation techniques on the guidance included in this report;
- *Academia* may identify research and development topics based on gaps in technical areas related to the functional, reliability, security, and scalability requirements of the Smart Grid; and
- *Regulators/policy makers* may use this report as guidance to inform decisions and positions, ensuring that they are aligned with appropriate power system and cybersecurity needs.

CONTENT OF THE REPORT

- Volume 1 – Smart Grid Document Development Strategy, Architecture, and High-Level Requirements
  - Chapter 1 – *Document Development Strategy* includes background information on the Smart Grid and the importance of cybersecurity in ensuring the reliability of the grid and the confidentiality of specific information. It also discusses the strategy used to develop this document.
  - Chapter 2 – *Logical Architecture* includes a high level diagram that depicts a composite high level view of the actors within each of the Smart Grid domains and includes an overall logical reference model of the Smart Grid, including all the major domains. The chapter also includes individual diagrams for each of the 22 logical interface categories. This architecture focuses on a short-term view (1–3 years) of the Smart Grid.
  - Chapter 3 – *High-Level Security Requirements* specifies the high-level security requirements for the Smart Grid for each of the 22 logical interface categories included in Chapter 2.

- Chapter 4 – *Cryptography and Key Management* identifies technical cryptographic and key management issues across the scope of systems and devices found in the Smart Grid along with potential alternatives.
- Appendix A – *Crosswalk of Cyber Security Documents*
- Appendix B – *Example Security Technologies and Procedures to Meet the High Level Security Requirements*

- Volume 2 – Privacy and the Smart Grid
  - Chapter 5 – *Privacy and the Smart Grid* includes a privacy impact assessment for the Smart Grid with a discussion of mitigating factors. The chapter also identifies potential privacy issues that may occur as new capabilities are included in the Smart Grid.
  - Appendix C – *State Laws – Smart Grid and Electricity Delivery*
  - Appendix D – *Privacy Use Cases*
  - Appendix E – *Privacy Related Definitions*
- Volume 3 – Supportive Analyses and References
  - Chapter 6 – *Vulnerability Classes* includes classes of potential vulnerabilities for the Smart Grid. Individual vulnerabilities are classified by category.
  - Chapter 7 – *Bottom-Up Security Analysis of the Smart Grid* identifies a number of specific security problems in the Smart Grid. Currently, these security problems do not have specific solutions.
  - Chapter 8 – *Research and Development Themes for Cyber Security in the Smart Grid* includes R&D themes that identify where the state of the art falls short of meeting the envisioned functional, reliability, and scalability requirements of the Smart Grid.
  - Chapter 9 – *Overview of the Standards Review* includes an overview of the process that is being used to assess standards against the high level security requirements included in this report.
  - Chapter 10 – *Key Power System Use Cases for Security Requirements* identifies key use cases that are architecturally significant with respect to security requirements for the Smart Grid.
  - Appendix F – *Logical Architecture and Interfaces of the Smart Grid*
  - Appendix G – *Analysis Matrix of Interface Categories*
  - Appendix H – *Mappings to the High Level Security Requirements*
  - Appendix I – *Glossary and Acronyms*
  - Appendix J – *SGIP-CSWG and SGIP 2.0 SGCC Membership*

CHAPTER 6
VULNERABILITY CLASSES

6.1 INTRODUCTION

This section is intended to be used by those responsible for designing, implementing, operating or procuring some part of the electric grid. It contains a list of five classes of potential vulnerabilities with descriptions of specific areas that can make an organization vulnerable as well as the possible impacts to an organization should the vulnerability be exercised. For the purpose of this document, a vulnerability class is a category of weakness which could adversely impact the operation of the electric grid. A "vulnerability" is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. This document contains a number of possible vulnerabilities, identified by management, operational and technical categories. It is best used as a stimulus for detailed risk analysis of real or proposed systems, and while it was created from many sources of vulnerability information, including NIST Special Publication (SP) 800-82, *Guide to Industrial Control Systems Security*, and 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, Open Web Application Security Project (OWASP) vulnerabilities, Common Weakness Enumeration (CWE) vulnerabilities, attack documentation from Idaho National Laboratory (INL), input provided by the NIST CSWG Bottom-Up group, and the North American Electric Reliability Corporation Critical Infrastructure Protection Standards (NERC CIP) standards, it is just a starting point for more detailed vulnerability identification in future SGCC work efforts.

6.2 PEOPLE, POLICY & PROCEDURE

Policies and procedures are the documented mechanisms by which an organization operates, and *people* are trained to follow them. Policies and procedures lay the groundwork for how the organization will operate; adequate training ensures that people understand how to and are responsible for implementing the policy and procedures. Individually, each is not effective without the others and should not be implemented as discreet elements. This section discusses cases where a failure in, lack of, or deficiency in policies and procedures can lead to security risks for the organization. An organization's policies and procedures are often the final protective or mitigating control against security breaches, and those policies and procedures should be examined closely to ensure that they are consistent with both the inherent business objectives and with secure operations.

6.2.1 Training

This category of vulnerabilities is related to personnel security awareness training associated with implementing, maintaining, and operating systems.

6.2.1.1 Insufficiently Trained Personnel

Description

Throughout the entire organization everyone needs to acquire a level of security awareness training; the degree of training should vary based on the technical responsibilities and/or the critical assets one is responsible for.

Through training, everyone in the organization gets a clear understanding of the importance of cybersecurity, but more importantly everyone begins to understand the role they play and the importance of each role in supporting security.

Examples

- Freely releasing information of someone's status, i.e. away on vacation, not in today, etc.,
- Opening emails and attachments from unknown sources,
- Posting passwords for all to see,
- Allowing people to dumpster-dive without alerting security, and
- Failure to notice inappropriate or suspicious network cables/devices outside the building.

Potential Impact:

Social engineering is used in acquiring as much information as possible about people, organizations and organizational operations. Insufficiently trained personnel may inadvertently provide the visibility, knowledge and opportunity to execute a successful attack.

6.2.1.2 Inadequate Security Training and Awareness Program

Description

An adequate security awareness program is a key element of an organization's policy framework to guard against vulnerabilities introduced by insufficiently trained personnel. Such programs highlight the need for a continuous retraining effort over an organization-defined period of time. The security profile will always be changing and so will the need for new procedures, new technologies, and reinforcement of the importance of the cybersecurity program.

Potential Impact

An inadequately trained workforce will not be aware of the policies and procedures necessary to secure organizational information and equipment, resulting in the potential for weaknesses to be exploited, for example:

- Inserting malicious USB sticks found in the parking lot into machines with access to control systems providing attackers control over the control systems.
- Holding the door for potential attackers carrying a big box entering a "secured premise", allowing them unauthorized access and physical proximity to critical / control systems.
- Surfing porn sites, which often includes 0-day exploits and can compromise workstations with bots or worms.

- Failing to respond to someone capturing wireless network traffic on the front lawn or parked in the guest parking lot, and
- Lack of care with id badges and credentials which can be leveraged to gain partial or complete access to critical control systems.

6.2.2 Policy & Procedure

6.2.2.1 Insufficient Identity Validation, Background Checks

Description

Identity validation/background checks are based on the individual's area of responsibility, the physical facilities/hardware/systems, and the type of information authorized to access. The more sensitive information available to an individual, the deeper and more detailed the identity validation and background check process should be.

Use of known references and background checks by established groups should be implemented.

Potential Impact

The human factor should always be considered the weakest element within any organization's security posture, thus identity validation and background checks are measures that are imperative in managing this risk. As the amount and sensitivity of the information and physical access to critical facilities/hardware/systems one is given responsibility for increases, consideration should be given to requiring separation of duties to ensure that no one individual is given "the keys to the kingdom."

6.2.2.2 Inadequate Security Policy

Description

Security policies must be structured with several key elements, be well understood, embody a practical approach, be well practiced and monitored, and be enforceable.

Additonally, they must be flexible enough that they can be continuously improved.

Potential Impact

Vulnerabilities are often introduced due to inadequate development or implementation policies or the lack of policies. Policies need to drive operating requirements and procedures, including security training.

6.2.2.3 Inadequate Privacy Policy

Description

A privacy policy should be established that documents the necessity of protecting private/personal information to help ensure that data is not exposed or shared unnecessarily.

Potential Impact

Insufficient privacy policies can lead to unwanted exposure of employee or customer/client personal information, leading to both business risk and security risk.

6.2.2.4 Inadequate Patch Management Process

Description

A patch management process is necessary to ensure that software and firmware are kept current to remediate against known vulnerabilities, or that a proper risk analysis and mitigation process is in place when patches cannot be promptly installed.

Potential Impact

Missing patches on firmware and software have the potential to present serious risk to the affected system.

6.2.2.5 Inadequate Change and Configuration Management

Description

Change and configuration management processes are essential to helping ensure that system configurations are governed appropriately in order to maximize overall system reliability.

Examples

- Changing software configuration enables an insecure profile,
- Adding vulnerable hardware,
- Changing network configuration that reduces the security profile of the system,
- Introduction of tampered devices into the system,
- Security organization not having a sign-off approval in the configuration management process, and
- Making a change to network configuration or software and failing to document that change.

Potential Impact

Improperly configured software/systems/devices added to existing software/systems/devices can lead to insecure configurations and increased risk of vulnerability.

6.2.2.6 Unnecessary System Access

Description

As a matter of policy, it needs to be very clear that system access and information is granted only on an as-needed basis. System access needs to be managed, monitored, and enforced based on the individual's access requirements and the level of impact that uncontrolled access could have on an organization.

Potential Impact

System access that is not managed can result in personnel obtaining, changing or deleting information they are no longer authorized to access, as well as:

- Administrators with false assumptions of what actions any one user may be capable of;
- Individual users with sufficient access permissions to cause complete failure or failure of large portions of the electric grid;
- The inability to prove responsibility for a given action or hold a party accountable;
- Accidental disruption of service by untrained individuals; and
- Raised value for credentials of seemingly insignificant personnel.

6.2.3 Risk Management

Deficiencies in a risk management program can lead to vulnerabilities throughout the organization. A well documented and implemented risk management program that encompasses the organization level, mission and business process level, and the IT system and industrial control system (ICS) level[1] will provide an in depth defense against many potential vulnerabilities.

6.2.3.1 Inadequate Periodic Security Audits

Description

Conducting independent security audits as part of the organization's continuous monitoring program should review and examine a system's records and activities to determine the adequacy of system security requirements and ensure compliance with established security policies and procedures. Audits should also be used to detect breaches in security services and recommend changes, which may include making existing security requirements more robust and/or adding new security requirements. Audits should not rely exclusively on interviews with system administrators.

Potential Impact

The audit process is the only true measure by which it is possible to continuously evaluate the status of the implemented security program in terms of conformance to policy, determine whether there is a need to enhance policies and procedures, and evaluate the robustness of the implemented security technologies.

6.2.3.2 Inadequate Security Oversight by Management

Description

An overall security program requires coordination and communication between organizational operating groups, has impact across many business areas, and requires an element of human

[1] For more about risk management and these levels, *see* The Department of Energy Risk Management Process, which can be obtained from http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

resourses and legal involvement. Without senior management oversight and ownership, it is very difficult to maintain a successful security program. A significant challenge can exist in establishing senior management oversight and ownership at the executive level within an organization.

Potential Impact

Lack of clear senior management ownership of a security program makes it almost impossible to enforce the provisions of the program in the event of a policy being compromised or abused.

6.2.3.3 Inadequate Continuity of Operations or Disaster Recovery Plan

Description

As part of the organization's incident response capabilities, it is essential to ensure within the various system disaster recovery plans that an associated cyber contingency plan and cybersecurity incident response plan are developed. Each system disaster recovery plan should highlight the need to determine if the disaster resulted from or is related to a cybersecurity incident. If such is the case, then part of the recovery process must be to ensure cyber incident recovery and contingency activities are implemented. This means taking added steps like validating backups, ensuring devices being recovered are clean before installing the backups, incident reporting, etc.

Potential Impact

An inadequate continuity of operations or disaster recovery plan could result in longer than necessary recovery from a possible plant or operational outage.

6.2.3.4 Inadequate Risk Assessment Process

Description

A documented risk assessment process should include consideration of business objectives, the impact to the organization if vulnerabilities are exploited, and the determination of the acceptable risk level by senior management is necessary to evaluate risk to the organization.

Potential Impact

Lack or misapplication of adequate risk assessment processes can lead to poor decisions based on inadequate understanding of actual risk.

6.2.3.5 Inadequate Incident Response Process

Description

An incident response process is required to ensure proper notification, response, and recovery in the event of an incident. Incident response capabilities should be coornidated with continuity of operations and disaster recovery capabilities.

Potential Impact

Without a sufficient incident response process, response-time critical actions may not be completed in a timely manner, leading to increased duration of risk exposure.

6.3 PLATFORM SOFTWARE/FIRMWARE VULNERABILITIES

Software and firmware are the programmable components of a computing environment. Errors or oversights in software and firmware design, development, and deployment may result in unintended functionality that allows attackers or other conditions to affect, via programmatic means, the confidentiality, integrity, and/or availability of information. These errors and oversights are discovered and reported as vulnerability instances in platform software and firmware. Discovery and reporting of vulnerability instances occurs continuously and the Common Vulnerability and Exposures (CVE) specification establishes a common identifier for known vulnerability instances. [§6.6-5] The Common Weakness Enumeration (CWE) [§6.6-4] and the Vulnerability Categories defined by OWASP [§6.6-1] are two taxonomies which provide descriptions of common errors or oversights that can result in vulnerability instances. Using the CWE and OWASP taxonomies as a guide this subsection describes classes and subclasses of vulnerabilities in platform software and firmware[2].

6.3.1 Software Development

Applications being developed for use in the Smart Grid should make use of a secure software development life cycle (SDLC). Vulnerabilities in this category can arise from a lack of oversight in this area, leading to poor code implementation, leading to vulnerability.

6.3.1.1 Code Quality Vulnerability (CWE-398)

Description

"Poor code quality," states OWASP, "leads to unpredictable behavior. From a user's perspective that often manifests itself as poor usability. For an attacker it provides an opportunity to stress the system in unexpected ways." [§6.6-1]

Examples

- Double free() errors (CWE-415),
- Failure to follow guideline/specification (CWE-573),
- Leftover debug code (CWE-489),
- Memory leak (CWE-401),
- Null dereference (CWE-476, CWE-690),
- Poor logging practice (CWE-778),
- Portability flaw (CWE-474, CWE-589),
- Undefined behavior (CWE-475),
- Uninitialized variable (CWE-457),
- Unreleased resource (CWE-404),
- Unsafe mobile code (CWE-490),

[2] The OWASP names are generally used with the exact or closest CWE-ID(s) match in parentheses. The mappings are informational only and are not to be considered authoritative.

- Use of obsolete methods (CWE-477),
- Using freed memory (CWE-416), and
- Buffer overflow (CWE-120).

6.3.1.2 Authentication Vulnerability (CWE-287)

Description

Authentication is the process of proving an identity to a given system. Users, applications, and devices may all require authentication. This class of vulnerability leads to authentication bypass or other circumvention/manipulation of the authentication process.

Examples [§6.6-1]

- CVE-2012-3024 - Tridium Niagara AX Framework through 3.6 uses predictable values for (1) session IDs and (2) keys, which might allow remote attackers to bypass authentication via a brute-force attack;
- CVE-2012-1799 - The web server on the Siemens Scalance S Security Module firewall S602 V2, S612 V2, and S613 V2 with firmware before 2.3.0.3 does not limit the rate of authentication attempts, which makes it easier for remote attackers to obtain access via a brute-force attack on the administrative password;
- CVE-2012-1808 - The web server in the ECOM Ethernet module in Koyo H0-ECOM, H0-ECOM100, H2-ECOM, H2-ECOM-F, H2-ECOM100, H4-ECOM, H4-ECOM-F, and H4-ECOM100 does not require authentication, which allows remote attackers to perform unspecified functions via unknown vectors;
- Allowing password aging (CWE-263),
- Authentication bypass via assumed-immutable data (CWE-302),
- Empty string password (CWE-258),
- Failure to drop privileges when reasonable (CWE-271),
- Hard-coded password (CWE-259),
- Not allowing password aging (CWE-262),
- Often misused: authentication (CWE-247),
- Reflection attack in an auth protocol (CWE-301),
- Unsafe mobile code (CWE-490),
- Using password systems (CWE-309),
- Using referrer field for authentication or authorization (CWE-293), and
- Using single-factor authentication (CWE-308).

Potential Impact

Access is granted without official permission.

6.3.1.3 Authorization Vulnerability (CWE-284)

Description

Authorization is the process of assigning correct system permissions to an authenticated entity. This class of vulnerability allows authenticated entities the ability to perform actions which policy does not allow.

Examples

- Access control enforced by presentation layer (CWE-602, CWE-425),
- File access race condition: time-of-check, time-of-use (TOCTOU) (CWE-367),
- Least privilege violation (CWE-272),
- Often misused: privilege management (CWE-250),
- Using referrer field for authentication or authorization (CWE-293),
- Insecure direct object references (CWE-639, CWE-22), and
- Failure to restrict universal resource locator (URL) access (CWE-425, CWE-288).

6.3.1.4 Cryptographic Vulnerability (CWE-310)

Description

Cryptography is the use of mathematical principles and their implementations to ensure that information is hidden from unauthorized parties, the information is unchanged, and the intended party can verify the sender. This vulnerability class includes issues that allow an attacker to view, modify, or forge encrypted data or impersonate another party through digital signature abuse.

Examples

- CVE-2012-4899 - WellinTech KingView 6.5.3 and earlier uses a weak password-hashing algorithm, which makes it easier for local users to discover credentials by reading an unspecified file;
- CVE-2012-3025 - The default configuration of Tridium Niagara AX Framework through 3.6 uses a cleartext base64 format for transmission of credentials in cookies, which allows remote attackers to obtain sensitive information by sniffing the network;
- Failure to encrypt data (CWE-311),
- Insecure Randomness (CWE-330),
- Insufficient Entropy (CWE-332),
- Insufficient Session-ID Length (CWE-6),
- Key exchange without entity authentication (CWE-322),
- Non-cryptographic pseudo-random number generator (CWE-338),
- Not using a random initialization vector with cipher block chaining mode (CWE-329),

- PRNG Seed Error (CWE-335),
- Password Management: Weak Cryptography (CWE-261),
- Reusing a nonce, key pair in encryption (CWE-323),
- Testing for SSL-TLS (OWASP-CM-001) (CWE-326),
- Use of hard-coded cryptographic key (CWE-321),
- Using a broken or risky cryptographic algorithm (CWE-327), and
- Using a key past its expiration date (CWE-324).

6.3.1.5 Environmental Vulnerability (CWE-2)

Description

"This category," states OWASP, "includes everything that is outside of the source code but is still critical to the security of the product that is being created. Because the issues covered by this kingdom are not directly related to source code, we separated it from the rest of the kingdoms." [§6.6-1]

Examples

- ASP.NET misconfigurations (CWE-10),
- Empty string password (CWE-258),
- Failure of true random number generator (CWE-333),
- Information leak through class cloning (CWE-498),
- Information leak through serialization (CWE-499),
- Insecure compiler optimization (CWE-14),
- Insecure transport (CWE-319, CWE-5),
- Insufficient session-ID length (CWE-6),
- Insufficient entropy in pseudo-random number generator (CWE-332),
- J2EE misconfiguration: unsafe bean declaration (CWE-8),
- Missing error handling (CWE-7),
- Publicizing of private data when using inner classes (CWE-492),
- Relative path library search (CWE-428),
- Reliance on data layout (CWE-188),
- Relying on package-level scope (CWE-487),
- Resource exhaustion (CWE-400), and
- Trust of system event data (CWE-360).

6.3.1.6 Error Handling Vulnerability (CWE-703)

Description

Error handling refers to the way an application deals with unexpected conditions - generally syntactical or logical. Vulnerabilities in this class provide means for attackers to use error handling to access unintended information or functionality.

Examples

- ASP.NET misconfigurations (CWE-10),
- Catch NullPointerException (CWE-395),
- Empty catch block (CWE-600),
- Improper cleanup on thrown exception (CWE-460),
- Improper error handling (CWE-390),
- Information leakage (CWE-200),
- Missing error handling (CWE-7),
- Often misused: exception handling (CWE-248),
- Overly-broad catch block (CWE-396),
- Overly-broad throws declaration (CWE-397),
- Return inside finally block (CWE-584),
- Uncaught exception (CWE-248),
- Unchecked error condition (CWE-391), and
- Unrestricted File Upload (CWE-434).

6.3.1.7 General Logic Error (CWE-691)

Description

Logic errors are programming missteps that allow an application to operate incorrectly, but usually without crashing. This vulnerability class covers those error types that have security implications.

Examples

- Addition of data-structure sentinel (CWE-464),
- Assigning instead of comparing (CWE-481),
- Comparing instead of assigning (CWE-482),
- Deletion of data-structure sentinel (CWE-463),
- Duplicate key in associative list (CWE-462),
- Failure to check whether privileges were dropped successfully (CWE-273),

- Failure to de-allocate data (CWE-401),
- Failure to provide confidentiality for stored data (CWE-493),
- Guessed or visible temporary file (CWE-379),
- Improper cleanup on thrown exception (CWE-460),
- Improper error handling (CWE-390),
- Improper temp file opening (CWE-378),
- Incorrect block delimitation (CWE-483),
- Misinterpreted function return value (CWE-253),
- Missing parameter (CWE-234),
- Omitted break statement (CWE-484),
- Passing mutable objects to an untrusted method (CWE-375),
- Symbolic name not mapping to correct object (CWE-386),
- Truncation error (CWE-197),
- Undefined Behavior (CWE-475),
- Uninitialized Variable (CWE-457),
- Unintentional pointer scaling (CWE-468),
- Use of sizeof() on a pointer type (CWE-467), and
- Using the wrong operator (CWE-480).

6.3.1.8 Business logic Vulnerability

Description

Business logic vulnerabilities occur when the legitimate processing flow of an application is used in a way that results in an unintended consequence. Discovery and testing of this vulnerability class tends to be specific to an application under analysis and require detailed knowledge of the business process. Additional information on this vulnerability may be found at [§6.6-10].

Examples

- Purchase orders are not processed before midnight,
- Written authorization is not on file before web access is granted, and
- Transactions in excess of $2000 are not reviewed by a person.

6.3.1.9 Input and Output Validation (CWE-20 AND CWE-116)

Description

Input validation is the process of ensuring that the user-supplied content contains only expected information. Input validation covers a wide assortment of potential exploitation but requires caution. Failing to properly validate external input may allow execution of unintended

functionality—and often “arbitrary code execution”. Output validation is encoding or escaping data during the preparation of a structured message for communication with another component. Improper output validation can allow attackers to change or replace the commands sent to other components.

Examples

- CVE-2012-3026 - rifsrvd.exe in the Remote Interface Service in GE Intelligent Platforms Proficy Real-Time Information Portal 2.6 through 3.5 SP1 allows remote attackers to cause a denial of service (memory corruption and service crash) or possibly execute arbitrary code via long input data,
- CVE-2012-3021 - APIFTP Server in Optimalog Optima PLC 1.5.2 and earlier allows remote attackers to cause a denial of service (infinite loop) via a malformed packet,
- Buffer overflow (CWE-120),
- Format string (CWE-134),
- Improper data validation (CWE-102, CWE-103, CWE-104, CWE-105, CWE-106, CWE-107, CWE-108, CWE-109, CWE-110),
- Log forging (CWE-117),
- Missing XML validation (CWE-112),
- Process control (CWE-114),
- String termination error (CWE-158),
- Unchecked return value: missing check against null (CWE-690, CWE-252),
- Unsafe Java Native Interface (JNI) (CWE-111),
- Unsafe reflection (CWE-470),
- Validation performed in client (CWE-602),
- Unvalidated redirects and forwards (CWE-819), and
- Improper Neutralization of HTTP Headers for Scripting Syntax (CWE-664).

6.3.1.10 Logging and Auditing Vulnerability (CWE-778 and CWE-779)

Description

Logging and auditing are common system and security functions aiding in system management, event identification, and event reconstruction. This vulnerability class deals with issues that either aid in an attack or increase the likelihood of its success due to logging and auditing.

Examples

- Addition of data-structure sentinel (CWE-464),
- Information leakage (CWE-200),
- Log forging (CWE-117),

- Log injection (CWE-117),
- Poor logging practice, and
- Cross-site scripting via HTML log-viewers (CWE-79, CWE-117).

6.3.1.11 Password Management Vulnerability (CWE-255)

Description

Passwords are the most commonly used form of authentication. This class of vulnerabilities deals with mistakes in handling passwords that may allow an attacker to obtain or guess them.

Examples

- CVE-2012-4879 - The Linux Console on the WAGO I/O System 758 model 758-870, 758-874, 758-875, and 758-876 Industrial PC (IPC) devices has a default password of wago for the (1) root and (2) admin accounts, (3) a default password of user for the user account, and (4) a default password of guest for the guest account, which makes it easier for remote attackers to obtain login access via a TELNET session,
- CVE-2012-3013 - WAGO I/O System 758 model 758-870, 758-874, 758-875, and 758-876 Industrial PC (IPC) devices have default passwords for unspecified Web Based Management accounts, which makes it easier for remote attackers to obtain administrative access via a TCP session,
- CVE-2012-3014 - The Management Software application in GarrettCom Magnum MNS-6K before 4.4.0, and 14.x before 14.4.0, has a hardcoded password for an administrative account, which allows local users to gain privileges via unspecified vectors,
- Empty string password (CWE-258),
- Hard-coded password (CWE-259),
- Not allowing password aging (CWE-262),
- Password management: hardcoded password (CWE-259),
- Password management: weak cryptography (CWE-261),
- Password plaintext storage (CWE-256),
- Password in configuration file (CWE-260), and
- Using password systems (CWE-309).

6.3.1.12 Path Vulnerability (CWE-21)

Description

“This category [Path Vulnerability],” states OWASP, “is for tagging path issues that allow attackers to access files that are not intended to be accessed. Generally, this is due to dynamically construction of a file path using unvalidated user input.” [§6.6-1]

Examples

- Path traversal attack (CWE-22),
- Relative path traversal attack (CWE-23),
- Virtual files attack (CWE-66),
- Path equivalence attack (CWE-41), and
- Link following attack (CWE-59).

6.3.1.13 Protocol Errors (CWE-254, CWE-573, CWE-668)

Description

Protocols are rules of communication. This vulnerability class deals with the security issues introduced during protocol design.

Examples

- Failure to add integrity check value (CWE-353),
- Failure to check for certificate revocation (CWE-299),
- Failure to check integrity check value (CWE-354),
- Failure to encrypt data (CWE-311),
- Failure to follow chain of trust in certificate validation (CWE-296),
- Failure to protect stored data from modification (CWE-766, CWE-767),
- Failure to validate certificate expiration (CWE-298),
- Failure to validate host-specific certificate data (CWE-297),
- Key exchange without entity authentication (CWE-322),
- Storing passwords in a recoverable format (CWE-257),
- Trusting self-reported domain name service (DNS) name (CWE-292),
- Trusting self-reported IP address (CWE-291),
- Use of hard-coded password (CWE-798, CWE-259),
- Insufficient transport layer protection (CWE-818),
- Use of weak secure socked layer / transport layer security (SSL/TLS) protocols (CWE-757),
- SSL/TLS key exchange without authentication (CWE-322),
- SSL/TLS weak key exchange (CWE-326), and
- Low SSL/TLS cipher strength (CWE-326).

Potential Impact

The compromise of security protocols such as TLS.

6.3.1.14 Range and Type Error Vulnerability (CWE-118, CWE-136)

Description

Range and type errors are common programming mistakes. This vulnerability class covers the various types of errors that have potential security consequences.

Examples

- Access control enforced by presentation layer (CWE-602, CWE-425),
- Buffer overflow (CWE-120),
- Buffer underwrite (CWE-124),
- Comparing classes by name (CWE-486),
- De-serialization of untrusted data (CWE-502),
- Doubly freeing memory (CWE-415),
- Failure to account for default case in switch (CWE-478),
- Format string (CWE-134),
- Heap overflow (CWE-122),
- Illegal pointer value (CWE-466),
- Improper string length checking (CWE-135),
- Integer coercion error (CWE-192),
- Integer overflow (CWE-190, CWE-680),
- Invoking untrusted mobile code (CWE-494),
- Log forging (CWE-117),
- Log injection (CWE-117),
- Miscalculated null termination (CWE-170),
- Null dereference (CWE-476, CWE-690),
- Often misused: string management (CWE-251),
- Reflection injection (CWE-470),
- Sign extension error (CWE-194),
- Signed to unsigned conversion error (CWE-195),
- Stack overflow (CWE-121),
- Truncation error (CWE-197),

- Trust boundary violation (CWE-501),
- Unchecked array indexing (CWE-129),
- Unsigned to signed conversion error (CWE-196),
- Using freed memory (CWE-416),
- Validation performed in client (CWE-602), and
- Wrap-around error (CWE-128).

6.3.1.15 Sensitive Data Protection Vulnerability (CWE-199)

Description

OWASP describes the sensitive data protection vulnerability as follows:

> This category is for tagging vulnerabilities that lead to insecure protection of sensitive data. The protection referred here includes confidentiality and integrity of data during its whole life cycles, including storage and transmission.
>
> Please note that this category is intended to be different from access control problems, although they both fail to protect data appropriately. Normally, the goal of access control is to grant data access to some users but not others. In this category, we are instead concerned about protection for sensitive data that are not intended to be revealed to or modified by any application users. Examples of this kind of sensitive data can be cryptographic keys, passwords, security tokens or any information that an application relies on for critical decisions. [§6.6-1]

Examples

- Information leakage results from insufficient memory clean-up (CWE-226),
- Inappropriate protection of cryptographic keys[3] (CWE-311, CWE-326, CWE-321, CWE-325, CWE-656),
- Lack of integrity protection for stored user data (CWE-693),
- Hard-coded password (CWE-259),
- Heap inspection (CWE-244),
- Information leakage (CWE-200),
- Password management: hardcoded password (CWE-259),
- Password plaintext storage (CWE-256), and
- Privacy violation (CWE-359).

[3] http://www.owasp.org/index.php/Top_10_2007-Insecure_Cryptographic_Storage

6.3.1.16 Session Management Vulnerability (CWE-718)

Description

Session management is the way with which a client and server connect, maintain, and close a connection. Primarily an issue with Web interfaces, this class covers vulnerabilities resulting from poor session management.

Examples

- Applications should not use variables that include any user personal information (user name, password, home address, etc.),
- Highly protected applications should not implement mechanisms that make automated requests to prevent session timeouts,
- Highly protected applications should not implement "remember me" functionality,
- Highly protected applications should not use URL rewriting to maintain state when cookies are turned off on the client,
- Applications should not use session identifiers for encrypted HTTPS transport that have once been used over HTTP,
- Insufficient Session-ID Length (CWE-6),
- Session Fixation (CWE-384),
- Cross site request forgery (CWE-352),
- Cookie attributes not set securely (e.g. domain, secure and HTTP only) (CWE-614), and
- Overly long session timeout (CWE-613).

6.3.1.17 Concurrency, Synchronization and Timing Vulnerability (CWE-361)

Description

Concurrency, synchronization and timing deals with the order of events in a complex computing environment. This vulnerability class deals with timing issues that affect security, most often dealing with multiple processes or threads which share some common resource (file, memory, etc.).

Examples

- Capture-replay (CWE-294),
- Covert timing channel (CWE-385),
- Failure to drop privileges when reasonable (CWE-271, CWE-653),
- Failure to follow guideline/specification (CWE-573),
- File access race condition: TOCTOU (CWE-367),
- Member field race condition (CWE-488),

- Mutable object returned (CWE-375),
- Overflow of static internal buffer (CWE-500),
- Race conditions (CWE-362),
- Reflection attack in an auth protocol (CWE-301),
- State synchronization error (CWE-373), and
- Unsafe function call from a signal handler (CWE-479).

6.3.1.18 Insufficient Safeguards for Mobile Code (CWE-490)

Description

Mobile code consists of programming instructions transferred from server to client that execute on the client machine without the user explicitly initiating that execution. Allowing mobile code generally increases attack surface. This subsection includes issues that permit the execution of unsafe mobile code.

Examples

- VBScript, JavaScript and Java sandbox container flaws,
- Insufficient scripting controls, and
- Insufficient code authentication.

6.3.1.19 Buffer Overflow (CWE-119, CWE-120)

Description

Software used to implement an industrial control system (ICS) could be vulnerable to buffer overflows; adversaries could exploit these to perform various attacks. [§6.6-3]

A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold, or when a program attempts to put data in a memory area outside of the boundaries of a buffer. The simplest type of error, and the most common cause of buffer overflows, is the "classic" case in which the program copies the buffer without checking its length at all. Other variants exist, but the existence of a classic overflow strongly suggests that the programmer is not considering even the most basic of security protections. [§6.6-4]

Examples [§6.6-4]

- CVE-2012-0227 - Buffer overflow in the VSFlex7.VSFlexGrid ActiveX control in ComponentOne FlexGrid 7.1, as used in Open Automation Software OPC Systems.NET, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a long archive file name argument to the Archive method;
- CVE-2012-3035 = Buffer overflow in Emerson DeltaV 9.3.1 and 10.3 through 11.3.1 allows remote attackers to cause a denial of service (daemon crash) via a long string to an unspecified port;

- CVE-2012-5163 - Buffer overflow in an unspecified third-party component in the Batch module for Schneider Electric CitectSCADA before 7.20 and Mitsubishi MX4 SCADA before 7.20 allows local users to execute arbitrary code via a long string in a login sequence.

6.3.1.20 Mishandling of Undefined, Poorly Defined, or "Illegal" Conditions (CWE-388, CWE-20)

Description

Some ICS implementations are vulnerable to packets that are malformed or contain illegal or otherwise unexpected field values [§6.6-3]

6.3.1.21 Use of Insecure Protocols (CWE-720)

Description

Protocols are expected patterns of behavior that allow communication among computing resources. This section deals with the use of protocols for which security was not sufficiently considered during the development process.

Examples

- Distributed Network Protocol (DNP) 3.0, Modbus, Profibus, and other protocols are common across several industries and protocol information is freely available. These protocols often have few or no security capabilities built in, [§6.6-3]
- Use of clear text protocols such as FTP and Telnet, and
- Use of proprietary protocols lacking security features

6.3.1.22 Weaknesses that Affect Files and Directories CWE-632)

Description

Weaknesses in this category affect file or directory resources. [§6.6-4]

Examples

- UNIX path link problems (CWE-60),
- Windows path link problems (CWE-63),
- Windows virtual file problems (CWE-68),
- Mac virtual file problems (CWE-70),
- Failure to resolve case sensitivity (CWE-178),
- Path traversal (CWE-22),
- Failure to change working directory in chroot jail (CWE-243),
- Often misused: path manipulation (CWE-785),
- Password in configuration file (CWE-260),

- Improper ownership management (CWE-282),
- Improper resolution of path equivalence (CWE-41),
- Information leak through server log files (CWE-533),
- Files or directories accessible to external parties (CWE-552),
- Improper link resolution before file access ('link following') (CWE-59),
- Improper handling of windows device names (CWE-67), and
- Improper sanitization of directives in statically saved code ('static code injection') (CWE-96).

6.3.2 API Usage & Implementation

6.3.2.1 API Abuse (CWE-227)

Description

OWASP describes the API abuse vulnerability as follows:

> An API is a contract between a caller and a callee. The most common forms of API abuse are caused by the caller failing to honor its end of this contract.
>
> For example, if a program fails to call chdir() after calling chroot(), it violates the contract that specifies how to change the active root directory in a secure fashion. Another good example of library abuse is expecting the callee to return trustworthy DNS information to the caller. In this case, the caller abuses the callee API by making certain assumptions about its behavior (that the return value can be used for authentication purposes). One can also violate the caller-callee contract from the other side. For example, if a coder subclasses SecureRandom and returns a non-random value, the contract is violated. [§6.6-1]

Examples

- Dangerous function (CWE-242, CWE-676),
- Directory restriction error (CWE-243),
- Failure to follow guideline/specification (CWE-573),
- Heap inspection (CWE-244),
- Ignored function return value (CWE-252),
- Object model violation: just one of equals() and hashCode() defined (CWE-581),
- Often misused: authentication (CWE-247),
- Often misused: exception handling (CWE-248),
- Often misused: file system (CWE-785),
- Often misused: privilege management (CWE-250), and
- Often misused: string management (CWE-251).

6.3.2.2 Use of Dangerous API (CWE-242, CWE-676)

Description

A dangerous API is one that is not guaranteed to work safely in all conditions or can be used safely but could introduce a vulnerability if used in an incorrect manner.

Examples

- Dangerous function such as the C function gets() (CWE-242),
- Directory restriction error (CWE-243),
- Failure to follow guideline/specification (CWE-573),
- Heap inspection (CWE-244),
- Insecure temporary file (CWE-377),
- Object model violation: just one of equals() and hashCode() defined (CWE-581),
- Often misused: exception handling (CWE-248),
- Often misused: file system (CWE-785),
- Often misused: privilege management (CWE-250),
- Often misused: string management (CWE-251),
- Unsafe function call from a signal handler (CWE-479), and
- Use of obsolete methods (CWE-477).

6.4 PLATFORM VULNERABILITIES

Platforms are defined as the software and hardware units, or systems of software and hardware, that are used to deliver software-based services.

The platform comprises the software, the operating system used to support that software, and the physical hardware. Vulnerabilities arise in this part of the Smart Grid network due to the complexities of architecting, configuring, and managing the platform itself. Platform areas identified as being vulnerable to risk include the security architecture and design, inadequate malware protection against malicious software attacks, software vulnerabilities due to late or nonexistent software patches from software vendors, an overabundance of file transfer services running, and insufficient alerts from log management servers and systems.

6.4.1 Design

6.4.1.1 Use of Inadequate Security Architectures and Designs

Description

Development schedule pressures and lack of security training can lead to the use of inadequate security architectures and designs. This includes reliance on in-house security solutions, security through obscurity, and other insecure design practices.

Examples

- Security design by untrained engineers,
- Reliance on nonstandard techniques and unproven algorithms, and
- Security through obscurity.

6.4.1.2 Lack of External or Peer Review for Security Design

Description

Lack of understanding regarding the complexity of secure systems leads designers to believe that proven techniques can be easily combined into a larger system while preserving the security of the individual techniques. These kinds of errors are often discovered only through thorough, external review.

Examples:

- Introduction of side-channel attacks,
- Poorly combined algorithms,
- Lack of understanding regarding identifying weakest links, and
- Insufficient analysis of cascaded risk, whereby compromise of one system leads to compromise of a downstream system.

6.4.2 Implementation

6.4.2.1 Whitelisting

Description

An application whitelist is a list of applications and application components (libraries, configuration files, etc.) that are known to be benign. The technologies used to apply application whitelists—to control which applications are permitted to execute on a host—are called whitelisting programs, application control programs, or application whitelisting technologies. Application whitelisting technologies are intended to stop the execution of malware, unlicensed software, and other unauthorized software. Unlike security technologies such as antivirus software, which block known bad activity and permit all other, application whitelisting technologies are designed to permit known good activity and block all other.

Examples

- Whitelisting to prevent unintentional use of software (unauthorized software, incorrect software version), and
- Whitelisting could be used to restrict unauthorized software.

6.4.2.2 File Integrity Monitoring

Description

Establishing a "known and trusted" state based on a policy or standard and using a methodology or tool that finds, asseses, and acts on changes to the known state as soon as a change occurs. This ensures ongoing system integrity and automates detecting, autiding, and reconciling changes.

Examples

- File system integrity checking to ensure files are not changed, and
- Configuration change setting to ensure operating system settings are not changed.

6.4.2.3 Inadequate Malware Protection

Description

Malicious software can result in performance degradation, loss of system availability, and the capture, modification, or deletion of data. Malware protection software, such as antivirus software, is needed to prevent systems from being infected by malicious software. [§6.6-3]

Examples

- Malware protection software not installed,
- Malware protection software or definitions not current, and
- Malware protection software implemented without exhaustive testing.

6.4.2.4 Installed Security Capabilities Not Enabled by Default

Description

Security capabilities must be turned on in order to be useful. There are many examples of operating systems where protections such as firewalls are configured but not enabled out-of-the-box. If protections are not enabled, the system may be unexpectedly vulnerable to attacks. In addition, if the administrator does not realize that protections are disabled, the system may continue in an unprotected state for some time until the omission is noticed.

6.4.2.5 Absent or Deficient Equipment Implementation Guidelines

Description

Unclear implementation guidelines can lead to unexpected behavior.

A system needs to be configured correctly in order to provide the desired security properties. This applies to both hardware and software configuration. Different inputs and outputs, both logical and physical, will have different security properties, and an interface that is intended for internal use may be more vulnerable than an interface designed for external use. Guidelines for installers, operators, and managers should be clear about the security properties expected of the system and how the system is to be implemented and configured in order to obtain those properties.

6.4.3 Operational

6.4.3.1 Lack of Prompt Security Patches from Software Vendors

Description

Software contains bugs and vulnerabilities. When a vulnerability is disclosed, there will be a race between hackers and patchers to either exploit or close the loophole. The security of the system using the software depends on vendors' ability to provide patches in a timely manner, and on administrators' ability to implement those patches. As zero-day exploits become more widespread, administrators may be faced with the alternatives of taking a system offline or leaving it vulnerable.

6.4.3.2 Unneeded Services Running

Description

Many operating systems are shipped and installed with a number of services running by default. For example, in the case of UNIX, an installation may automatically offer telnet, ftp, and http servers. Every service that runs is a security risk, because intended use of the service may provide access to system assets, and the implementation may contain exploitable bugs. Services should run only if needed, and an unneeded service is a vulnerability with no benefit.

6.4.3.3 Insufficient Log Management

Description

Events from all devices should be logged to a central log management server. Alerts should be configured according to the criticality of the event or a correlation of certain events. For instance, when the tamper-detection mechanism on a device is triggered, an alert should be raised to the appropriate personnel. When a remote power disconnect command is issued to *x* (organization-defined) number of meters within a certain time, alerts should also be sent.

Examples

- Inadequate network security architecture [§6.6-3, Table 3-8];
- Inadequate firewall and router logs [§6.6-3, Table 3-11];
- No security monitoring on the network [§6.6-3, Table 3-11]; and
- Critical monitoring and control paths are not identified [§6.6-3, Table 3-12].

Potential Impact

- Failure to detect critical events;
- Removal of forensic evidence; and
- Log wipes.

6.4.4 Poorly configured security equipment (800-82 3-8)

6.4.4.1 Inadequate Anomaly Tracking

Description

Alerts and logging are two useful techniques for detecting and mitigating the risk of anomalous events, but can present security risks or become vulnerabilities if not instituted thoughtfully. The appropriate reaction to an event will vary according to the criticality of the event or a correlation of certain events. The event may also need to be logged, and a central logging facility may be necessary for correlating events. Appropriate event reactions could include automatic paging of relevant personnel in the event of persistent tamper messages or may require positive acknowledgement to indicate supervisory approval has been attained before executing a potentially disruptive command (e.g., simultaneously disconnecting many loads from the electrical grid or granting control access rights to hundreds of users).

6.5 NETWORK

Networks are defined by connections between multiple locations or organizational units and are composed of many differing devices using similar protocols and procedures to facilitate a secure exchange of information. Vulnerabilities and risks occur within Smart Grid networks when policy management and procedures do not conform to required standards and compliance polices as they relate to the data exchanged.

Network areas identified as being susceptible to risk and with policy and compliance impacts are: data integrity, security, protocol encryption, authentication, and device hardware.

6.5.1 Network

6.5.1.1 Inadequate Integrity Checking

Description

The integrity of message protocol and message data should be verified before routing or processing. Devices receiving data not conforming to the protocol or message standard should not act on such traffic (e.g., forwarding to another device or changing its own internal state) as though the data were correctly received.

Such verification should be done before any application attempts to use the data for internal processes or routing to another device. Additionally, special security devices acting as application-level firewalls should be used to perform logical bounds checking, such as preventing the shutdown of all power across an entire neighborhood area network (NAN).

Most functions of the Smart Grid, such as demand response (DR), load shedding, automatic meter reading (AMR), time of use (TOU), and distribution automation (DA), require that data confidentiality and/or data integrity be maintained to ensure grid reliability, prevent fraud, and enable reliable auditing. Failure to apply integrity and confidentiality services where needed can result in vulnerabilities such as exposure of sensitive customer data, unauthorized modification of telemetry data, transaction replay, and audit manipulation.

Examples

- Lack of integrity checking for communications [§6.6-3, Table 3-12],
- Failure to detect and block malicious traffic in valid communication channels,
- Inadequate network security architecture [§6.6-3, Table 3-8],
- Poorly configured security equipment [§6.6-3, Table 3-8], and
- No security monitoring on the network [§6.6-3, Table 3-11].

Potential Impact

- Compromise of smart device, head node, or utility management servers,
- Buffer overflows,
- Covert channels,
- Man-in-the-middle (MitM), and
- Denial of service or distributed denial of service (DoS /DDoS).

6.5.1.2 Inadequate Network Segregation

Description

Network architectures often do not clearly define security zones and control traffic between security zones, providing a flat network, wherein traffic from any portion of the network is allowed to communicate with any other portion of the network. Smart Grid examples of inadequate network segregation might include failure to install a firewall to control traffic between a head node and the utility company or failure to prevent traffic from one NAN to another NAN.

Examples

- Failure to define security zones,
- Failure to control traffic between security zones,
- Inadequate firewall ruleset,
- Firewalls nonexistent or improperly configured [§6.6-3, Table 3-10],
- Improperly configured VLAN,
- Inadequate access controls applied [§6.6-3, Table 3-8],
- Inadequate network security architecture [§6.6-3, Table 3-8],
- Poorly configured security equipment [§6.6-3, Table 3-8],
- Control networks used for non-control traffic [§6.6-3, Table 3-10],
- Control network services not within the control network [§6.6-3, Table 3-10], and
- Critical monitoring and control paths are not identified [§6.6-3, Table 3-12].

Potential Impact

- Direct compromise of any portion of the network from any other portion of the network,
- Compromise of the Utility network from a NAN network,
- VLAN hopping,
- Network mapping,
- Service/Device exploit,
- Covert channels,
- Back doors,
- Worms and other malicious software, and
- Unauthorized multi-homing.

6.5.1.3 Inappropriate Protocol Selection

Description

It is important to note that the use of encryption is not always the appropriate choice. A full understanding of the information management capabilities that are lost through the use of encryption should be completed before encrypting unnecessarily.

Use of unencrypted network protocols or weakly encrypted network protocols exposes authentication keys and data payload. This may allow attackers to obtain credentials to access other devices in the network and decrypt encrypted traffic using those same keys. The use of clear text protocols may also permit attackers to perform session hijacking and MitM attacks allowing the attacker to manipulate the data being passed between devices.

Examples

- Standard, well-documented communication protocols are used in plain text in a manner which creates a vulnerability [§6.6-3, Table 3-12], and
- Inadequate data protection is permitted between clients and access points [§6.6-3, Table 3-13].

Potential Impact

- Compromise of all authentication and payload data being passed,
- Session Hijacking,
- Authentication Sniffing,
- MitM Attacks, and
- Session Injection.

6.5.1.4 Weaknesses in Authentication Process or Authentication Keys

Description

Authentication mechanism does not sufficiently authenticate devices or exposes authentication keys to attack.

Examples

- Inappropriate Lifespan for Authentication Credentials/Keys;
- Inadequate Key Diversity;
- Authentication of users, data, or devices is substandard or nonexistent [§6.6-3, Table 3-12];
- Insecure key storage;
- Insecure key exchange;
- Insufficient account lockout;
- Inadequate authentication between clients and access points [§6.6-3, Table 3-13]; and
- Inadequate data protection between clients and access points [§6.6-3, Table 3-13].

Potential Impact

- DoS / DDoS,
- MitM,
- Session Hijacking,
- Authentication Sniffing, and
- Session Injection.

6.5.1.5 Insufficient Redundancy

Description

Architecture does not provide for sufficient redundancy, thus exposing the system to intentional or unintentional denial of service.

Examples

- Lack of redundancy for critical networks [§6.6-3, Table 3-9].

Potential Impact

- DoS / DDoS.

6.5.1.6 Physical Access to the Device

Description

Access to physical hardware may lead to a number of hardware attacks that can lead to the compromise of all devices and networks. Physical access to Smart Grid devices should be limited according to the criticality or sensitivity of the device. Ensuring the physical security of Smart Grid elements, such as by physically locking them in some secure building or container, is preferred where practical. In other circumstances, tamper resistance, tamper detection, and intrusion detection and alerting are among the many techniques that can complement physically securing devices.

Examples

- Unsecured physical ports,
- Inadequate physical protection of network equipment [§6.6-3, Table 3-9],
- Loss of environmental control [§6.6-3, Table 3-9], and
- Noncritical personnel have access to equipment and network connections [§6.6-3, Table 3-9].

Potential Impact

- Malicious configurations,
- MitM,
- EEPROM dumping,
- Micro controller dumping,
- Bus snooping, and
- Key extraction.

6.6 REFERENCES

The following are cited in this chapter—

1. Open Web Application Security Project (OWASP), 2011. http://www.owasp.org/index.php/Category:Vulnerability (accessed December 5, 2012).
2. Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Gaithersburg: NIST, 2012. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
3. Stouffer, Keith, Joe Falco, and Karen Scarfone. NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*. Gaithersburg, MD: NIST, 2011. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.
4. Common Weakness Enumeration (CWE), 2012. http://cwe.mitre.org (accessed December 5, 2012).

5. Common Vulnerabilities and Exposures (CVE), 2012. http://cve.mitre.org/ (accessed December 5, 2012).

6. North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards, http://www.nerc.com/page.php?cid=2|20 (accessed December 5, 2012).

7. Stoneburner, Gary, Clark Hayden, and Alexis Feringa. NIST SP 800-27 Rev. A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*. Gaithersburg, MD: NIST, 2004. http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.

8. CMMI Product Team, *CMMI for Development, Version 1.3* (CMU/SEI-2010-TR-033). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm.

9. ISO/IEC 21827:2008, Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®), Geneva, Switzerland: International Organization for Standardization (ISO), 2008. http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44716 (accessed December 5, 2012)

10. OWASP, "Testing for business logic (OWASP-BL-001)", 2012. http://www.owasp.org/index.php/Testing_for_business_logic_%28OWASP-BL-001%29 (accessed December 5, 2012).

CHAPTER 7
BOTTOM-UP SECURITY ANALYSIS OF THE SMART GRID

7.1 SCOPE

A subgroup of the CSWG performed a bottom-up analysis of cybersecurity issues in the evolving Smart Grid. The goal was to identify specific protocols, interfaces, applications, best practices, etc., that could and should be developed to solve specific Smart Grid cybersecurity problems. The approach taken was to perform the analysis from the bottom up; that is, to identify some specific problems and issues that need to be addressed but not to perform a comprehensive gap analysis that covers all issues. This effort was intended to complement the top-down efforts being followed elsewhere in the CSWG (now the SGCC). By proceeding with a bottom-up analysis, our hope was to more quickly identify fruitful areas for solution development, while leaving comprehensive gap analysis to other efforts of the CSWG, and to provide an independent completeness check for top-down gap analyses. This effort proceeded simultaneously in several phases.

First, we have identified a number of *evident and specific security problems* in the Smart Grid that are amenable to and should have open and interoperable solutions but which are not obviously solved by existing standards, de facto standards, or best practices. This list includes only cybersecurity problems that have some specific relevance to or uniqueness in the Smart Grid. Thus we do not list general cybersecurity problems such as poor software engineering practices, key management, etc., unless these problems have some unique twist when considered in the context of the Smart Grid.

In conjunction with developing the list of specific problems, we have developed a separate list of more *abstract security issues* that are not as specific as the problems in the first list, but are nevertheless of significant importance. Considering these issues in specific contexts can reveal specific problems.

Next, drawing in part from the specific problems and abstract issues enumerated in the first two lists, we developed a third list of cybersecurity *design considerations* for Smart Grid systems. These design considerations discuss important cybersecurity issues that arise in the design, deployment, and use of Smart Grid systems and that should be considered by system designers, implementers, purchasers, integrators, and users of Smart Grid technologies. In discussing the relative merits of different technologies or solutions to problems, these design considerations stop short of recommending specific solutions or even requirements. Our intention is to highlight important issues that can serve as a means of identifying and formulating requirements and high-level designs for key protocols and interfaces that are missing and need to be developed.

7.2 EVIDENT AND SPECIFIC CYBERSECURITY PROBLEMS

This subsection documents specific cybersecurity problems in the Smart Grid insofar as possible by describing actual field cases that explain exactly the operational, system, and device issues. The problems listed herein are intentionally *not* ordered or categorized in any particular way.

7.2.1 Authenticating and Authorizing Users to Substation IEDs

The problem addressed in this subsection is how to authenticate and authorize users (maintenance personnel) to intelligent electronic devices (IEDs) in substations in such a way that access is specific to a user, authentication information (e.g., password) is specific to each user (i.e., not shared between users), and control of authentication and authorization can be centrally managed across all IEDs in the substation and across all substations belonging to the utility and updated reasonably promptly to ensure that only intended users can authenticate to intended devices and perform authorized functions.

Currently many substation IEDs have a notion of "role" but no notion of "user." Passwords are stored locally on the device, and several different passwords allow different authorization levels. These role passwords are shared amongst all users of the device performing the role in question, possibly including nonutility employees such as contractors and vendors. Furthermore, due to the number of devices, these passwords are often the same across all devices in the utility and are seldom changed.

A device may be accessed locally in the sense that the user is physically present in the substation and accesses the IED from a front panel connection, a wired network connection, or possibly via a wireless connection. The device may also be accessed remotely over a low-speed (dial-up) or high-speed (network) connection from a different physical location.

Substations generally have some sort of connectivity to the control center that might be used to distribute authentication information and collect audit logs, but this connectivity may be as slow as 1200 baud. Performing an authentication protocol such as Remote Authentication Dial In User Service (RADIUS) or Lightweight Directory Access Protocol (LDAP) over this connection is probably not desirable. Furthermore, reliance on central authentication servers is unwise, since authentication should continue to apply for personnel accessing devices locally in the substation when control center communications are down.

A provision to ensure that necessary access is available in emergency situations may be important, even if it means bypassing normal access control—but with an audit trail.

7.2.2 Authenticating and Authorizing Users to Outdoor Field Equipment

Some newer pole-top and other outdoor field equipment supports 802.11 or Bluetooth for near-local user access from a maintenance truck. The problem is how to authenticate and authorize users (maintenance personnel) to such devices in such a way that access is specific to a user (person), authentication information (e.g. password) is specific to each user (not shared between users), and control of authentication and authorization can be centrally managed across the utility and updated reasonably promptly to ensure that only intended users can authenticate to intended devices and perform authorized functions.

Pole-top and other outdoor field equipment may not have connectivity to the control center.

Access will usually be local via wired connections, or near-local via short-range radio, although some devices may support true remote access.

Strong authentication and authorization measures are preferable, and in cases where there is documented exception to this due to legacy and computing constrained devices, compensating controls should be given due consideration. For example, in many utility organizations, very strong operational control and workflow prioritization is in place, such that all access to field

equipment is scheduled, logged, and supervised. In the general sense, the operations department typically knows exactly who is at any given field location at all times. In addition, switchgear and other protective equipment generally have tamper detection on doors as well as connection logging and reporting such that any unexpected or unauthorized access can be reported immediately over communications.

7.2.3 Authenticating and Authorizing Maintenance Personnel to Meters

Like IED equipment in substations, current smart meter deployments use passwords in meters that are not associated with individual users. Passwords are shared between users, and the same password is typically used across the entire meter deployment. The problem is how to authenticate and authorize users who are maintenance personnel to meters in such a way that access is specific to a user, authentication information (e.g., password) is specific to each user (i.e., not shared between users), and control of authentication and authorization can be centrally managed and updated reasonably promptly to ensure that only intended users can authenticate to intended devices and perform authorized functions.

Access may be local through the optical port of a meter or remote through the advanced metering infrastructure (AMI) infrastructure.

Meters generally have some sort of connectivity to an AMI head end, but this connectivity may be as slow as 1200 baud or lower (e.g., some power line carrier devices have data rates measured in millibaud). This connectivity cannot be assumed to be present in a maintenance scenario.

7.2.4 Authenticating and Authorizing Consumers to Meters

Where meters act as home area network gateways for providing energy information to consumers and/or control for demand response programs, will consumers be authenticated to meters? If so, authorization would likely be highly limited. What would the roles be? Authorization and access levels need to be carefully considered, i.e., a consumer capable of supplying energy to the power grid may have different access requirements than one who does not.

7.2.5 Authenticating Meters to/from AMI Head Ends

It is important for a meter to authenticate any communication from an AMI head end in order to ensure that an adversary cannot issue control commands to the meter, update firmware, etc. It is important for an AMI head end to authenticate the meter, since usage information retrieved from the meter will be used for billing and commands must be assured of delivery to the correct meter.

As utilities merge and service territories change, a utility will eventually end up with a collection of smart meters from different vendors. Meter to/from AMI head end authentication should be interoperable to ensure that authentication and authorization information need not be updated separately on different vendor's AMI systems.

7.2.6 Authenticating HAN Devices to/from HAN Gateways

Demand response HAN devices must be securely authenticated to the HAN gateway and vice versa. It is important for a HAN device to authenticate any demand-response commands from the DR head end in order to prevent control by an adversary. Without such authentication, coordinated falsification of control commands across many HAN devices and/or at rapid rates

could lead to grid stability problems. It is important that the DR head end authenticate the HAN device both to ensure that commands are delivered to the correct device and that responses from that device are not forged.

Interoperability of authentication is essential in order to ensure competition that will lead to low-cost consumer devices. This authentication process must be simple and fairly automatic, since to some degree it will be utilized by consumers who buy/rent HAN devices and install them. HAN devices obtained by the consumer from the utility may be preprovisioned with authentication information. HAN devices obtained by the consumer from retail stores may require provisioning through an Internet connection or may receive their provisioning through the HAN gateway.

Should a HAN device fail to authenticate, it will presumably be unable to respond to DR signals. It should not be possible for a broad denial of service (DoS) attack to cause a large number of HAN devices to fail to authenticate and thereby not respond to a DR event.

7.2.7 Authenticating Meters to/from AMI Networks

Meters and AMI networks are more susceptible to widespread compromise and DoS attacks if no authentication and access control is provided in AMI access networks such as neighborhood area networks (NANs) and HANs. The vulnerability exists even if the rest of the AMI network is secured, and encryption and integrity are provided by an AMI application protocol. Network access authentication tied with access control in the AMI access networks can mitigate the threat by ensuring that only authenticated and authorized entities can gain access to the NANs or HANs. In mesh networks, this “gatekeeper” functionality must be enforced at each node. The network access authentication must be able to provide mutual authentication between a meter and an access control enforcement point. A trust relationship between the meter and the enforcement point may be dynamically established using a trusted third party such as an authentication server.

Providing network access authentication for mesh networks can be more challenging than for non-mesh networks due to the difference in trust models between mesh and non-mesh networks. One trust model for mesh networks is based on a dynamically created hop-by-hop chain of trust between adjacent mesh nodes on the path between a leaf mesh node and the gateway to the AMI network where access control is performed on each intermediate mesh node and the gateway. Another trust model for mesh networks is end-to-end trust between a leaf mesh node and the gateway where intermediate mesh nodes are considered untrusted to the leaf node and a secured tunnel may be created between each leaf node and the gateway. These two trust models can coexist in the same mesh network. When two or more interconnected mesh networks are operated in different trust models, end-to-end security across these mesh networks is the only way to provide data security for applications running across the mesh networks. There has been some research done in the area of wireless sensor networks that is relevant to mesh networks. For instance, there are scalable key pre-distribution schemes [§7.5-11] that are resistant to node capture and operate well on devices with limited computational capabilities.

7.2.8 Securing Serial SCADA Communications

Many substations and distribution communication systems still employ slow serial links for various purposes, including supervisory control and data acquisition (SCADA) communications with control centers and distribution field equipment. Furthermore, many of the serial protocols currently in use do not offer any mechanism to protect the integrity or confidentiality of

messages, i.e., messages are transmitted in cleartext form. Solutions that simply wrap a serial link message into protocols like Secure Socket Layer (SSL) or Internet Protocol Security (IPSec) over Point-to-Point Protocol (PPP) will suffer from the overhead imposed by such protocols (both in message payload size and computational requirements) and would unduly impact latency and bandwidth of communications on such connections. A solution is needed to address the security and bandwidth constraints of this environment.

7.2.9 Securing Engineering Dial-up Access

Dial-up is often used for engineering access to substations. Broadband is often unavailable at many remote substation locations. Security is limited to modem callback and passwords in the answering modem and/or device connected to the modem. Passwords are not user-specific and are seldom changed. A solution is needed that gives modern levels of security while providing for individual user attribution of both authentication and authorization.

7.2.10 Secure End-to-End Meter to Head End Communication

Secure end-to-end communications protocols such as transport layer security (TLS) and IPSec ensure that confidentiality and integrity of communications is preserved regardless of intermediate hops. End-to-end security between meters and AMI head ends is desirable, and even between HAN devices and DR control services.

7.2.11 Access Logs for IEDs

Not all IEDs create access logs. Due to limited bandwidth to substations, even where access logs are kept, they are often stranded in the substation. In order for a proper security event management (SEM) paradigm to be developed, these logs will need to become centralized and standardized so that other security tools can analyze their data. This is important in order to detect malicious actions by insiders as well as systems deeply penetrated by attackers that might have subtle misconfigurations as part of a broader attack. A solution is needed that can operate within the context of bandwidth limitations found in many substations as well as the massively distributed nature of the power grid infrastructure.

7.2.12 Remote Attestation of Meters

Remote attestation provides a means to determine whether a remote field unit has an expected and approved configuration. For meters, this means the meter is running the correct version of untampered firmware with appropriate settings and has *always* been running untampered firmware. Remote attestation is particularly important for meters given the easy physical accessibility of meters to attackers.

7.2.13 Protection of Routing Protocols in AMI Layer 2/3 Networks

In the AMI space, there is increasing likelihood that mesh routing protocols will be used on wireless links. Wireless connectivity suffers from several well-known and often easily exploitable attacks, partly due to the lack of control to the physical medium (the radio waves). Modern mechanisms like the IEEE 802.11i and 802.11w security standards have worked to close some of these holes for standard wireless deployments. However, wireless mesh technology potentially opens the door to some new attacks in the form of route injection, node impersonation, L2/L3/L4 traffic injection, traffic modification, etc. Most current on-demand and

link-state routing mechanisms do not specify a scheme to protect the data or the routes the data takes, because it is outside of the scope of routing protocols. They also generally lack schemes for authorizing and providing integrity protection for adjacencies in the routing system. Without end-to-end security (like IPsec), attacks such as eavesdropping, impersonation, and man-in-the-middle (MITM) could be easily mounted on AMI traffic. With end-to-end security in place, routing security is still required to prevent denial of service (DoS) attacks.

7.2.14 Protection of Dial-up Meters

Reusing older, time-proven technologies such as dial-up modems to connect to collectors or meters without understanding the subtle differences in application may provide loss of service or worse. Dial-up technology using plain old telephone service (POTS) has been a preferred method for connecting to network gear, particularly where a modem bank providing 24, 48, or even 96 modems / phone numbers and other anti-attack intelligence is used. However, dialing into a collector or modem and connecting, even without a password, can tie up a line and effectively become a denial of service attack. Consider a utility which, for the sake of manageability places all their collectors or modems on phone numbers in a particular prefix. Every collector then can be hit by calling 202-555-WXYZ.

7.2.15 Outsourced WAN Links

Many utilities are leveraging existing communications infrastructure from telecommunications companies to provide connectivity between generation plants and control centers, between substations and control centers (particularly SCADA), and increasingly between pole-top AMI collectors and AMI head end systems, and pole-top distribution automation equipment and distribution management systems.

Due to the highly distributed nature of AMI, it is more likely that an AMI wide area network (WAN) link will be over a relatively low bandwidth medium such as cellular band wireless (e.g., Evolution Data Optimized (EvDO), General Packet Radio Service (GPRS)), or radio networks like FlexNet. The link layer security supported by these networks varies greatly. Later versions of WiMax can utilize Extensible Authentication Protocol (EAP) for authentication, but NIST Special Publication (SP) 800-127, *Guide to Security for Worldwide Interoperability for Microwave Access (WiMAX) Technologies*, provides a number of recommendations and cautions about WiMax authentication. With cellular protocols, the AirCards used by the collector modems are no different than the ones used for laptops. They connect to a wireless cloud typically shared by all local wireless users with no point-to-point encryption and no restrictions on whom in the wireless cloud can connect to the collector modem's interface. From the wireless, connectivity to the head end system is usually over the Internet, sometimes (hopefully always) using a virtual private network (VPN) connection. Given the proliferation of botnets, it is not farfetched to imagine enough wireless users being compromised to launch a DoS attack via a collector modem.

Regardless of the strength of any link layer security implemented by the communications service provider, without end-to-end VPN security the traffic remains accessible to insiders at the service provider. This can permit legitimate access such as lawful intercept but also can allow unscrupulous insiders at the service provider access to the traffic.

Additionally, like the mesh wireless portion, cellular networks are subject to intentional and unintentional interference and congestion. Cellular networks were significantly disrupted in

Manhattan during the 9/11 attacks by congestion and were rendered mostly unusable to first responders. Similar congestion events could disrupt utility communications relying on commercial WAN links.

7.2.16 Insecure Firmware Updates

The ability to perform firmware updates on meters in the field allows for the evolution of applications and the introduction of patches without expensive physical visits to equipment. However, it is critical to ensure that firmware update mechanisms are not used to install malware. This can be addressed by a series of measures that provide a degree of defense in depth. First, measures can be taken to ensure that software is created without flaws such as buffer overflows that can enable protection measures to be circumvented. Techniques for programming languages and static analysis provide a foundation for such measures. Second, principals attempting updates must be properly authenticated and authorized for this function at a suitable enforcement point such as on the meter being updated. Third, software can be signed in a way that it can be checked for integrity at any time. Fourth, remote attestation techniques can provide a way to assess existing and past software configuration status so that deviations from expected norms can generate a notification or alarm event. Fifth, there must be a suitable means to detect a penetration of a meter or group of meters in a peer-to-peer mesh environment and isolate and contain any subsequent attempts to penetrate other devices. This is important, as it must be assumed that if an attacker has the capability to reverse engineer a device that any inbuilt protections can eventually be compromised as well. It is an open and challenging problem to do intrusion detection in a peer-to-peer mesh environment.

7.2.17 Side Channel Attacks on Smart Grid Field Equipment

A side-channel attack is based on information gained from the physical implementation of a cryptosystem and is generally aimed at extracting cryptographic keys. For example, early smart card implementations were particularly vulnerable to power analysis attacks that could determine the key used by a smart card to perform a cryptographic operation by analysis of the card's power consumption. TEMPEST attacks similarly can extract data by analyzing various types of electromagnetic radiation emitted by a central processing unit (CPU), display, keyboard, etc. Van Eck phreaking in particular can reconstruct the contents of a screen from the radiation emitted by the cathode ray tube (CRT) or liquid crystal display (LCD), and can be performed at some distance. TEMPEST attacks are nearly impossible to detect. Syringe attacks use a needle syringe as a probe to tap extremely fine wire traces on printed circuit boards. Timing attacks exploit the fact that cryptographic primitives can take different lengths of time to execute for different inputs, including keys. In any side-channel attack, it is not necessary for an attacker to determine the entire key; the attacker needs only enough of the key to facilitate the use of other code-breaking methods.

Smart Grid devices that are deployed in the field, such as substation equipment, pole-top equipment, smart meters and collectors, and in-home devices, are at risk of side-channel attacks due to their accessibility. Extraction of encryption keys by side-channel attacks from Smart Grid equipment could lead to compromise of usage information, personal information, passwords, etc. Extraction of authentication keys by side-channel attacks could allow an attacker to impersonate Smart Grid devices and/or personnel, and potentially gain administrative access to Smart Grid systems.

7.2.18 Securing and Validating Field Device Settings

Numerous field devices contain settings. A prominent example is relay settings that control the conditions such as those under which the relay will trip a breaker. In microprocessor devices, these settings can be changed remotely. One potential form of attack is to tamper with relay settings and then attack in some other way. The tampered relay settings would then exacerbate the consequences of the second attack..

A draft NERC white paper on identifying cyber-critical assets recognizes the need for protecting the system by which device settings are determined and loaded to the field devices themselves. This can include the configuration management process by which the settings are determined. It should likely extend to ongoing surveillance of the settings to ensure that they remain the same as intended in the configuration management process.

7.2.19 Absolute & Accurate Time Information

Absolute time is used by many types of power system devices for different functions. In some cases, time may be only informational, but increasingly more and more advanced applications will critically depend on an accurate absolute time reference. According to the draft NERC Control Systems Security Working Group (CSSWG) document, *Security Guideline for the Electricity Sector: Time Stamping of Operational Data Logs*, "these applications include, but are not limited to, Power Plant Automation Systems, Substation Automation Systems, Programmable Logic Controllers (PLC), Intelligent Electronic Devices (IED), sequence of event recorders, digital fault recorders, intelligent protective relay devices, Energy Management Systems (EMS), Supervisory Control and Data Acquisition (SCADA) Systems, Plant Control Systems, routers, firewalls, Intrusion Detection Systems (IDS), remote access systems, physical security access control systems, telephone and voice recording systems, video surveillance systems, and log collection and analysis systems." [§7.5-14] Some detailed examples follow.

7.2.19.1 Security Protocols

Time has impact on multiple security protocols, especially in regard to the integrity of authentication schemes and other operations, if it is invalid or tampered with. For example, some protocols can rely on time stamp information to ensure against replay attacks or in other cases against time-based revoked access. Due care needs to be taken to ensure that time cannot be tampered with in any system or if it is, to ensure that the breach can be detected, responded to, and contained.

7.2.19.2 Synchrophasors

Syncrophasor measurement units are increasingly being deployed throughout the grid. A phasor is a vector consisting of magnitude and angle. The angle is a relative quantity and can be interpreted only with respect to a time reference. A synchrophasor is a phasor that is calculated from data samples using a standard time signal as the reference for the sampling process.

Initial deployments of synchrophasor measurement units use synchrophasors to measure the current state of the power system more accurately than it can be determined through state estimation. If the time references for enough synchrophasor measurements are incorrect, the measured system state will be incorrect, and corrective actions based on this inaccurate information could lead to grid destabilization.

Synchrophasor measurements are beginning to be used to implement wide area protection schemes. With inaccurate time references, these protection schemes may take inappropriate corrective actions that may further destabilize the system.

7.2.19.3 Certificates Time & Date Issues

Certificates are typically used to bind an identity to a public key or keys, facilitating such operations as digital signatures and data encryption. They are widely used on the Internet, but there are some potential problems associated with their use.

Absolute time matters for interpretation of validity periods in certificates. If the system time of a device interpreting a certificate is incorrect, an expired certificate could be treated as valid or a valid certificate could be rejected as expired. This could result in incorrect authentication or rejection of users, incorrect establishment or rejection of VPN tunnels, etc. The Kerberos network authentication protocol (on which Windows domain authentication is based) also depends critically on synchronized clocks.

7.2.19.4 Event Logs and Forensics

Time stamps in event logs must be based on accurate time sources so that logs from different systems and locations can be correlated to reconstruct historical sequences of events. This applies both to logs of power data and to logs of cybersecurity events. Correlating power data from different locations can lead to an understanding of disturbances and anomalies—and a difficulty in correlating logs was a major issue in investigating the August 14, 2003, blackout. Correlating cybersecurity events from different systems is essential to forensic analysis to determine if and how a security breach occurred and to support prosecution.

7.2.20 Personnel Issues in Field Service of Security Technology

Device security features or security devices themselves may add to labor complexity if field personnel have to interact with these devices in any way to accomplish maintenance and installation operations. This complexity may mean significant increases in costs that can lead to barriers for security features and devices being used. Thus due care must be taken when introducing any security procedures and technology to ensure that their management requires minimum disruption to affected labor resources.

For instance, some utilities operate in regulated labor environments. Contractual labor agreements can impact labor costs if field personnel have to take on new or different tasks to access, service, or manage security technology. This can mean a new class or grade of pay and considerable training costs for a large part of the organization. In addition, there are further complexities introduced by personnel screening, clearance, and training requirements for accessing cyber assets.

Another potential ramification of increased labor complexity due to security provisions can occur if employees or subcontractors have a financial incentive to bypass or circumvent the security provisions. For example, if a subcontractor is paid by the number of devices serviced, anything that slows down production, including both safety and security measures, directly affects the bottom line of that subcontractor, thus giving rise to an unintended financial motivation to bypass security or safety measures.

7.2.21 Weak Authentication of Devices in Substations

Inside some substations, where the components are typically assumed to be in a single building or enclosure, access control protection may be weak in that physical security is assumed to exist. For example, some systems may provide access control by MAC address filtering. When a substation is extended to incorporate external components such as solar panels, wind turbines, capacitor banks, etc., that are not located within the physical security perimeter of the substation, this protection mechanism is no longer sufficient.

An attacker who gains physical access to an external component can then eavesdrop on the communication bus and obtain (or guess) MAC addresses of components inside the substation. Indeed, the MAC addresses for many components are often physically printed or stamped on the component. Once obtained, the attacker can fabricate packets that have the same MAC addresses as other devices on the network. The attacker may therefore impersonate other devices, reroute traffic from the proper destination to the attacker, and perform MITM attacks on protocols that are normally limited to the inside of the substation.

7.2.22 Weak Security for Radio-Controlled Distribution Devices

Remotely controlled switching devices that are deployed on pole-tops throughout distribution areas have the potential to allow for faster isolation of faults and restoration of service to unaffected areas. Some of these products that are now available on the market transmit open and close commands to switches over radio with limited protection of the integrity of these control commands. In some cases, no cryptographic protection is used, while in others the protection is weak in that the same symmetric key is shared among all devices.

7.2.23 Weak Protocol Stack Implementations

Many IP stack implementations in control systems devices are not as evolved as the protocol stacks in modern general-purpose operating systems. Improperly formed or unexpected packets can cause some of these control systems devices to lock up or fault in unexpected ways.

7.2.24 Insecure Protocols

Few if any of the control systems communication protocols currently used (primarily DNP3 and sometimes IEC 61850) are typically implemented with security measures. This applies to both serial protocols and IP protocols, such as Distributed Network Protocol (DNP) over Transmission Control Protocol (TCP). IEC 62351 (which is the security standard for these protocols) is now available but implementation adoption and feasibility is not yet clear. There is a secure authentication form of DNP3 under development.

7.2.25 License Enforcement Functions

Vendors and licensors are known to have embedded functions in devices and applications to enforce terms and conditions of licenses and other contracts. When exercised either intentionally or inadvertently, these functions can affect a DoS or even destroy data on critical systems. These functions occur in four general categories:

- **Misuse of authorized maintenance access.** The classic case involves a major consumer product warehouse system where there is a software dispute and the vendor disables the system through a previously authorized maintenance port.

- **Embedded shutdown functions.** Some applications contain shutdown functions that operate on a predetermined schedule unless the user performs a procedure using information supplied by the vendor. The necessary information is supplied to the user if the vendor believes the terms and conditions are being met. If the functions contain errors, they can shut down prematurely and cause DoS. This has reportedly happened on at least one mission-critical hospital-related system.

- **Embedded capability for the licensor to intrude and shut down the system.** Authority for such intrusions is contained in the Uniform Computer Information Transactions Act (UCITA).[4] This uniform state law was promulgated by the Conference of Commissioners on Uniform State Laws, and was highly controversial. It was enacted in Maryland and Virginia, but several states enacted "bomb-shelter" legislation preventing its applicability to consumers and businesses in their states. The intrusion authority is termed "self-help," which is the term used in commercial law for repossession of automobiles and other products by lenders where the purchaser has defaulted. For the licensor to be able to intrude if they believe there is noncompliance with license terms, it is necessary for the operating system or application to have an embedded backdoor.

- **Requiring the application or device to contact a vendor system over the public Internet.** This may occur to authorize initial startup or regularly during operation. It is problematic if the application or device has security requirements that prevent access to the public Internet.

7.2.26 Unmanaged Call Home Functions

Many recent commercial off-the-shelf (COTS) software applications and devices attempt to connect to public IP addresses in order to update software or firmware, synchronize time, provide help/support/diagnostic information, enforce licenses, or utilize Internet resources such as mapping tools, search systems, etc. In many cases, use of such call home functions is not obvious and is poorly documented, if any documentation exists. Configuration options to modify or disable call home functions are often hard to find if available. Examples of such call home functions include:

- Operating system updaters;
- Application updaters, including Web browsers, rendering tools for file formats such as PDF, Flash, QuickTime, Real, etc., printing software and drivers, digital camera software, etc.;
- Network devices that obtain time from one or more Network Time Protocol (NTP) servers;
- Voice-over-Internet-Protocol (VoIP) devices that register with a public call manager;
- Printers that check for updates and/or check a Web database to ensure valid ink cartridges;
- Applications that link to Web sites for documentation; and
- Applications that display information using mapping tools or Google Earth.

[4] http://www.ucitaonline.com/

Some call home functions run only when an associated application is used; some are installed as operating system services running on a scheduled basis; and some run continuously on the device or system. Some call home updaters request confirmation from the user before installing updates, while others quietly install updates without interaction. Some call home functions use insecure channels.

Unexpected call home functions that are either unknown to or not anticipated by the Smart Grid system designer can have serious security consequences. These include:

- Network information leakage;
- Unexpected changes in system configuration through software, firmware, or settings updates;
- Risk of network compromise via compromise of the call home channel or external endpoint;
- Unexpected dependence on external systems, including not only the systems that the call home function calls, but also public DNS and public time sources;
- False positives on IDS systems when outbound connection attempts from call home functions are blocked by a firewall;
- System resource consumption; and
- Additional resource consumption when call home functions continuously attempt to retry connections that are blocked by a firewall.

For the specific case of software or firmware updaters, best practices for patch management recommend deploying patch servers that provide patches to endpoints rather than having those endpoints reach out to the Internet. This provides better control of the patching process. However, most applications use custom updating mechanisms, which can make it difficult to deploy a comprehensive patch system for all operating systems, applications, and devices that may be used by the Smart Grid system. Further, not all applications and devices provide a way to change their configuration to direct them to a patch server.

7.3 Nonspecific Cyber Security Issues

This subsection lists cybersecurity issues that are too abstract to describe in terms of specific security problems but when considered in different contexts (control center, substation, meter, HAN device, etc.) are likely to lead to specific problems.

7.3.1 IT vs. Smart Grid Security

The differences between information technology (IT), industrial, and Smart Grid security need to be accentuated in any standard, guide, or roadmap document. NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*, can be used as a basis, but more needs to be addressed in that control system security operates in an industrial campus setting and is not the same as an environment that has the scale, complexity, and distributed nature of the Smart Grid.

7.3.2 Patch Management

Specific devices such as IEDs, PLCs, smart meters, etc., will be deployed in a variety of environments and critical systems, and their accessibility may necessitate undertaking complex activities to enable software upgrades or patches because of how distributed and isolated the equipment can be. Also, many unforeseen consequences can arise from changing firmware in a device that is part of a larger engineered system. Control systems require considerable testing and qualification to maintain reliability factors.

The patch, test, and deploy life cycle is fundamentally different in the electrical sector. It can take a year or more (for good reason) to go through a qualification of a patch or upgrade. Thus there are unique challenges to be addressed in how security upgrades to firmware need to be managed.

Deployment of a security upgrade or patch is unlikely to be as rapid as in the IT industry. Thus there needs to be a process whereby the risk and impact of vulnerability can be determined in order to prioritize upgrades. A security infrastructure also needs to be in place that can mitigate possible threats until needed upgrades can be qualified and deployed so that the reliability of the system can be maintained.

7.3.3 Authentication

There is no centralized authentication in the decentralized environment of the power grid, and authentication systems need to be able to operate in this massively distributed and locally autonomous setting. For example, substation equipment such as IEDs needs to have access controls that allow only authorized users to configure or operate them. However, credential management schemes for such systems cannot rest on the assumption that a constant network connection to a central office exists to facilitate authentication processes. What is called for are secure authentication methods that allow for local autonomy when needed and yet can provide for revocation and attribution from a central authority as required. Equally important is the recognition that any authentication processes must securely support emergency operations and not become an impediment at a critical time.

7.3.4 System Trust Model

There has to be a clear idea of what elements of the system are trusted—and to what level and why. Practically speaking, there will always be something in the system that has to be trusted; the key is to identify the technologies, people, and processes that form the basis of that trust. For example, we could trust a private network infrastructure more than an open public network, because the former poses less risk. However, even here there are dependencies based on the design and management of that network that would inform the trust being vested in it.

7.3.5 User Trust Model

Today and in the future, many operational areas within the Smart Grid are managed and maintained by small groups of trusted individuals operating as close-knit teams. These individuals are characterized by multi-decade experience and history in their companies. Examples include distribution operations departments, field operations, and distribution engineering/planning. Security architectures designed for large-scale, public access systems such as credit card processing, database applications, etc., may be completely inappropriate in such settings and actually weaken security controls. IT groups will almost always be required for

proper installation of software and security systems on user PCs. However, for these unique systems, administration of security assets, keys, passwords, etc., that require heavy ongoing dependence on IT resources may create much larger and unacceptable vulnerabilities.

In terms of personnel security, it may be worthwhile considering what is known as "two-person integrity," or "TPI." TPI is a security measure to prevent single-person access to key management mechanisms. This practice comes from national security environments but may have some applicability to the Smart Grid where TPI security measures might be thought of as somewhat similar to the safety precaution of having at least two people working in hazardous environments.

Another area of concern related to personnel issues has to do with not having a backup to someone having a critical function; in other words, a person (actor) as a single point of failure (SPOF).

7.3.6 Security Levels

A security model needs to be built with different security levels that depend on the design of the network/system architecture, security infrastructure, and how trusted the overall system and its elements are. This model can help put the choice of technologies and architectures within a security context and guide the choice of security solutions.

7.3.7 Distributed vs. Centralized Model of Management

There are unique issues respecting how to manage something as distributed as the Smart Grid and yet maintain good efficiency and reliability factors that imply centralization. Many grid systems are highly distributed, are geographically isolated, and require local autonomy—as commonly found in modern substations. Yet these systems need to have a measure of centralized security management in terms of event logging/analysis, authentication, etc. There needs to be a series of standards in this area that can strike the right balance and provide for the "hybrid" approach necessary for the Smart Grid.

7.3.8 Local Autonomy of Operation

Any security system must have local autonomy; for example, it cannot always be assumed there is a working network link back to a centralized authority, and particularly in emergency-oriented operations, it cannot be the security system that denies critical actions from being taken.

7.3.9 Intrusion Detection for Power Equipment

One issue specific to power systems is handling specialized protocols like Modbus, DNP3, 61850, etc., and standardized IDS and security event detection and management models need to be built for these protocols and systems. More specifically, these models need to represent a deep contextual understanding of device operation and state to be able to detect when anomalous commands might create an unforeseen and undesirable impact.

7.3.10 Network and System Monitoring and Management for Power Equipment

Power equipment does not necessarily use common and open monitoring protocols and management systems. Rather, those systems often represent a fusion of proprietary or legacy-based protocols with their own security issues. There is a need for openly accessibility

information models and protocols that can be used over a large variety of transports and devices. There might even be a need for bridging power equipment into traditional IT monitoring systems for their cyber aspects. The management interfaces themselves should also be secure, as early lessons with the Simple Network Management Protocol (SNMP) have taught the networking community. Also, and very importantly, the system monitoring and management will have to work within a context of massive scale, distribution, and often, bandwidth-limited connections.

7.3.11 Security Event Management

Building on more advanced IDS forms for Smart Grid, security monitoring data/information from a wide array of power and network devices/systems must start to become centralized and analyzed for detecting events on a correlated basis. There also need to be clear methods of incident response to events that are coordinated between control system and IT groups. Both of these groups must be involved in security event definition and understanding as only they have the necessary operational understanding for their respective domains of expertise to understand what subtleties could constitute a threat.

7.3.12 Cross-Utility / Cross-Corporate Security

Unfortunately, many Smart Grid deployments are going forward without much thought to what happens behind the head end AMI systems and further on down the line for SCADA and other real-time control systems supporting substation automation and other distribution automation projects, as well as the much larger transmission automation functions. Many utilities have not thought about how call centers and DR control centers will handle integration with head end systems. Moreover, in many markets, the company that controls the head end to the meter portion is different than the one who decides what load to shed for a demand response. In many cases, those interconnections and the processes that go along with them have yet to be built or even discussed. Even in a completely vertically integrated system, there are many challenges with respect to separation of duties and least privilege versus being able to get the job done when needed. This also means designing application interfaces that are usable for the appropriate user population and implementing threshold controls, so someone can't disconnect hundreds of homes in a matter of a few seconds either accidentally or maliciously.

7.3.13 Trust Management

Appropriate trust of a device must be based on the physical and logical ability to protect that device, and on protections available in the network. There are many devices that are physically accessible to adversaries by the nature of their locations, such as meters and pole-top devices, which also have limited anti-tamper protections due to cost. Systems that communicate with these devices should use multiple methods to validate messages received, should be designed to account for the possibility that exposed devices may be compromised in ways that escape detection, and should never fully trust those devices.

For example, even when communicating with meters authenticated by public key methods and with strong tamper resistance, unexpected or unusual message types, message lengths, message content, or communication frequency or behavior could indicate that the meter's tamper resistance has been defeated and its private keys have been compromised. Such a successful attack on a meter must not result in possible compromise of the AMI head end.

Similarly, because most pole-top devices have very little physical protection, the level of trust for those devices must be limited accordingly. An attacker could replace the firmware, or, in many systems, simply place a malicious device between the pole-top device and the network connection to the Utility network since these are often designed as separate components with RJ45 connectors. If the head end system for the pole-top devices places too much trust in them, a successful attack on a pole-top device can be used as a stepping stone to attack the head end.

Trust management lays out several levels of trust based on physical and logical access control and the criticality of the system (i.e., most decisions are based on how important the system is). In this type of trust management, each system in the Smart Grid is categorized not only for its own needs (CI&A, etc.) but according to the required trust and/or limitations on trust mandated by our ability to control physical and logical access to it and the desire to do so (criticality of the system). This will lead to a more robust system where compromise of a less trusted component will not easily lead to compromise of more trusted components.

7.3.14 Management of Decentralized Security Controls

Many security controls, such as authentication and monitoring, may operate in autonomous and disconnected fashion because of the often remote nature of grid elements (e.g., remote substations). However, for auditing and centralized security management (e.g., revocation of credentials) requirements, this presents unique challenges.

7.3.15 Password Management

Passwords for authentication and authorization present many problems when used with highly distributed, decentralized, and variedly connected systems such as the Smart Grid. Unlike enterprise environments where an employee typically accesses organization services from one, or at most a few, desktop, laptop, or mobile computing systems, maintenance personnel may need to access hundreds of different devices, including IEDs, RTUs, relays, meters, etc. These devices may sometimes be accessed remotely from a central site, such as a control center, using simple tools such as terminal emulators, sometimes from a front panel with keyboard, sometimes from a locally connected laptop using a terminal emulator, or sometimes from specialized local access ports such as the optical port on a meter. Access must be able to operate without relying on communications to a central server (e.g., RADIUS, Active Directory) since access may be required for power restoration when communications are out. Setting different passwords for every device and every user may be impractical—see Sections 7.2.1, 7.2.2, 7.2.3, and 7.2.9.

NIST SP 800-118, *DRAFT Guide to Enterprise Password Management*, gives reasonable guidance regarding password complexity requirements, but the password management techniques it describes will often be inapplicable due to the nature of power system equipment as discussed above. Suitable password management schemes need to be developed—if possible—that take into account both the nature of Smart Grid systems and of users. Alternatively, multi-factor authentication approaches should be considered.

7.3.16 Authenticating Users to Control Center Devices and Services

Control center equipment based on modern operating systems such as UNIX or Windows platforms is amenable to standard Enterprise solutions such as RADIUS, LDAP, or Active Directory. Nevertheless, these mechanisms may require modification or extension in order to incorporate “break glass” access or to interoperate with access mechanisms for other equipment.

Some access policies commonly used in enterprise systems, such as expiring passwords and locking screen savers, are not appropriate for operator consoles.

7.3.17 Authentication of Devices to Users

When accessing Smart Grid devices locally, such as connecting to a meter via its optical port, authentication of the device to the user is generally not necessary due to the proximity of the user. When accessing Smart Grid devices via a private secure network such as a LAN in a substation tunneled to the control center, or an AMI network with appropriate encryption, non-secure identification of devices, such as by IP address, may be sufficient.

A similar problem to this is that of ensuring that the correct Web server is reached via a Web site address. In Web systems, this problem is solved by SSL certificates that include the Domain Name Service (DNS) identity.

7.3.18 Tamper Evidence

In lieu of or in addition to tamper resistance, tamper evidence will be desirable for many devices. Both tamper resistance and tamper evidence should be resistant to false positives in the form of both natural actions, such as earthquakes, and adversarial actions. Tamper evidence for meters cannot require physical inspection of the meter since this would conflict with zero-touch after installation, but physical indicators might be appropriate for devices in substations.

7.3.19 Challenges with Securing Serial Communications

Cryptographic protocols such as TLS can impose too much overhead on bandwidth-constrained serial communications channels. Bandwidth-conserving and latency-sensitive methods are required in order to secure many of the legacy devices that will continue to form the basis of many systems used in the grid.

7.3.20 Legacy Equipment with Limited Resources

The life cycle of equipment in the electricity sector typically extends beyond 20 years. Compared to IT systems, which typically see 3–5 year life cycles, this is an eternity. Technology advances at a far more rapid rate, and security technologies typically match the trend. Legacy equipment, being 20 years old or more, is resource-limited, and it would be difficult and in some cases impractical to add security to the legacy device itself without consuming all available resources or significantly impacting performance to the point that the primary function and reliability of the device is hindered. In many cases, the legacy device simply does not have the resources available to upgrade security on the device through firmware changes. Security needs to be developed in such a manner that it has a low footprint on devices so that it can scale beyond 20 years, and more needs to be done to provide a systemic and layered security solution to secure the system from an architectural standpoint.

7.3.21 Costs of Patch and Applying Firmware Updates

The costs associated with applying patches and firmware updates to devices in the electricity sector are significant. The balance of cost versus benefit of the security measure in the risk mitigation and decision process can prove prohibitive for the deployment if the cost outweighs the benefits of the deployed patch. Decision makers may choose to accept the risk if the cost is too high compared to the impact.

The length of time to qualify a patch or firmware update, and the lack of centralized and remote patch/firmware management solutions, contributes to higher costs associated with patch management and firmware updates in the electricity sector. Upgrades to devices in the electricity sector can take a year or more to qualify. Extensive regression testing is extremely important to ensure that an upgrade to a device will not negatively impact reliability, but that testing also adds cost. Once a patch or firmware update is qualified for deployment, asset owners typically need to perform the upgrade at the physical location of the device due to a lack of tools for centralized and remote patch/firmware management.

7.3.22 Forensics and Related Investigations

It is already well known that industrial control systems do not generate a lot of security event data and typically do not report it back to a centralized source on a regular basis. Depending on the device, system health, usage, and other concerns, little data may get relayed back to data historians and/or maintenance management systems. Furthermore, as a matter of business policy, when faced with potential cybersecurity threats, electric utilities prioritize their obligation to maintain electric service over the requirements of the evidence collection needed to properly prosecute the perpetrators. With Smart Grid technology, additional threats are arising that may require a greater capability for generating and capturing data. Technologically sophisticated devices such as smart meters are being publicly exposed. At minimum, the meters should be capable of detecting and reporting physical tampering to identify energy theft or billing fraud. Moreover, HAN-level equipment will need to interact with the meter to support demand response. That necessitates having the tools and data to diagnose any problems resulting from either intentional manipulation or other causes. While it is rare that computer forensics is ever the sole basis for a successful prosecution or civil suit, it is critical that reliable means be defined to gather evidentiary material where applicable and that the tools be provided to maintain chain of custody, reduce the risk of spoliation, and ensure that the origin of the evidence can be properly authenticated. Tools should be capable of retrieving data from meters, collectors, and head end systems, as well as other embedded systems in substations, commercial and industrial customer equipment, and sensors along the lines in a read-only manner either at the source or over the network.

7.3.23 Roles and Role-Based Access Control

A *role* is a collection of permissions that may be granted to a user. An individual user may be given several roles or may be permitted different roles in different circumstances and may thereby exercise different sets of permissions in different circumstances.

Roles clearly need to relate to the structure of the using entity and its policies regarding appropriate access. Both the structure and access policies properly flow down from regulatory requirements and organizational governance (i.e., from the high, nontechnical levels of the GridWise Architecture Council [GWAC] stack).

Issues in implementing role-based access control (RBAC) include the following:

1. The extent to which roles should be predefined in standards versus providing the flexibility for individual entities to define their own. Is there a suitable default set of roles that is applicable to the majority of the utility industry but can be tailored to the needs of a specific entity? Such roles might include—

- Auditors: users with the ability to only read/verify the state of the devices (this may include remote attestation);
- System dispatchers: users who perform system operational functions in control centers;
- Protection engineers: users who determine and install/update settings of protective relays and retrieve log information for analysis of disturbances;
- Substation maintainers: users who maintain substation equipment and have access requirements to related control equipment;
- Administrators: users who can add, remove, or modify the rights of other users; and
- Security officers: users who are able to change the security parameters of the device (e.g., authorize firmware updates).

2. Management and usability of roles. How many distinct roles become administratively unwieldy?
3. Policies need to be expressed in a manner that is implementable and relates to an entity's implemented roles. Regulators and entity governance need guidance on how to express implementable policies.
4. Support for nonhierarchical roles. The best example is originator and checker (e.g., of device settings). Any of a group of people can originate and check, but the same person cannot do both for the same item.
5. Approaches to expressing roles in a usable manner.
6. Support for emergency access that may need to bypass normal role assignment.
7. Which devices need to support RBAC? Which do not?

7.3.24 Limited Sharing of Vulnerability and/or Incident Information

There is a significant reticence with respect to sharing information about vulnerabilities or incidents in any critical infrastructure industry. This is based on many sound reasons—not the least of which may be that lives could be on the line and that it can take a considerable amount of time to qualify an upgrade or patch to fix any issue in complex control systems. There needs to exist a better framework for securely sharing such information and quickly coming to field-level mitigations until infrastructure can be upgraded. There also needs to be a better system of accountability and confidentiality when sharing sensitive vulnerability information with any third party, be it government or private institution.

7.3.25 Data Flow Control Vulnerability Issue

The power grid will encompass many networks and subnetworks, and the challenge will be to regulate which system can access or talk to another system.

If a user on system A is authorized to perform a device firmware upgrade on device A, if device A is moved (stolen, replaced, etc.) to system B, how is the authorization tracked? How do you ensure that the control information is not being diverted to another unauthorized device/system?

There is probably a need for intersection of security at various layers.

7.3.26 Public vs. Private Network Use

There is ongoing debate in the industry over the use of public network infrastructures such as the Internet or of the public cellular or WiMax networks that telecommunication companies provide. (Here the term *public network* should not be confused with the use of the Internet Protocol or IP in a *private network* infrastructure.) The reality is that many elements of the Smart Grid might already or will in future make use of public networks. The cybersecurity risks that this introduces need to be addressed by a risk management framework and model that takes this reality into account. It should be clear that if critical real-time command and control functions are carried over public networks such as the Internet (even if technically possible), such a scheme carries significantly more risk of intrusion, disruption, tampering, and general reliability regardless of the countermeasures in place. This is true because of the sheer accessibility of the system by anyone in the world regardless of location and the fact that countermeasures are routinely defeated because of errors in configuration, implementation, and sometimes design. These should be self-evident facts in a risk metric that a model would produce.

Any risk management framework would be well served to address this issue by—

- Building a model that takes the nature of the network, its physical environment, and its architecture into account (e.g., is it private or public, is critical infrastructure sufficiently segmented away from general IT networks, are there physical protection/boundaries, etc.);
- Assigning criticality and impact levels to Smart Grid functions/applications (e.g., retrieval of metering data is not as critical as control commands); and
- Identifying countermeasure systems (e.g., firewalls, IDS/IPS, SEM, encrypted links and data, etc.) and assigning mitigating levels as well as which Smart Grid functions they can reasonably be applied to and how.

The end goal for the model should be to make the best security practices self-evident through a final quantitative metric without giving a specific prohibition.

7.3.27 Traffic Analysis

Traffic analysis is the examination of patterns and other communications characteristics to glean information. Such examination is possible, even if the communication is encrypted. Examples of relevant characteristics include—

- The identity of the parties to the communication (possibly determined from address or header information sent “in the clear” even for otherwise encrypted messages);
- Message length, frequency, and other patterns in the communications; and
- Characteristics of the signals that may facilitate identification of specific devices, such as modems. An example of such a characteristic might be the detailed timing or shape of the waveforms that represent bits.

Regulations such as Federal Energy Regulatory Commission (FERC) Order No. 889 establish “Standards of Conduct” that prohibit market participants from having certain information on the operational state of the grid as known to grid control centers. In the Smart Grid, future

regulations could possibly extend this concept to information outside the bulk power domain. Traffic analysis could enable an eavesdropper to gain information prohibited by such regulations. In addition, even if operational information were encrypted, traffic analysis could provide an attacker with enough information on the operational situation to enable more sophisticated timing of physical or cyber attacks.

7.3.28 Poor Software Engineering Practices

Poor software engineering practices, such as those identified in NISTIR 7628, Chapter 6, "Vulnerability Classes," can lead to software that misoperates and may represent a security problem. Such problems are well known in software, but it should be recognized that embedded firmware may also be susceptible to such vulnerabilities [§7.5-12], and that many of the same good software engineering practices that help prevent these vulnerabilities in software may also be used for that purpose with firmware.

7.3.29 Attribution of Faults to the Security System

When communications or services fail in networks, there is sometimes a tendency to assume this failure is caused by the security system. This can lead to disabling the security system temporarily during problem resolution—or even permanently if re-enabling security is forgotten. Security systems for the Smart Grid need to allow and support troubleshooting.

7.3.30 Need for Unified Requirements Model

Within each operating domain (such as distribution operations, control center operations, etc.) multiple, ambiguous, or potentially conflicting implementation requirements must be resolved and settled upon. If security advisors cannot know what to expect from products meeting a certain standard, then each acquisition cycle will involve a unique security specification. Under such circumstances, it will be nearly impossible for suppliers to provide products in a timely fashion, and diverse systems will be difficult or impossible for customers to administer. The scope of this effort should cover such things as password complexity, required security roles, minimum numbers of supported user IDs, etc.

7.3.31 Broad Definition of Availability

One of the stated goals of the NIST cybersecurity effort is to assure "availability" at the application level. "Availability" according to the DHS *Catalog of Control Systems Security: Recommendations for Standards Developers* [§7.5-13], is—

> Availability— The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.

Presenting such a broad definition to the power delivery organization responsible for achieving that availability, considering the complexity of the Smart Grid, represents a very substantial and perhaps impractical challenge, for several reasons—

- The system, being so broadly defined, could be considered many different systems or many different combinations of systems. Does the system need to be defined as including all of the Smart Grid applications? Does it include future applications?

- As a result, just defining what the "system" is that is being protected could be difficult to reach consensus on.
- "Performance specifications" even for well-defined systems such as a SCADA system will often not be stated in a way that allows underlying media and subsystems to be evaluated. For example, most SCADA systems are designed with certain maximum poll rates and response times, but not necessarily with any requirement for availability in terms of communication interruptions or interference effects. These systems are usually purchased in pieces, with master stations, communications, and field equipment as entirely separate components without any overall specification of the system performance requirements. Thus, the traceability of the performance of all of the individual components and features to system availability as a whole may prove to be extremely difficult.
- Availability in power system reliability means something different from availability (or non-denial of service) in security.
- "Usable upon demand" in the definition of availability could mean many things in terms of response time.

If these systems were used for different purposes, perhaps some very general, functional requirements would suffice to guide the use of the Roadmap by the power delivery organizations. However, all of these systems deliver power; they are all structured similarly, with generation, transmission, and distribution as separate but interconnected systems.

7.3.32 Utility Purchasing Practices

Unlike many other industries, many customers (utilities) in the utility industry are large enough, and have enough purchasing power and longevity (these companies have very long histories and steady income) to be able to specify unique, often customer-specific product features and requirements. For example, prior to the advent of the DNP3 communication protocol, in North America alone, there were over 100 different SCADA protocols developed over the period from roughly 1955 to 1990. Many of these protocols were unique due to a customer requirement for what may have appeared to be a minor change but one which made their protocol implementation unique.

Recently there have been efforts by region, state, and regulatory entities to create purchasing requirements. If not carefully coordinated, these efforts could have similar harmful effects.

With regard to cybersecurity requirements, if security requirements are subject to interpretation, customers will each use their own preferences to specify features that will re-create the problem of the SCADA protocols. For the Smart Grid, this would be a serious problem, since the time and effort necessary to analyze, negotiate, implement, test, release, and maintain a collection of customer-specific implementations will greatly delay deployment of the Smart Grid.

Specifically, with regard to the Smart Grid, recent procurements have shown little consistency, with each calling out different requirements. This can have an adverse affect on both interoperability and security.

7.3.33 Cyber Security Governance

From the IT Governance Institute (ITGI), and adopted by the Chartered Institute of Management Accountants (CIMA) and the International Federation of Accountants (IFAC), *governance* is defined as follows:

> Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.

Cyber security governance is really a subset of enterprise governance. What's included in enterprise governance that directly impacts cybersecurity governance for the Smart Grid is strategic direction: ensuring that goals and objectives are achieved, that business risk (including security risk) is managed appropriately, that resource utilization is efficiently and effectively managed in a responsible fashion, and that enterprise security activities are monitored to ensure success or risk mitigation as needed if there are failures in security.

Since cybersecurity (information security), as opposed to IT security, encompasses an overall perspective on all aspects of data/information (whether spoken, written, printed, electronic, etc.) and how it is handled—from its creation to how it is viewed, transported, stored, and/or destroyed—it is up to the utility's board and executive management to ensure that the Smart Grid, as well as the overall electric grid, is protected as much as feasibly possible.

The utility's board of directors and its executive management must be cognizant of the risks that must be taken into account regarding what vulnerabilities to security threats of any sort may ensue if Smart Grid systems are not created and managed carefully and how such risks may be mitigated.[5]

Borrowing again from ITGI and its guide to "Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition," the following represents a slightly edited perspective on the responsibilities of a utility's board of directors and executive management team regarding cybersecurity:

> *Utility's Boards of Directors/Trustees*
>
> It is a fundamental responsibility of Senior Management to protect the interests of the utility's stakeholders. This includes understanding risks to the business and the electric grid to ensure they are adequately addressed from a governance perspective. Doing so effectively requires risk management, including cyber security risks, by integrating cyber security governance into the overall enterprise governance framework of the utility.
>
> Cyber security governance for the electric grid as a whole requires strategic direction and impetus. It requires commitment, resources and assignment of responsibility for cyber and information security management, as well as a means for the Board to determine that its intent has been met for the electric grid as part of the critical infrastructure of the United States. Experience has shown that effectiveness of cyber security governance is dependent on the involvement of senior management in approving policy, and appropriate monitoring and metrics coupled with reporting and trend analysis regarding threats and vulnerabilities to the electric grid.
>
> Members of the Board need to be aware of the utility's information assets and their criticality to ongoing business operations of the electric grid. This can be accomplished by

[5] See Title XIII, Section 1309 of the Energy Independence and Security Act of 2007 (EISA), U.S Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE).

periodically providing the board with the high-level results of comprehensive risk assessments and business impact analysis. It may also be accomplished by business dependency assessments of information resources. A result of these activities should include Board Members validating/ratifying the key assets they want protected and confirming that protection levels and priorities are appropriate to a recognized standard of due care.

The tone at the top (top-down management) must be conducive to effective security governance. It is unreasonable to expect lower-level personnel to abide by security policies if senior management does not. Visible and periodic board member endorsement of intrinsic security policies provides the basis for ensuring that security expectations are met at all levels of the enterprise and electric grid. Penalties for non-compliance must be defined, communicated and enforced from the board level down.

Utility Executives

Implementing effective cyber security governance and defining the strategic security objectives of the utility are complex, arduous tasks. They require leadership and ongoing support from executive management to succeed. Developing an effective cyber security strategy requires integration with and cooperation of business unit managers and process owners. A successful outcome is the alignment of cyber security activities in support of the utility's objectives. The extent to which this is achieved will determine the effectiveness of the cyber security program in meeting the desired objective of providing a predictable, defined level of management assurance for business processes and an acceptable level of impact from adverse events.

An example of this is the foundation for the U.S. federal government's cyber security, which requires assigning clear and unambiguous authority and responsibility for security, holding officials accountable for fulfilling those responsibilities, and integrating security requirements into budget and capital planning processes.

Utility Steering Committee

Cyber security affects all aspects of the utility. To ensure that all Stakeholders affected by security considerations are involved, a Steering Committee of Executives should be formed. Members of such a committee may include, amongst others, the Chief Executive Officer (CEO) or designee, business unit executives, Chief Financial Officer (CFO), Chief Information Officer (CIO)/IT Director, Chief Security Officer (CSO), Chief Information Security Officer (CISO), Human Resources, Legal, Risk Management, Audit, Operations and Public Relations.

A Steering Committee serves as an effective communication channel for Management's aims and directions and provides an ongoing basis for ensuring alignment of the security program with the utility's organizational objectives It is also instrumental in achieving behavior change toward a culture that promotes good security practices and policy compliance.

Chief Information Security Officer

All utility organizations have a CISO whether or not anyone actually holds that title. It may be the CIO, CSO, CFO, or, in some cases, the CEO, even when there is an Information Security Office or Director in place. The scope and breadth of cyber security concerns are such that the authority required and the responsibility taken inevitably end up with a C-level officer or Executive Manager. Legal responsibility, by default, extends up the command structure and ultimately resides with Senior Management and the Board of Directors.

Failure to recognize this and implement appropriate governance structures can result in Senior Management being unaware of this responsibility and the attendant liability. It usually results in a lack of effective alignment of security activities with organizational objectives of the utility.

Increasingly, prudent and proactive management is elevating the position of Information Security Officer to a C-level or Executive Position as utilities begin to understand their dependence on information and the growing threats to it. Ensuring that the position exists, and assigning it the responsibility, authority and required resources, demonstrates Management's and Board of Directors' awareness of and commitment to sound cyber security governance.

7.4 DESIGN CONSIDERATIONS

This subsection discusses cybersecurity considerations that arise in the design, deployment, and use of Smart Grid systems and should be taken into account by system designers, implementers, purchasers, integrators, and users of Smart Grid technologies. In discussing the relative merits of different technologies or solutions to problems, these design considerations stop short of recommending specific solutions or even requirements.

7.4.1 Break Glass Authentication

Authentication failure must not interfere with the need for personnel to perform critical tasks during an emergency situation. An alternate form of "break glass" authentication may be necessary to ensure that access can be gained to critical devices and systems by personnel when ordinary authentication fails for any reason. A "break glass" authentication mechanism should have the following properties—

- Locally autonomous operation—to prevent failure of the "break glass" authentication mechanism due to failure of communications lines or secondary systems;
- Logging—to ensure that historical records of use of the "break glass" mechanism, including time, date, location, name, employee number, etc., are kept;
- Alarming—to report use of the "break glass" mechanism in real-time or near real-time to an appropriate management authority, e.g., to operators at a control center or security desk;
- Limited authorization—to enable only necessary emergency actions and block use of the "break glass" mechanism for non-emergency tasks; disabling logging particularly should not be allowed; and
- Appropriate policies and procedures—to ensure the "break glass" authentication is used only when absolutely necessary and does not become the normal work procedure.

Possible methods for performing "break glass" authentication include but are not limited to—

- Backup authentication via an alternate password that is not normally known or available but can be retrieved by phone call to the control center, by opening a sealed envelope carried in a service truck, etc.;
- Digital certificates stored in two-factor authentication tokens; and
- One-time passwords.

7.4.2 Biometrics

7.4.3 Password Complexity Rules

Password complexity rules are intended to ensure that passwords cannot be guessed or cracked by either online or offline password-cracking techniques. Offline password cracking is a particular risk for field equipment in unmanned substations or on pole-tops where the equipment is vulnerable to physical attack that could result in extraction of password hash databases and for unencrypted communications to field equipment where password hashes could be intercepted.

Incompatible password complexity requirements can make reuse of a password across two different systems impossible. This can improve security since compromise of the password from one system will not result in compromise of password of the other system. Incompatible password complexity requirements might be desirable to force users to choose different passwords for systems with different security levels, e.g., corporate desktop vs. control system. However, forcing users to use too many different passwords can cause higher rates of forgotten passwords and lead users to write passwords down, thereby reducing security. Due to the large number of systems that utility engineers may need access to, reuse of passwords across multiple systems may be necessary. Incompatible password complexity requirements can also cause interoperability problems and make centralized management of passwords for different systems impossible. NIST SP 800-63, *Electronic Authentication Guideline*, contains some guidance on measuring password strength and recommendations for minimum password strengths.

Some considerations for password complexity rules—

1. Are the requirements based on a commonly recognized standard?
2. Are the requirements strong enough to measurably increase the effort required to crack passwords that meet the rules?
3. Are there hard constraints in the requirements (e.g., minimum and maximum lengths, min and max upper and lowercase, etc.) or soft constraints that simply measure password strength?
4. Are any hard constraints "upper bounds" that can make selecting a password that meets two or more different complexity requirement sets impossible? For example, “must start with a number” and “must start with a letter” are irreconcilable requirements, whereas “must contain a number” and “must contain a letter” do not conflict.
5. Are there alternatives to password complexity rules (such as running password-cracking programs on passwords as they are chosen) or two-factor authentication that can significantly increase security over that provided by password complexity rules while minimizing user burden?

Draft NIST SP 800-118 gives further guidance on password complexity.

7.4.4 Authentication

There is no standard currently in the Smart Grid Framework and Roadmap that supports or provides guidance on how to accomplish strong authentication. The initial release of the NERC Critical Infrastructure Protection (CIP) standards did not require strong authentication. In accepting that version of the standards, FERC Order 706 requested NERC to incorporate strong authentication into a future version of the standards.

During the drafting of IEEE-1686, the *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*, an effort was made to incorporate strong authentication. The best source of information on strong authentication was found to be NIST SP 800-63, but the format of that document was found unsuitable as a normative reference for an IEEE standard. However, the technical material in NIST SP 800-63 provides some useful advantages for the following reasons:

- The NERC CIP standards are moving from a concept of critical and noncritical assets to three levels of impact: High, Medium, Low;
- NIST SP 800-63-1 provides four levels of authentication assurance, potentially mappable to both the NERC CIP impact levels and the similar approach being taken in the High-Level Requirements of NISTIR 7628;
- NIST SP 800-63 provides a framework of requirements but is not overly prescriptive regarding implementation; and
- The multilevel approach taken in NIST SP 800-63 is compatible with similar approaches previously taken in guidelines produced for the Bulk Electric System by the NERC Control Systems Security Working Group.

NIST SP 800-63 is a performance specification with four levels of authentication assurance, selectable to match risk. The alternative levels range from Level 1, that allows a simple user ID and password, to Level 4, that is "intended to provide the highest practical remote network authentication assurance." [§7.5-15] Multi-factor authentication is required at Levels 3 and 4. The NIST document grades the levels in terms of protection against increasingly sophisticated attacks.

7.4.5 Network Access Authentication and Access Control

Several link-layer and network-layer protocols provide network access authentication using Extensible Authentication Protocol [§7.5-1]. EAP supports a number of authentication algorithms—so called EAP methods.

Currently EAP-TLS [§7.5-2] and EAP-GPSK Generalized Pre-Shared Key) [§7.5-3] are the IETF Standard Track EAP methods generating key material and supporting mutual authentication. EAP can also be used to provide a key hierarchy to allow confidentiality and integrity protection to be applied to link-layer frames.

EAP IEEE 802.1X [§7.5-4] provides port access control and transports EAP over Ethernet and Wi-Fi. In WiMAX, PKMv2 (Privacy Key Management version 2) in IEEE 802.16e [§7.5-5] transports EAP. PANA (Protocol for carrying Authentication for Network Access) [§7.5-6] transports EAP over UDP/IP (User Datagram Protocol/Internet Protocol). TNC (Trusted Network Connect) [§7.5-7] is an open architecture to enable network operators to enforce policies regarding endpoint integrity using the above mentioned link-layer technologies. There are also ongoing efforts in ZigBee® Alliance [§7.5-8] to define a network access authentication mechanism for ZigBee Smart Energy 2.0.

In a large-scale deployment, EAP is typically used in pass-through mode where an EAP server is separated from EAP authenticators, and an AAA (Authentication, Authorization, and Accounting) protocol such as RADIUS [§7.5-9] is used by a pass-through EAP authenticator for forwarding EAP messages back and forth between an EAP peer to the EAP server. The pass-

through authenticator mode introduces a three-party key management, and a number of security considerations so called EAP key management framework [§7.5-10] have been made. If an AMI network makes use of EAP for enabling confidentiality and integrity protection at link-layer, it is expected to follow the EAP key management framework.

7.4.6 Use of Shared/Dedicated and Public/Private Cyber Resources

The decision whether to use the public Internet or any shared resource, public or private, will have significant impact on the architecture, design, cost, security, and other aspects of any part of the Smart Grid. This section provides a checklist of attributes with which architects and designers can conduct a cost/trade analysis of these different types of resources.

The objective of any such analysis is to understand the types of information that will be processed by the cyber resources under consideration, and to evaluate the information needs relative to security and other operational factors. These needs should be evaluated against the real costs of using different types of resources. For example, use of the public Internet may be less costly than developing, deploying, and maintaining a new infrastructure, but it may carry with it performance or security considerations to meet the requirements of the Smart Grid information that would have to be weighed against the cost savings.

Each organization should conduct its own analyses—there is not one formula that is right for all cases.

7.4.6.1 Definitions

There are two important definitions to keep in mind when performing the analysis—

1. Cyber Equipment—anything that processes or communicates Smart Grid information or commands.
2. Internet—An element of Smart Grid data is said to have used the Internet if at any point while traveling from the system that generates the data-containing message to its ultimate destination it passes through a resource with an address within an RIR (Regional Internet Registry) address space.

7.4.6.2 Checklist/Attribute Groupings

There following five lists contain attributes relevant to one dimension of the cost/trade analysis—

1. Attributes related to Smart Grid Information—this list could be viewed as the requirements of the information that is to be processed by the Smart Grid cyber resource;
    a. Sensitivity and Security Requirements;
        - Integrity,
        - Confidentiality,
        - Timeliness considerations—how long is the information sensitive?
        - Availability, and
        - Strategic vs. tactical information—aggregation considerations/impacts;
    b. Ownership—who owns the data;

c. Who has a vested interest in the data (e.g., customer use data);

d. Performance/Capacity/Service-level requirements; and

- Latency,
- Frequency of transmission,
- Volume of data,
- Redundancy/Reliability, and
- Quality of Service; and

e. Legal/Privacy considerations—in this context, privacy is not related to protection of the data as it moves through the Smart Grid. It is related to concerns stakeholders in the information would have in its being shared. For example, commercial entities might not wish to have divulged how much energy they use.

2. Attributes of a Smart Grid Cyber Resource—cyber resources have capabilities/attributes that must be evaluated against the requirements of the Smart Grid information;

a. Ownership

- Dedicated, and
- Shared;

b. Controlled/managed by

- Internal management,
- Outsourced management to another organization, and
- Outsourced management where the resource can be shared with others;

c. Geographic considerations—jurisdictional consideration;

d. Physical Protections that can be used

- Media,
  1. Wired, and
  2. Wireless.
     a. Not directed, and
     b. Directed
- Equipment, and
- Site;

e. Performance/Scale Characteristics

- Capacity per unit time (for example, a measure of bandwidth),
- Maximum utilization percentage,

- Ability to scale—are forklift upgrades needed? Related to this is the likelihood of a resource being scaled—what are the factors (economic and technical) driving or inhibiting upgrade?
- Latency, and
- Migration—ability to take advantage of new technologies;

f. Reliability;

g. Ability to have redundant elements; and

h. Known security vulnerabilities.

- Insider attacks,
- DOS,
- DDOS, and
- Dependency on other components.

3. Attributes related to Security and Security Properties—given a type of information and the type of cyber resource under consideration, a variety of security characteristics could be evaluated—including different security technologies and appropriate policies given the information processed by, and attributes of, the cyber resource.

a. Physical security and protection;

b. Cyber protection

- Application level Controls,
- Network level controls, and
- System;

c. Security/Access policies

- Inter organizational, and
- Intra organizational;

d. Cross-administrative domain boundary policies; and

e. Specific technologies.

4. Attributes related to Operations and Management—one of the most complex elements of a network is the ongoing operations and management necessary after it has been deployed. This set of attributes identifies key issues to consider when thinking about different types of Smart Grid cyber resources (e.g., public/private and shared/dedicated).

a. Operations

- People,
  1. Domain Skills (e.g., knowledge of control systems), and
  2. IT Operations Skills (e.g., systems and network knowledge).
- Processes

1. Coordination
    a. Within a department,
    b. Across departments, and
    c. Across organizations/enterprises.
2. Access Controls
    a. Third Party, and
        - Frequency,
        - Control, and
        - Trusted/Untrusted party (e.g., vetting process).
    b. Employees; and
3. Auditing.

b. System-level and Automated Auditing;

c. Monitoring
    - Unit(s) monitored—granularity,
    - Frequency,
    - Alarming and events,
    - Data volume,
    - Visibility to data,
    - Sensitivity, and
    - Archival and aggregation; and

d. Management.
    - Frequency of change,
    - Granularity of change,
    - Synchronization changes,
    - Access control,
    - Rollback and other issues, and
    - Data management of the configuration information.

5. Attributes related to Costs—the cost attributes should be investigated against the different types of cyber resources under consideration. For example, while a dedicated resource has a number of positive performance attributes, there can be greater cost associated with this resource. Part of the analysis should be to determine if the benefits justify the cost. The cost dimension will cut across many other dimensions.

    a. Costs related to the data
        - Cost per unit of data,

- Cost per unit of data over a specified time period, and
- Oversubscription or SLA costs;

b. Costs related to resources (cyber resources)
- Resource acquisition cost (properly apportioned),
- Resource installation cost,
- Resource configuration,
- Resource operation and management cost, and
- Monitoring cost;

c. Costs related to operational personnel
- Cost of acquisition,
- Cost of ongoing staffing, and
- Cost of Training;

d. Costs related to management software
- Infrastructure costs,
- Software acquisition costs,
- Software deployment and maintenance costs, and
- Operational cost of the software—staff, etc.; and

e. How are the common costs being allocated and shared?

7.5 REFERENCES

1. Aboba, B., L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC3748. The Internet Society, 2004. http://www.ietf.org/rfc/rfc3748.txt (accessed December 5, 2012).
2. D. Simon, B. Aboba and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, The Internet Society, 2008. http://www.ietf.org/rfc/rfc5216.txt (accessed December 5, 2012).
3. Clancy, T. and H. Tschofenig, “Extensible Authentication Protocol - Generalized Pre-Shared Key (EAP-GPSK) Method”, RFC5433, The Internet Society, 2009. http://www.ietf.org/rfc/rfc5433.txt (accessed December 5, 2012).
4. *IEEE Standard for Local and Metropolitan Area Networks Port-based Network Access Control*, IEEE Std 802.1X-2004. New York, NY: The Institute of Electrical and Electronics Engineers, Inc. (IEEE), 2004.
5. *IEEE Draft Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems ((Revision of IEEE Std 802.16-2004 and consolidates material from IEEE Std 802.16e-2005, IEEE Std 802.16-2004/Cor1-2005, IEEE Std 802.16f-2005 and IEEE Std 802.16g-2007))*, IEEE Unapproved Draft Standard P802.16Rev2_D4, New York, NY: IEEE, 2008..

6. D. Forsberg and others, “Protocol for Carrying Authentication for Network Access (PANA)”, RFC5191, The Internet Society, 2008. http://www.ietf.org/rfc/rfc5191.txt (accessed December 5, 2012).
7. Trusted Network Connect (TNC), the Trusted Computing Group. http://www.trustedcomputinggroup.org/developers/trusted_network_connect (accessed December 5, 2012).
8. ZigBee® Alliance, http://www.zigbee.org/
9. Rigney C, Willens S, Rubens A and Simpson W, "Remote authentication dial in user service (RADIUS)", RFC 2865, http://www.ietf.org/rfc/rfc2865.txt, June 2000.
10. B. Aboba, D. Simon and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework", RFC 5247, http://www.ietf.org/rfc/rfc5247.txt, August 2008.
11. Donggang Liu, Peng Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03), pages 52--61, Washington D.C., October, 2003.
12. Katie Fehrenbacher "Smart Meter Worm Could Spread Like a Virus", http://earth2tech.com/2009/07/31/smart-meter-worm-could-spread-like-a-virus/.
13. Department of Homeland Security, National Cyber Security Division, *Catalog of Control Systems Security: Recommendations for Standards Developers*, March 2010.
14. NERC Control Systems Security Working Group (CSSWG) document, *Security Guideline for the Electricity Sector: Time Stamping of Operational Data Logs*, v. 0.995, http://www.nerc.com/docs/cip/sgwg/Timestamping_Guideline_009-11-11_Clean.pdf
15. Burr, William E. and others. NIST Special Publication (SP) 800-63-1, *Electronic Authentication Guideline*, Gaithersburg, MD: NIST, 2011.
16. Stouffer, Keith, Joe Falco, and Karen Scarfone, NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*, Gaithersburg, MD: NIST, 2011.
17. Scarfone, Karen and Murugiah Souppaya, DRAFT NIST SP 800-118, *Guide to Enterprise Password Management*, Gaithersburg, MD: NIST, 2009.
18. Scarfone, Karen, Cyrus Tibbs, and Matthew Sexton, NIST SP 800-127, *Guide to Securing WiMAX Wireless Communications*, Gaithersburg, MD: NIST, 2010.

CHAPTER 8
RESEARCH AND DEVELOPMENT THEMES FOR CYBERSECURITY IN THE SMART GRID

8.1 INTRODUCTION

Cybersecurity is one of the key technical areas where the state of the art falls short of meeting the envisioned functional, reliability, and scalability requirements of the Smart Grid. This chapter is the deliverable originally produced by the R&D subgroup of SGIP-CSWG based on the inputs from various group members with updates made for the first revision of this document. In general, *research* involves discovery of the basic science that supports a product's viability (or lays the foundation for achieving a target that is currently not achievable), *development* refers to turning something into a useful product or solution, and *engineering* refines a product or solution to a cost and scale that makes it economically viable. Another differentiation is basic research, which delves into scientific principles (usually done in universities), and applied research, which uses basic research to better human lives. Research can be theoretical or experimental. Finally, there is long-term (5–10 years) and short-term (less than 5 years) research. This chapter stops short of specifying which of the above categories each research problem falls into. That is, we do not discuss whether something is research, development, engineering, short-term, or long-term, although we might do so in future revisions. In general, this chapter distills research and development themes that are meant to present paradigm changing directions in cybersecurity that will enable higher levels of reliability and security for the Smart Grid as it continues to become more technologically advanced.

The topics are based partly on the experience of members of the SGIP-CSWG R&D group and research problems that are widely publicized. The raw topics submitted by individual group members were collected in a flat list and iterated over to disambiguate and re-factor them to a consistent set. The available sections were then edited, consolidated, and reorganized as the following five high-level theme areas:

- Device Level
- Cryptography and Key Management
- Systems and Distributed Systems Level
- Networking Issues
- Other Security Issues in the Smart Grid Context

These five groups collectively represent an initial cut at the thematic issues requiring immediate research and development to make the Smart Grid vision a viable reality. It is expected that this work will continue to be revised and updated as new topics are identified by SGIP-SGCC subgroups; by comments from readers; and by tracking government, academic, and industry research efforts that are related to Smart Grid cybersecurity. These research efforts include the U.S. Department of Energy Control System Security and the National SCADA Testbed programs, U.S. Department of Homeland Security Control System Security program and Cyber

Physical Systems Security efforts,[6] the industry Roadmap to Secure Control Systems, the UCA International Users group focusing on AMI security, and the North American Synchrophasor Initiative.

This document is written as an independent collection of research themes, and as such, the sections do not necessarily flow from introduction to summary.

8.2 Device-Level Topics—Cost-Effective Tamper-Resistant Device Architectures

8.2.1 Improve Cost-Effective High Tamper-Resistant & Survivable Device Architectures

With intelligent electronic devices (IEDs) playing more critical roles in the Smart Grid, there is an increasing need to ensure that those IEDs are not easily attacked by firmware updates, commandeered by a spoofed remote device, or swapped out by a rogue device. At the same time, because of the unique nature and scale of these devices, protection measures need to be cost-effective as to deployment and use, and the protection measures must be mass-producible. Some initial forms of these technologies are in the field, but there is a growing belief that further improvement is needed, as security researchers have already demonstrated penetrations of these devices—even with some reasonable protections in place. Further, it is important to assume devices *will be* penetrated, and there must be a method for their containment and implementing secure recovery measures using remote means. This is of great importance to maintain the reliability and overall survivability of the Smart Grid.[7]

Research is needed in devising scalable, cost-effective device architectures that can form a robust hardware and software basis for overall systems-level survivability and resiliency. Such architectures must be highly tamper-resistant and evident, and provide for secure remote recovery. Research into improved security for firmware/software upgrades is also needed. Without these R&D advances, local attacks can become distributed/cascading large-scale attack campaigns.

Potential starting points for these R&D efforts are

- NIST crypto tamper-evident requirements;
- Mitigating (limiting) the value of attacks at end-points (containment regions in the Smart Grid architecture); and
- Expiring lightweight keys.

8.2.2 Intrusion Detection with Embedded Processors

Research is needed to find ways to deal with the special features and specific limitations of embedded processors used in the power grid. A large number of fairly powerful processors, but with tighter resources than general-purpose computers and strict timeliness requirements, embedded in various types of devices, are expected to form a distributed internetwork of

[6] See https://www.enstg.com/Signup/files/DHS%20ST%20Cyber%20Workshop%20Final%20Report-v292.pdf.
[7] Please see Chapter 2 for discussion of defense-in-depth on a system-wide basis that would begin to address these issues.

embedded systems. Intrusion detection in such systems does not merely consist in adapting the types of intrusion detection developed for classical IT systems.[8]

This work should also investigate the possible applications of advanced intrusion detection systems and the types of intrusion detection that may be possible for embedded processors, such as real-time intrusion detection.

8.3 Cryptography and Key Management

8.3.1 Topics in Cryptographic Key Management

Smart Grid deployments such as AMI will entail remote control of a large number of small processors acting as remote sensors, such as meters and smart devices. Home Area Networks (HANs) provide local sensing and actuation of smart appliances. HANs and devices may communicate and negotiate in a peer-to-peer manner. Security for such systems entails both key management on a scale involving possibly tens of millions of credentials and keys, and local cryptographic processing on the sensors such as encryption and digital signatures. This calls for research on large-scale, economic key management in conjunction with cryptography that can be carried out effectively on processors with strict limits on space and computation. This cryptography and key management should ideally be strong and open (free of intellectual property issues) to foster the necessary interoperability standards of the Smart Grid. Existing key management systems and methods could be explored as a basis of further innovation; examples can include public key infrastructure (PKI), identity-based encryption (IBE), and hierarchical, decentralized, and delegated schemes and their hybridization.

There are also problems of ownership (e.g., utility vs. customer-owned) and trust, and how both can be optimally managed in environments where there is little physical protection and access may happen across different organizational and functional domains (e.g., a hub of multiple vendors/service providers, in-home gateway, aggregator, etc.) with their own credentials and security levels. This requires research into new forms of trust management, partitioning, tamper-proofing/detection, and federated ID management that can scale and meet reliability standards needed for the Smart Grid.

The various devices/systems that will be found in the areas of distributed automation, AMI, distributed generation, substations, etc., will have many resource-constraining factors that have to do with limited memory, storage, power (battery or long sleep cycles), bandwidth, and intermittent connections. All of these factors require research into more efficient, *ad hoc*, and flexible key management that requires less centralization and persistent connectivity and yet can retain the needed security and trust levels of the entire infrastructure as compared to conventional means.

Emergency (bypass) operations are a critical problem that must optimally be addressed. We cannot afford to have security measures degrade the reliability of the system by, for example, "locking out" personnel/systems during a critical event. Similarly, restoring power may require systems to "cold boot" their trust/security with little to no access to external authentication/authorization services. This requires research into key management and cryptography schemes that can support bypass means and yet remain secure in their daily operations.

[8] Subsection 8.6.3 of this report discusses this issue in the context of protecting cyber-power systems.

We must ensure that encrypted communications do not hinder existing power system and information and communication systems monitoring for reliability and security requirements (possibly from multiple parties of different organizations). Depending on the system context, this problem may require research into uniquely secure and diverse escrow schemes and supporting key management and cryptography that meet the various Smart Grid requirements discussed in this report.

8.3.2 Advanced Topics in Cryptography

Several security and privacy requirements for the Smart Grid may benefit from advanced cryptographic algorithms.

8.3.2.1 Privacy-enhancing cryptographic algorithms

Privacy-enhancing cryptographic algorithms can mitigate privacy concerns related to the collection of consumer data by computing functions on ciphertexts. This can be beneficial for third-party providers who want to access encrypted databases and would like to compute statistics over the data. Similarly, while utilities need to collect individual measurements for billing, they do not require real-time individual data collection to operate their network. Therefore, they can use aggregated data representing the consumption at a data aggregator. Homomorphic encryption schemes can provide privacy-preserving meter aggregation by performing additive computations on encrypted data. Using aggregated data limits the ability of the utility or any third party from learning individual consumer usage profiles . Research is needed on extending the efficiency and generality of current homomorphic encryption schemes to provide universal computation.

8.3.2.2 Cryptographic in-network aggregation schemes

Cryptographic in-network aggregation schemes have the potential of improving the efficiency of many-to-one communications in the Smart Grid, like those generated from multiple sensors to a single or a small number of designated collection points. To achieve efficient in-network aggregation, intermediate nodes in the routing protocol need to modify data packets in transit; for this reason, standard signature and encryption schemes are not applicable, and it is a challenge to provide resilience to tampering by malicious nodes. Therefore, we require homomorphic encryption and signature schemes tailored for efficient in-network aggregation.

8.3.2.3 Identity-Based Encryption

Key distribution and key revocation are some of the most fundamental problems in key distribution for systems. IBE is a new cryptographic primitive that eliminates the need for distributing public keys (or maintaining a certificate directory) because identities are automatically bound to their public keys. This allows, for example, a third party for energy services to communicate securely to their customers without requiring them to generate their keys. IBE also eliminates the need for key revocation because IBE can implement time-dependent public keys by attaching a validity period to each public key. In addition, for enterprise systems, a key escrow is an advantage for recovering from errors or malicious insiders. IBE provides this service because the private-key generator (PKG) can obtain the secret key of participants. This property suggests that IBE schemes are suitable for applications where the PKG is unconditionally trusted. Extending this level of trust for larger federated systems is not possible; therefore, very large deployments require hybrid schemes with traditional public

key cryptography and certificates for the IBE parameters of each enterprise or domain. Alternatively, we can extend pure IBE approaches with further research on certificate-based encryption.

8.3.2.4 Access control without a mediated, trusted third party

The limited (or intermittent) connectivity of several Smart Grid devices requires further research into access control mechanisms without an online third party. Attribute-Based Encryption (ABE) is an emerging crypto-system that can be thought of as a generalization of IBE. In ABE schemes, a trusted entity distributes attribute or predicate keys to users. Data owners encrypt their data using the public parameters and attributes provided by the trusted entity or an attribute policy of their choosing. In ABE, users are able to decrypt ciphertexts only if the attributes associated with the ciphertext (or the keys of the users) satisfy the policy associated with the ciphertext (or the predicate associated with their keys); therefore, access control can be achieved without an online trusted server.

8.3.2.5 Interoperability with limited (or no) online connectivity

The limited (or intermittent) connectivity of Smart Grid devices may require local (e.g., HAN) mechanisms for key and content management. Proxy re-encryption and proxy re-signature schemes can alleviate this problem. In these schemes, a semi-trusted proxy (e.g., a HAN interoperability device) can convert a signature or a ciphertext computed under one key (e.g., the public key of device A) to another (e.g., the public key of device B), without the proxy learning any information about the plaintext message or the secret keys of the delegating party.

8.4 Systems-Level Topics - Security and Survivability Architecture of the Smart Grid

While it is not uncommon for modern distribution grids to be built to withstand some level of tampering to meters and other systems that cannot be physically secured, as well as a degree of invalid or falsified data from home area networks, the envisioned Smart Grid will be a ripe target for malicious, well-motivated, well-funded adversaries. The increased dependence on information and distributed and networked information management systems in SCADA, WAMS, and PLCs imply that the Smart Grid will need much more than device authentication, encryption, failover, and models of normal and anomalous behavior, all of which are problems on their own given the scale and timeliness requirement of the Smart Grid. The Smart Grid is a long-term and expensive resource that must be built future-proof. It needs to be built to adapt to changing needs in terms of scale and functionality, and at the same time, it needs to be built to tolerate and survive malicious attacks of the future that we cannot even think of at this time. Research is clearly needed to develop an advanced protection architecture that is dynamic (can evolve) and focuses on resiliency (tolerating failures, perhaps of a significant subset of constituents). A number of research challenges that are particularly important in the Smart Grid context are described in the following subsections.

8.4.1 Scalability

The introduction of smart appliances and home area networks (HANs) increases the number of devices that a utility must manage by orders of magnitude. A utility with 1million customers currently monitoring 1million meters will conservatively see the number of devices two orders of

magnitude higher (perhaps 100 million devices). The ability to control and schedule these through a central SCADA system will be severly limited. As such reliance will need to be on scheduling through HANs and distributed peer-to-peer energy management, or, an "energy internet." System vulnerabilities will be increased through the addition of potential attack points. The increased number of devices will impact system reliability and system reliability models.

8.4.2 Architecting for bounded recovery and reaction

Effective recovery requires containing the impact of a failure (accidental or malicious); enough resources and data (e.g., state information) positioned to regenerate the lost capability; and real-time decision making and signaling to actuate the reconfiguration and recovery steps. Even then, guaranteeing the recovery within a bounded time is a hard problem and can be achieved only under certain conditions. To complicate things further, different applications in the Smart Grid will have different elasticity and tolerance, and recovery mechanisms may themselves affect the timeliness of the steady state, not-under-attack operation.

With the presence of renewable energy sources that can under normal operation turn on or off unpredictably (cloud cover or lack of wind) and mobile energy sinks (such as the hybrid vehicle) whose movement cannot be centrally controlled, the Smart Grid becomes much more dynamic in its operational behavior. Reliability will increasingly depend on the ability to react to these events within a bounded time while limiting the impact of changes within a bounded spatial region. How does one architect a wide area distributed system of the scale of the Smart Grid such that its key components and designated events have a bounded recovery and reaction time and space? What resources need to be available? What cryptographic/key material needs to be escrowed or made available? How much data needs to be checkpointed and placed at what location? What is the circle of influence that needs to be considered to facilitate bounded recovery and reaction? These are the questions that the R&D task should answer.

8.4.3 Architecting Real-time security

In the context of Smart Grid, the power industry will increasingly rely on real-time systems for advanced controls. These systems must meet requirements for applications that have a specific window of time to correctly execute. Some "hard real-time" applications must execute within a few milliseconds. Wide area protection and control systems will require secure communications that must meet tight time constraints. Cyber physical systems often entail temporal constraints on computations because control must track the dynamic changes in a physical process. Typically such systems have been treated as self-contained and free of cybersecurity threats. However, increasing openness and interoperability, combined with the threat environment today, requires that such systems incorporate various security measures ranging from device and application authentication, access control, redundancy and failover for continued operation, through encryption for privacy and leakage of sensitive information. Real-time requirements must include the overhead resulting from insertion of these mechanisms. In some cases, security mechanisms have the potential to violate the real-time requirements by introducing uncontrollable or unbounded delays.

Research in this area should provide strategies for minimizing and making predictable the timing impacts of security protections such as encryption, authentication, and rekeying and exploiting these strategies for grid control with security.

8.4.4 Calibrating assurance and timeliness trade-offs

There are various sources of delay in the path between two interacting entities in the Smart Grid (e.g., from the sensor that captures the measurement sample such as the PMU to the application that consumes it, or from the applications at the control center that invoke operations, upload firmware, or change parameter values to the affected remote smart device). Some such delay sources represent security mechanisms that already exist in the system, and many of these can be manipulated by a malicious adversary. To defend against potential attacks, additional security mechanisms are needed—which in turn may add more delay. On the other hand, security is not absolute, and quantifying cybersecurity is already a hard problem. Given the circular dependency between security and delay, the various delay sources in the wide area system, and the timeliness requirements of the Smart Grid applications, there is a need and challenge to organize and understand the delay-assurance tradespace for potential solutions that are appropriate for grid applications. As the smart grid scales, the ability of humans to react to systems operating in the millisecond time scale becomes limited. As such, there will need to be more reliance on embedded monitors and distributed embedded monitors to provide diagnosis and recovery actions. Only at the highest level of control can human operators become effective. Without an understanding of delay-assurance tradeoffs, at times of crisis operators will be ill-prepared and will have to depend on individual intuition and expertise. On the other hand, if the trade-offs are well understood, it will be possible to develop and validate contingency plans that can be quickly invoked or offered to human operators at times of crisis.

8.4.5 Legacy system integration

Integrating with legacy systems is a hard and inescapable reality in any realistic implementation of the Smart Grid. This poses a number of challenges to the security architecture of the Smart Grid:

- Compatibility problems when new security solutions are installed in new devices resulting in mismatched expectations that may cause the devices to fail or malfunction (an anecdotal story tells of a network scan using tools like the Network MAPper [NMAP] tripping IEDs because they do not fully implement the TCP/IP stack); and
- Backwards compatibility, which may often be a requirement (regulator, owner organization) and may prevent deployment of advanced features.

Relevant effort:

- Not just linking encryptors but conducting research in legacy systems beyond SCADA encryption; American Gas Association (AGA), AGA 12 Cryptography Working Group.

Potential avenues of investigation include:

- Compositionality (enhanced overlays, bump-in-the-wire[9], adapters) that contain and mask legacy systems; and
- Ensuring that the weakest link does not negate new architectures through formal analysis and validation of the architectural design, possibly using red team methodology.

[9] An implementation model that uses a hardware solution to implement IPSec.

8.4.6 Resiliency Management and Decision Support

Research into resiliency management and decision support will look at threat response escalation as a method to maintain system resiliency. While other Smart Grid efforts are targeted at improving the security of devices, this research focuses on the people, processes, and technology options available to detect and respond to threats that have breached those defenses in the context of the Smart Grid's advanced protection architecture. Some of the responses must be autonomic—timely response is a critical requirement for grid reliability. However, for a quick response to treat the symptom locally and effectively, the scope and extent of the impact of the failure needs to be quickly determined and mitigated. Not all responses can be autonomic, however. New research is needed to measure and identify the scope of a cyber attack and the dynamic cyber threat response options available in a way that can serve as a decision support tool for the human operators.

8.4.7 Efficient Composition of Mechanisms

It can sometimes be the case that even though individual components work well in their domains, compositions of them can fail to deliver the desired combination of attributes, or fail to deliver them efficiently. For example, a protocol in the X.509 draft standard was found to have a flaw which allowed an old session key to be accepted as new. Formal methods for cryptographic algorithm composition have helped but tend to concentrate on small, specific models of individual protocols rather than the composition of multiple algorithms as is typically the case in real implementations. In other circumstances, the composition of two useful models can cause unintended and unwanted inefficiencies. An example of this is the combination of the congestion control of TCP overlaid upon *ad hoc* mobile radio networks.

Research that systematizes the composition of communications and/or cryptographic mechanisms and which assists practitioners in avoiding performance, security, or efficiency pitfalls would greatly aid the creation and enhancement of the Smart Grid.

8.4.8 Risk Assessment and Management

A risk-based approach is a potential way to develop viable solutions to security threats and measure the effectiveness of those solutions. Applying risk-based approaches to cybersecurity in the Smart Grid context raises a number of research challenges. The following subsections describe three important ones.

8.4.8.1 Advanced Attack Analysis

While it is clear that cyber attacks or combined cyber/physical attacks pose a significant threat to the power grid, advanced tools and methodologies are needed to provide a deep analysis of cyber and cyber/physical attack vectors and consequences on the power grid. For example, answering questions such as, "Can a cyber or combined cyber/physical attack lead to a blackout such as described in 8.6.5?"

8.4.8.2 Local Privacy

Detailed management of home devices (in a HAN) has the potential to divulge private information both through cyber channels and also through physical channels. Recent work in Non Intrusive Appliance Load Monitoring (NIALM) has shown very high fidelity event reconstruction through techniques such as hidden Markov models. Signifcant threats to

individual privacy can be envisioned (in addition to the enterprise concerns in 8.6.1.1).[10] Privacy cannot be ensured through cryptographic methods, alone.

8.4.8.3 Measuring Risk

The state of the art in the risk measurement area is limited to surveys and informal analysis of critical assets and the impact of their compromise or loss of availability. Advanced tools and techniques that provide quantitative notions of risks—that is, threats, vulnerabilities, and attack consequences for current and emerging power grid systems—will allow for better protection and regulation of power systems.

8.4.8.4 Risk-based Cyber/Physical Security Investment

When cybersecurity solutions are deployed, they mitigate risks. However, it is hard to assess the extent to which risk has been mitigated. A related question is how much investment in cybersecurity is appropriate for a given entity in the electric sector? Research into advanced tools and technologies based on quantitative risk notions that take into account not only cyber risks and physical risks, but combined cyber-physical risks in which cyber/physical vulnerabilities become interdependent. These include physical attacks informed by cyber in which uncovering cyber decisions leads to knowledge of physical system vulnerabilities such as congestion. These can also include cyber attacks enhancing physical attacks or a cyber system used to cause physical harm.

8.5 Networking Topics

8.5.1 Safe use of COTS / Publicly Available Systems and Networks

Economic and other drivers push the use of COTS (commercial off-the-shelf) components, public networks like the Internet, or available Enterprise systems. Research is needed to investigate if such resources can be used in the Smart Grid reliably and safely, and how they would be implemented.

8.5.1.1 Internet Usage in Smart Grid

A specific case is the use of the existing Internet in Smart Grid–related communications, including possibly as an emergency out-of-band access infrastructure. The Internet is readily available, evolving, and inherently fault tolerant. But it is also shared, containing numerous instances of malicious malware and malicious activities. Research into methods to deal with denial of service as well as to identify other critical issues will serve our understanding of the strengths and weaknesses as well as the cautions inherent in using the existing Internet for specific types of Smart Grid applications. In particular, this is a quality of service issue; how can enough bandwidth be guaranteed to a distributed embedded application such as a smart grid. What are the effects of delays on the physical control, for example, when physical delay or computation delay cannot be easily bounded, particularly in the face of changing network topologies and state.

[10] For more on the privacy concerns related to NIALM, please see Volume 2, Section 5.3.1.

8.5.1.2 TCP/IP Security and Reliability Issues

Security/reliability issues surrounding the adoption of TCP/IP for Smart Grid networks is a related research topic separate from the subject of Internet use. Research into the adoption of Internet protocols for Smart Grid networks could include understanding the current state of security designs proposed for advanced networks. Features such as quality of service (QoS), mobility, multi-homing, broadcasting/multicasting, and other enhancements necessary for Smart Grid applications must be adequately secured and well managed if TCP/IP is to be adopted.

8.5.2 Advanced Networking

The prevalent notion is that Smart Grid communications will be primarily TCP/IP-based. Advanced networking technologies independent of the Internet protocols are being explored in multiple venues under the auspices of the National Science Foundation (NSF), Defense Advanced Research Projects Agency (DARPA), and others. Advanced networking development promises simpler approaches to networking infrastructures that solve by design some of the issues now affecting the Internet protocols. The work, although not complete, should be understood in the context of providing secure networks with fewer complexities that can be more easily managed and offer more predictable behavior.

A wide variety of communication media and protocols are currently available and being used today—leased lines, microwave links, wireless, power line communication, etc. Two substation automation protocols and protocol suites, DNP3 and IEC 61850, are in use today. Any advanced networking technology that aims to provide a uniform abstraction for Smart Grid communication must also need support these various physical, data link, and transport layers for SCADA, substation automation, and peer-to-peer communication.

8.5.3 IPv6

It is very difficult to predict the consequences of large-scale deployments of networks. As the Smart Grid will likely be based on IPv6 in the future, and it is predicted that millions of devices will be added to the Smart Grid, it is not obvious that the backbone will function flawlessly. Research is needed to ensure that the IPv6-based network will be stable, reliable, and secure.

In particular, these issues need more research—

- Will current and future protocols scale to millions of devices?
- Is current modeling, simulation, and emulation technology sufficient to model future networks using IPv6?
- How is the accuracy of projected performance validated?
- Will devices interoperate properly in multi-vendor environments?
- Are the routing protocols suitable? Do new standards need to be developed?
- Are there any security concerns? How will the network be partitioned?
- Should NAT (Network Addresses Translation) be used?
- Is a fundamentally new network architecture needed?

8.6 Other Security Issues in the Smart Grid Context

If the Smart Grid is viewed as a cyber-physical system, then the cyber cross section of the Smart Grid will look like a large federated, distributed environment where information systems from various organizations with very different characteristics and purpose will need to interoperate. Among the various interacting entities are utilities, power generators, regulating authorities, researchers, and institutions—even large industrial consumers if the likes of Google are allowed to buy electricity directly; and with the advent of home-based renewable-energy and electric vehicles, residential customers may possibly be included. Effectively securing the interfaces between environments will become an increasing challenge as users seek to extend Smart Grid capabilities. Scalable and secure interorganizational interaction is a key security and management issue. Privacy policies involving data at rest, in transit, and in use will have to be enforced within and across these environments. Research is needed in the areas discussed in the following subsections.

8.6.1 Privacy and Access Control in Federated Systems

8.6.1.1 Managed Separation of Business Entities

Research in the area of managed separation will focus on the network and systems architecture that enables effective communication among various business entities without inadvertent sharing/leaking of their trade secrets, business strategies, or operational data and activities. It is anticipated that fine-grained energy data and various other types of information will be collected (or will be available as a byproduct of interoperability) from businesses and residences to realize some of the advantages of Smart Grid technology. Research into managing the separation between business entities needs to address multiple areas:

- Techniques to specify and enforce the appropriate sharing policies among entities with various cooperative, competing, and regulatory relationships are not well understood today. Work in this area would mitigate these risks and promote confidence among the participants that they are not being illegitimately monitored by their energy service provider, regulatory bodies, or competitors. Architectural solutions will be important for this objective, but there are also possibilities for improvements, for example, by using privacy-enhancing technologies based on cryptography or work on anonymity protections.
- As they collect more information, energy service providers will need to manage large amounts of privacy-sensitive data in an efficient and responsible manner. Research on privacy policy and new storage management techniques will help to diminish risk and enhance the business value of the data collected while respecting customer concerns and regulatory requirements. Such work would contribute to improved tracking of the purpose for which data was collected and enable greater consumer discretionary control.
- Verifiable enforcement of privacy policies regardless of the current state and location of data will provide implicit or explicit trust in the Smart Grid. Research is needed to develop better mechanisms for such enforcement.

8.6.1.2 Authentication and Access Control in a Highly Dynamic Federated Environment

Collaborating autonomous systems in a federated environment must need to invoke operations on each other, other than accessing collected data (e.g., an ISO asking for more power from a plant). Access control (authentication and authorization), especially when the confederates enter into dynamic relationships such as daily buying/selling, long-term contracts, etc., is an issue that needs added research.

8.6.2 Auditing and Accountability

The concept of operation of the envisioned Smart Grid will require collecting audit data from various computer systems used in the Smart Grid. The existence of multiple autonomous federated entities makes auditing and accountability a complex problem: Who is responsible for auditing whom? How are the audit trails collected at various points to be linked? What mechanism can be used to mine the data thus collected? Such data will be needed to assess status, including evidence of intrusions and insider threats. Research is needed on a range of purposes for which audit data will be needed and on finding the best ways to assure accountability for operator action in the system. This will include research on forensic techniques to support tracing and prosecuting attackers and providing evidence to regulatory agencies without interrupting operations.

8.6.3 Infrastructure Interdependency Issues

Maintaining the resiliency and continuous availability of the power grid itself as a critical national infrastructure is an important mandate. There are also other such critical national infrastructure elements, such as telecommunications, oil and natural gas pipelines, water distribution systems, etc., with as strong a mandate for resiliency and continuous availability. However, the unique nature of the electrical grid is that it supplies key elements toward the well-being of these other critical infrastructure elements. And additionally, there are reverse dependencies emerging on Smart Grid being dependent on the continuous well-being of the telecommunications and digital computing infrastructure, as well as on the continuing flow of the raw materials to generate the power. These interdependencies are sometimes highly visible and obvious, but many remain hidden below the surface of the detailed review for each. There is little current understanding of the cascading effect outages and service interruptions might have, especially those of a malicious and judiciously placed nature with intent to cause maximum disruption and mass chaos. Research into interdependency issues would investigate and identify these dependencies and work on key concepts and plans toward mitigating the associated risks from the perspective of the Smart Grid. Such research should lead to techniques that show not only how communication failures could impact grid efficiency and reliability, how power failures could affect digital communications, and how a simultaneous combination of failures in each of the systems might impact the system as a whole, but should also apply a rigorous approach to identifying and highlighting these key interdependencies across all of these critical common infrastructure elements. The research would lead to developing and applying new system-of-systems concepts and design approaches toward mitigating the risks posed by these interdependencies on a nationwide scale.

8.6.4 Cross-Domain (Power/Electrical to Cyber/Digital) Security Event Detection, Analysis, and Response

The implication of failures or malicious activity in the cyber domain on the electrical domain, or vice versa, in the context of a large-scale and highly dynamic distributed cyber-physical system like the Smart Grid, is not well understood. Without further research, this is going to remain a dark area that carries a big risk for the operational reliability and resiliency of the power grid.

As mentioned throughout various sections of this report, there is a need to better integrate the cyber and power system view. This is especially important in regard to detecting security events such as intrusions, unauthorized accesses, misconfigurations, etc., as well as anticipating cyber and power system impacts and forming a correct and systematic response on this basis. This is driven by the goal of using the modern IT and communications technologies in the Smart Grid to enhance the reliability of the power system while not offering a risk of degrading it. This will require research into new types of risk and security models as well as methods and technologies.

There is need to further research and develop models, methods, and technologies in the following areas:

- Unified risk models that have a correlated view of cyber and power system reliability impacts;
- Response and containment models/strategies that use the above unified risk models;
- Security and reliability event detection models that use power and IT and communication system factors in a cross-correlated manner and can operate on an autonomous, highly scaled, and distributed basis (e.g., security event detection in mesh networks with resource-constrained devices, distributed and autonomous systems with periodic connectivity, or legacy component systems with closed protocols)). New security models need to be developed to overcome the limitations of purely cryptographic solutions. These models must embrace power, IT, and communications in a unifed fashion;
- Unified intrusion detection/prevention systems that use the models/methods above and have a deep contextual understanding of the Smart Grid and its various power system and operations interdependencies;
- Very large-scale wide area security event detection and response systems for the Smart Grid that can interoperate and securely share event data across organizational boundaries and allow for intelligent, systematic, and coordinated responses on a real-time or near real-time basis;
- Development of distributed IED autonomous security agents with multi-master Security Information and Event Management (SIEM) reporting for wide area situational awareness;
- Development of distributed IED autonomous security agents with continuous event and state monitoring and archiving in the event of islanding, security state restoration and forensics when isolated from master SIEM systems;
- Advanced Smart Grid integrated security and reliability analytics that provide for event and impact prediction, and continual infrastructure resiliency improvement; and

- Advanced security visual analytics for multidimensional, temporal, and geo-spatial views of real-time security data capable of digesting structured and unstructured data analysis for system and security operation control center operators.

To develop and refine the modeling and systems necessary for much of the proposed research, there would also be a need for developing new simulation capabilities for the distribution grid that incorporate communications with devices/models for distribution control, distributed generation, storage, PEV, etc., to provide a representative environment for evaluating the impact of various events. To provide a realistic assessment of impact, the simulation capabilities should be similar in fidelity to the transmission grid simulation capabilities that currently exist. However, both the distribution and transmission grid system simulations need to be further developed to integrate cyber elements and evaluate their possible cross-impacts on each other.

8.6.5 Covert network channels in the Smart Grid: Creation, Characterization, Detection and Elimination

The idea of covert channels was introduced by Lampson in 1973 as an attack concept that allows for secret transfer of information over unauthorized channels. These channels demonstrate the notion that strong security models and encryption/authentication techniques are not sufficient for protection of information and systems. Earlier research on covert channels focused on multilevel, secure systems but more recently a greater emphasis has been placed on "covert network channels" that involve network channels and can exist in discretionary access control systems and Internet-like distributed networks. Given that many Smart Grid networks are being designed with Internet principles and technologies in mind, the study of covert network channels for the Smart Grid becomes an interesting research problem. Like the more general covert channels, covert network channels are typically classified into storage and timing channels. Storage channels involve the direct/indirect writing of object values by the sender and the direct/indirect reading of the object values by the receiver. Timing channels involve the sender signaling information by modulating the use of resources (e.g., CPU usage) over time such that the receiver can observe it and decode the information.

The concern over covert network channels stems from the threat of miscreants using such channels for communication of sensitive information and coordination of attacks. Adversaries will first compromise computer systems in the target organization and then establish covert network channels. Typically, such channels are bandwidth-constrained as they aim to remain undetected. Sensitive information that may be sent over such channels include Critical Energy Infrastructure Information (CEII), FERC 889 involving the leakage of operational information to power marketing entities, and cryptographic keying material that protects information and systems. In addition, information exchange for coordination of attacks such as management and coordination of botnets, and spreading worms and viruses are also important concerns.

For example, covert network channels have been created using IP communication systems by a variety of means including the use of unused header bits, modulating packet lengths, and modifying packets rates/timings. Similarly, such channels have been shown to be possible with routing protocols, wireless LAN technologies, and HTTP and DNS protocols. For the Smart Grid, an interesting research challenge is to identify new types of covert network channels that may be created. For example, given that the Smart Grid involves an extensive cyber-physical infrastructure, perhaps the physical infrastructure can be leveraged to design covert network channels. Additional challenges include identification of other covert network channels that can

be established on Smart Grid networks, for example, using relevant weaknesses in Smart Grid protocols. For all created channels, it is important to characterize the channels. This includes estimating channel capacity and noise ratios.

Covert channels can be detected at the design/specification level and also while they are being exploited. A variety of formal methods-based techniques have been developed in the past. An example is those based on information flow analysis. For runtime identification, several techniques specific to the type of covert network channel have been developed. Research challenges include identification of covert network channels for Smart Grid systems both at the design level and while they may be exploited. Once identified, the next challenge lies in eliminating them, limiting their capacity, and being able to observe them for potential exploitation. Means for doing so include the use of host and network security measures, and traffic normalization at hosts and network endpoints, such as firewalls or proxies. Again, research challenges include developing means for eliminating covert network channels, and in a case where that is not feasible, the objective is to limit their capacity and be able to monitor their use. Potential avenues of research include analyzing and modifying garbage collection processes in Smart Grid systems, and developing signature and anomaly-based detection techniques.

Covert channels are not limited to network observations. The power system itself, in a cyber-physical environment, provides covert channel information. Power line changes resulting from cyber actions on smart devices divulge those cyber actions.

8.6.6 Denial of Service Resiliency

8.6.6.1 Overview

Smart Grid communications are progressing toward utilizing IP-based transport protocols for energy utility information and operational services. As IP-based nodes propagate, more opportunities for exploitation by miscreants are evolving. If a network component can be probed and profiled as part of the Smart Grid or other critical infrastructures, it is most likely to be targeted for some form of intrusion by miscreants. This is especially relevant with the growing use of wireless IP communications.

8.6.6.2 DoS/DDoS Attacks

Denial of Service and Distributed Denial of Service (DoS/DDoS) attacks have become an effective tool to take advantage of vulnerabilities. The attack objective is to take actions that deprive authorized individuals access to a system, its resources, information stored thereon, or the network to which it is connected.

A simple DoS attack attempts to consume resources in a specific application, operating system, or specific protocols or services, or a particular vendor's implementation of any of these targets to deny access by legitimate users. It may also be used in conjunction with other actions (attacks) to gain unauthorized access to a system, resources, information, or network.

The DDoS attack seeks to deplete resource capacity, such as bandwidth or processing power, in order to deny access to authorized users and can be levied against the infrastructure layer or the application layer. This technique utilizes a network of attack agents (a "botnet" comprised of systems that have had attack software installed surreptitiously) to amass a large, simultaneous

assault of messages on the target. As with the DoS attack, DDoS may be combined with other techniques for malicious purposes.

IP-based networks are vulnerable to other attacks due to deficiencies of underlying protocols and applications. A man-in-the-middle, session-based hijack, or other technique may accompany the DoS/DDoS attack to inflict further damage on the target. Wireless networks in the AMI/HAN environment can be difficult to secure and are of particular concern as the object of an attack or an entry point to the upstream network and systems.

8.6.6.3 Research and Development Requirements

The SGIP CSWG R&D subgroup desires to highlight and seek further research and development support in order to improve DoS/DDoS resiliency. We have identified the following areas of work as offering potential solutions worthy of further pursuit by Smart Grid stakeholders:

1. **Network architectures for survivability:** The Smart Grid networks and the public Internet will have several interface points which might be the target of DoS/DDoS attacks originating from the public Internet. A survivable Smart Grid network will minimize the disruption to Smart Grid communications, even when publicly addressable interfaces are subject to DDoS attacks;

2. **Policy-based routing and capabilities:** Policy-based routing is a fundamental redesign of routing with the goal of allowing communications if, and only if, all participants (source, receiver, and intermediaries) approve. A particular policy of interest for defending against DDoS attacks is the use of Capabilities. In this framework, senders must obtain explicit authorization (a capability) from the receiver before they are allowed to send significant amounts of traffic (enforced by the routing infrastructure). Smart Grid networks provide a good opportunity to design from the ground up a new routing infrastructure supporting capabilities;

3. **Stateless dynamic packet filtering:** Filtering and rate-limiting are basic defenses against DDoS attacks. We require further research in stateless packet filtering techniques to significantly reduce packet-processing overhead.

   An example of this is “Identity-Based Privacy-Protected Access Control Filter” (IPACF) which is advertised as having the “capability to resist massive denial of service attacks.” IPACF shows promise for using “stateless, anonymous and dynamic” packet filtering techniques without IP/MAC address, authentication header (AH) and cookie authentication dependencies, especially for resource-constrained devices (RCDs).

   When compared to stateful filtering methods, IPACF may significantly reduce packet processing overhead and latencies even though it is dynamically applied to each packet. IPACF describes the ability to utilize discarded packets for real-time intrusion detection (ID) and forensics without false positives.

   Initial modeling reveals that embedded stateless packet filtering techniques may significantly mitigate DoS/DDoS and intrusion and could be evolved to defend man-in-the-middle attacks, while offering considerable device implementation options and economies of scale; and

4. **Lightweight authentication and authorization:** There is a distinct need for an embedded-level, lightweight, secure, and efficient authentication and authorization (AA)

protocol to mitigate intrusion and DDoS attacks targeting resource-intense AA mechanisms. See Item 3 above.

5. **Power system DDoS:** The smart grid elements, themselves, can initiate denial of service by advertising energy that they do not possess or creating demand that does not exist (fake supply or fake demand attacks). . This can deplete stored energy or cause shortages in reactive power during periods of high demand and can have the potential to destabilize the grid.

8.6.7 Cloud Security

With the advent of cloud computing in the Smart Grid, special attention should be given to the use of cloud computing resources and the implications of leveraging those resources. There are several organizations that are focusing on security and appropriate use of cloud computing resources, including the Cloud Security Alliance. They have produced a document that addresses security areas for cloud computing that provides valuable guidelines to security in this environment. Work has also been done by NIST's cloud computing group that provides some guidelines for cloud computing use in government agencies.

As with any shared resource that will host potentially sensitive information, security mechanisms must be deployed that provide the appropriate protection and auditing capabilities throughout the cloud. Cloud computing must be evaluated with consideration of the unique constraints and consequences of control systems in the context of the Smart Grid. Impact of cloud provider engagement must also be considered in terms of liabilities for data existing in the cloud, in what is likely to be a multi-tenancy environment.

Data security issues must be addressed such as data ownership, data protection both in and out of the cloud for storage and transit, access control to the data and the cloud, and authorization considerations for trust and permissions. Trust models must be put in place to provide these guarantees in a manner that is verifiable and compliant with emerging regulations like NERC CIPs, FERC 889, user data privacy concerns, and other emerging compliance regulations. These types of regulations may have corollaries in industries like the health sector that could be considered, but differ enough that there are unique concerns.

WAN security and optimization issues must also be addressed depending on the data access patterns and flow of information in the cloud. This could include new work in encryption, key management, data storage, and availability model views. For instance, securely moving synchrophasor data from end nodes into the cloud on a global basis could be overly resource intensive. This might make real-time use infeasible with current cloud computing technology without further research in this area. Current distributed file system approaches may not be appropriately optimized to operate in a secure WAN environment, favoring network-expensive replication in a LAN environment as a trade-off for speed.

8.6.8 Security Design & Verification Tools (SD&VT)

Complexity breeds security risks. This is most evident with the Smart Grid, as it is a collection of many complex, interconnected systems and networks that represent a fusion of IT, telecommunications, and power system domains. Each of these domains represents distinct forms of technology and operations that have unique interdependencies on each other and can

indeed lead to elements of the cyber system (i.e., IT and communications) impacting the reliability of elements of the power system and vice-versa.

Correctly designing security for each of the domains is primarily done from the perspective of only the power or cyber domain. For example, designing certain security controls (without an adequate understanding of an overall power system context) to prevent excessive failed authentication attempts by lockout on a communication/control device might in fact create a denial of service condition that is more likely to degrade the reliability of the broader system than mitigate the original security risk that one was trying to address. System-wide security design and implementation is not commonly done using formal methods that can be verified, nor can it give any deterministic analysis of expected performance or behavior for given system states, faults, or threat events.

Research and development should be conducted into SD&VT that can—

a. Formally model Smart Grid cyber and power systems, their interactions, and their underlying components using a formal language. Candidates for examination and further adaptation can include: SysML, Formal ontologies and knowledge representation based on semantic Web technologies such as OWL, or other novel forms. The language should allow one to communicate certain assertions about the expected function of a device/system and its security controls and risks, as well as the relationship between components, systems, and system communication. Most importantly, the model must provide a basis to represent multiple concurrent and independently interacting complex processes with distributed system states;

b. Provide automatic, intelligent methods of verification that discover reliability and security issues in component and system states for the Smart Grid, in a formal design model (as represented using the methods in (a.) using any number of machine learning or knowledge/logic inference techniques; and

c. Simulate any number of scenarios based on the intelligent model built using (a.) and (b.), and provide predictive analytics that can optimize a security design that minimizes risks and costs, as well as maximizing security and reliability in the power and cyber domain.

8.6.9 Distributed versus Centralized Security

Several models for designing intelligent and autonomous actions have been advanced for the Smart Grid, particularly in automated distribution management. Several models have also been deployed in the advanced metering space, where, for example, there is ongoing debate regarding the functions and processing which should be carried out by the meter, versus centralized systems (such as Meter Data Management or Load Control applications in the Control Center). Some approaches offer embedded security controls, while some externalize security and some offer combinations of both approaches. In the larger context of advanced distribution automation, there is a similar debate regarding how much “intelligence” should be deployed within IEDs, distributed generation endpoints, etc., versus reliance on centralized systems.

Also, Wide Area Situational Awareness (WASA) systems and actors are distributed by nature, yet most security mechanisms in place today are centralized. What is an appropriate security mechanism to place in a distributed environment that will not compromise an existing security framework, yet allow third-party WASA systems and actor’s visibility into security intelligence,

as well as allow appropriate functional capability to act and respond to distributed security events?

We propose advanced security research be conducted to determine an underlying security model to support these various approaches to distributed versus centralized security intelligence and functionality in the grid. Some factors to consider include the following:

- Communication with centralized security mechanisms may be interrupted. Research should be conducted into hybrid approaches and the appropriate layering of security controls between centralized and distributed systems. For example, centralized security mechanisms may be supplemented with local "break glass" security mechanisms for many devices, but does this "local" control support a distributed model?
- Externalized security mechanisms, such as in some control system protocol implementations (e.g., ANSI C12.22), may be desirable because they can be scaled and upgraded independently in response to evolving threats and technology changes, possibly without retrofitting or upgrading (perhaps millions of) devices deployed in the field. On the other hand, some mechanisms should be deployed locally, such as bootstrap trusted code verification modules for firmware, logging, etc. Research should be conducted in best practices to determine the appropriate model for deployment.
- Rapid changes of cryptographic keys and authentication credentials may be needed to contain security incidents or provide ongoing assurance, and centralized security systems may be needed. Would a distributed or centralized model be more efficient and secure?
- Functionality of some components (e.g., breakers, IEDs, relays, etc.) and communications functions should not fail due to failure of a security mechanism. Is a distributed model appropriate for WASA?
- Integration of security mechanisms between security domains is needed (for example, between logical and physical security mechanisms of remote sensors). How does a distributed vs. centralized model effect the integration?
- Edge devices such as distributed generation controllers and substation gateways need to be capable of autonomous action (e.g., self-healing), but these actions should be governed by business rules and under certain circumstances data from the devices should not be trusted by decision support systems and systems that have more than local control of the grid. Does a distributed model manage edge devices more efficiently and securely than a centralized model?
- A trust model is needed to govern autonomous actions, especially by systems outside the physical control of the utility. Will there be a centralized trust model or will the industry evolve to a distributed trust model allowing numerous Smart Grid actors to interact trustfully in regards to security interactions?
- Do distributed or centralized trust models force over-reliance by control systems support groups on IT groups?
- What are the actions to be taken during a security event; are they centralized or distributed?

While it is not be clear which security functions should be centralized or decentralized for a particular implementation, research into coherent reference models and taxonomies for layering these controls following best practice should be conducted. The model should contain a standard approach by which Smart Grid actors can make better security architecture decisions based on risks to their environment and efficiencies of security operations.

8.6.10 System Segmentation and Virtualization

The first principles of cybersecurity are isolation and defense-in-depth. The objective of this research is to develop methods to protect network end-points through Intense System Segmentation. The research should seek to create a platform that implements the characteristics of time-tested and recognized security principles. These principles include isolation, a minimal trusted computing base, high usability and user transparency, a limited privilege capability that provides for user, process, and application class of service definitions, and a default-deny rules engine enforcing such privileges.

The requirement for continuous availability of Utility Grid operations necessitates a high degree of reliability within and across domains. Many domain end-points, such as legacy substation equipment, rely on outdated operating systems with little or no encryption capabilities, posing numerous challenges to the overall security of the Smart Grid. By enclosing an Intense System Segmentation framework around the existing computer architecture of these localized end-points, the legacy infrastructure should gain a layer of redundancy and security. Intense System Segmentation within a single Virtual Machine (VM) should provide granular isolation to reduce the attack surface to a single file and/or single application, and reduce the ability of threats to virally propagate. End-point protection must also be customizable to address the specific needs of subsectors within individual Energy Sector Domains.

Traditional virtualization techniques that use sandboxing have known, exploitable vulnerabilities. This is largely the result of the communication that traditional VMs require in order to perform sharing functions between applications and administrative requirements. Sandboxing also relies on binary decisions for processes and communication that might compromise security. Intense System Segmentation should allow communication between isolated environments to occur while eliminating any execution of code outside of an isolated environment. An Intense System Segmentation platform may use some of the tools of virtualization, such as a sealed hypervisor to provide protection of end-point resources, and sealed VMs to perform computing in intense isolation. Hypervisors are designed to streamline communication between a wide range of applications and processes, and utilize APIs and other communication entry points. A sealed hypervisor should block these communication entry points, for both the hypervisor and an attestable kernel.

Maintaining the resiliency and continuous availability of the power grid should be one of the primary goals in creating a system segmentation platform. As this platform assumes that end-points will be penetrated, secure recovery, containment, and resiliency should be a focus of continued research. The inherent redundancy of hypervisor-driven segmentation can be utilized to enclose legacy systems and should allow customizable interoperability between the DHS-defined critical infrastructure sectors. An open platform that uses a secure computing architecture and leverages the tools of virtualization will enhance the resiliency of existing Energy Sector critical infrastructure. The use of virtualization has also been recognized as building block to implement resiliency through agility (a “moving target” paradigm). This can be

used to increase uncertainty and cost to attackers. Thus this research should help to leverage "moving target" paradigm in Smart Grid systems as well as improving security of Smart Grid legacy systems.

8.6.11 Vulnerability Research

Vulnerabilities may be caused by many things in computer devices. Poor coding is the primary cause of vulnerabilities in computer systems today, but physical attacks have much higher value in Smart Grid devices than in standard computing environments. Both design and implementation vulnerabilities represent varying and potentially great risks to the power grid. While future code revisions and hardware versions may introduce new vulnerabilities, many vulnerabilities may exist in the current systems that require significant time to identify and address. For many years, SCADA systems have been quarantined from security scans for fear of causing outages. While care and prudence should be taken with critical systems, the fragility of these systems represents a great existing risk to the grid. Newer Smart Grid systems such as advanced metering infrastructure, hybrid/electric vehicles and supporting infrastructure, and demand response all represent new unknowns. A few significant projects have undertaken security research on some of these devices, and positive results have resulted but more research is necessary. Security research grants are key to ensuring greater scrutiny of the existing systems to find vulnerabilities that may currently exist in Smart Grid equipment.

8.6.12 Vulnerability Research Tools

Smart Grid networks represent a great deal of proprietary, obtuse systems and protocols. Before security can be reasonably well tested, tools must be created to maximize the value of security research. Several freely available tools have already been in active development but lack resources. Other tools are important but nonexistent.

Examples of existing security research tools include:

- GoodFET—Hardware analysis tool allowing debugging of numerous platforms/chipsets, largely focused on the predictability of power-glitching to bypass hardware security mechanisms; http://goodfet.sourceforge.net/
- KillerBee—ZigBee® analysis tool allowing for capture and analysis of ZigBee® networks and interaction with devices.

Examples of security research tools yet to be started:

- Devices to easily interact with, capture, and analyze traffic of metering networks for different vendors. Currently, the best toolset available is the software-defined radio named USRP2 from Ettus Research, costing roughly $2k. This toolset allows for RF analysis and indeed can capture data bits. However, the ideal toolset would allow an analyst's computer to interface to the metering networks and provide an appropriate network stack in a popular operating system such as Linux. The tools would allow the customers (mostly IOU's due to funding) to perform their own security research against the platforms, and allow them to validate their own security;
- Open-source Protocol analysis tools, such as the protocol parsers included in the open-source tool Wireshark. Protocols like IEC61850, IEC61968/ANSI C12.*, proprietary AMI protocols, DNP3, Modbus, and other popular power grid protocols being included

in the Smart Grid should be freely available for analysis by asset-owners and researchers; and

- Firmware analysis tools that can be configured to understand address/IO mapping and input vectors, and can identify potential vulnerabilities for a given platform.

8.6.13 Data Provenance

We cannot assume that the Smart Grid will never be compromised. Once we assume that there are insiders who have access, operational data can no longer be trusted. In addition, while traditional security-related protocols reject data if the security fails, we cannot afford to ignore operational data because the data is suspect.

Therefore, we need methods to deal with such data while maintaining the operational integrity and state of many systems. Some of the issues include:

- Measuring the quality of the data from a security perspective. This may include both subjective and objective viewpoints, and may have to deal with uncertainty about the data.
- How do we make operational decisions based on data that may have questionable attributes of confidentiality, integrity, authenticity, non-repudiation, and timeliness?
- How do organizations coordinate their beliefs with other organizations? What happens if the other organizations are suffering from a significant security breach? How should one organization react with data of uncertain trustworthiness?

8.6.14 Security and Usability

One of the issues with the implementation of security is the usability of security, or the ease of use and impact on convenience. Some organizations weaken their security for various reasons (e.g., operational cost, profit, effort, lack of understanding). To encourage users to deploy strong security, certain issues must be overcome. These include:

- Security must be self-configuring. That is, the systems should be able to configure themselves to maximize security without requiring expert knowledge of security.
- Security options should be simple and understandable by users who lack a background in security. Concepts like certificates and keys are not well understood by end users. These details should be hidden.
- The relationship between a security policy, the protection the policy provides, and the security configuration should be clear. If a system is “misconfigured” in a way that reduces the protection, the risk should be clear to the user.
- Security should be reconfigured. In other words, if a policy is changed (for instance, stronger security is enabled), the systems should adapt to meet the new requirements. It should not be necessary to physically visit devices to reconfigure them. However, if policy changes, some devices might be unable to change, and end up being isolated from the new configuration. How can the user minimize the disruption?
- Part of usability is maintainability. There needs to be ways to upgrade security without replacing equipment. Firmware upgrades are often proprietary, vendor-specific, and have

uncertain security. How can a vendor best plan their migration strategy between security revisions and major policy changes?

Usability of security technologies needs to improve to address these issues.

8.6.15 Cyber Security Issues for Electric Vehicles

PEVs have a similar entry point to the electric grid as the smart meters. Thus, they are associated with largely the same security and privacy issues. When PEVs connect to the grid to charge their batteries, it is necessary to communicate across a digital network to interface with a payment and settlement system. Assuming that proper standards are adopted, these charging solutions will have the same issues as payment and settlement systems for other products. Appropriate physical security measures and tamper-evident mechanisms must be developed to prevent or detect the insertion of "cloning" devices to capture customer information and electric use debit and credit information. One may expect that miscreants will develop means to clone legitimate PEV interfaces for criminal activity.

It has been reported that a terminated employee from a car dealership logged into the company's Web-based system and was able to remotely wreak havoc on more than 100 vehicles. The dealership's system was able to disable the starter system and trigger incessant horn honking for customers that have fallen behind on car payments as an alternative to repossessing the vehicle. It is necessary to develop mechanisms that make sure car buyers are properly informed and fully protected.

Like other areas that depend on a supply chain, PEVs have similar issues. Thus, it is necessary to make sure that car repair shops will not be able to install illegal devices at time of car maintenance.

Utilities and private/public charging stations may also be subject to law enforcement search warrants and subpoenas in regards to PEV usage. A PEV may be stolen and used in the act of a crime. Law enforcement may issue an "alert" to control areas to determine if the suspected PEV is "connected" to the grid and would want to know where and when. Research may also be requested by law enforcement to enable a utility to be able to "disable" a PEV in order to preserve evidence and apprehend the criminals. Authentication and non-repudiation are key in this process, otherwise a theif can use the same processes to steal a car (or disable cars as in the example, above).

8.6.16 Detecting Anomalous Behavior Using Modeling

Various sensors in the power/electrical domain already collect a wide array of data from the grid. In the Smart Grid, there will also be a number of sensors in the cyber domain that will provide data about the computing elements as well as about the electrical elements. In addition to naturally occurring noise, some of the sensor data may report effects of malicious cyber activity and "misinformation" fed by an adversary.

Reliable operation of the Smart Grid depends on timely and accurate detection of outliers and anomalous events. Power grid operations will need sophisticated outlier detection techniques that enable the collection of high integrity data in the presence of errors in data collection.

Research in this area will explore developing normative models of steady state operation of the grid and probabilistic models of faulty operation of sensors. Smart Grid operators can be

misguided by intruders who alter readings systematically, possibly with full knowledge of outlier detection strategies being used. Ways of detecting and coping with errors and faults in the power grid need to be reviewed and studied in a model that includes such systematic malicious manipulation. Research should reveal the limits of existing techniques and provide better understanding of assumptions and new strategies to complement or replace existing ones.

Some example areas where modeling research could lead to development of new sensors include:

- Connection/disconnection information reported by meters may identify an unauthorized disconnect, which in the context of appropriate domain knowledge can be used to determine root cause. This research would develop methods to determine when the number of unauthorized disconnects should be addressed by additional remediation actions to protect the overall AMI communications infrastructure, as well as other distribution operations (DR events, etc.).
- Information about meters running backwards could generally be used for theft detection (for those customers not subscribed to net metering). This research would identify thresholds where too many unauthorized occurrences would initiate contingency operations to protect the distribution grid.

Related prior work includes fraud detection algorithms and models that are being used in the credit card transactions.

CHAPTER 9
OVERVIEW OF THE STANDARDS REVIEW

9.1 OBJECTIVE

The objective of the standards review is to ensure that all standards applicable to the Smart Grid adequately address the cybersecurity requirements included in this report. If the standards do not have adequate coverage, this review will identify those where changes may need to be made or where other standards may need to be applied to provide sufficient coverage in that area. If the standard passes the Smart Grid Cybersecurity Committee (SGCC) cybersecurity assessment, then it may be included in the SGIP Catalog of Standards.

The SGCC works with the SGIP and the standards bodies to identify the standards for review and to gain appropriate access to the standards. This is an ongoing effort as there are many standards that apply and must be assessed. To undertake the process, the CSWG/SGCC established a standards subgroup to perform the assessments. This CSWG/SGCC Standards Subgroup developed a review process and an assessment template for performing the assessments.

9.2 REVIEW PROCESS

9.2.1 Overview

This document contains a catalog of cybersecurity requirements that can be used as a checklist for determining what types of cybersecurity requirements are applicable to specific Smart Grid interactions and cybersecurity requirement families that should be considered in the review document. (*see* Volume 1, Chapter 3.)

9.2.2 CSWG/SGCC Review Process

Before the SGCC compares the standards document against this document, the SGCC reviews the scope of the standard and documents additional assumptions as to whether cybersecurity should be part of the standards document. The cybersecurity content can take the form of detailed cybersecurity technologies, specific cybersecurity requirements to meet specific cybersecurity goals, general cybersecurity best practices, or high-level policy statements. This cybersecurity content can also cover reliability/availability requirements, confidentiality requirements, data integrity requirements, and privacy issues.

Some of these requirements are general, such as having policies and procedures for specific types of interactions, for example “SG.CM-1: Configuration Management Policy and Procedures.”[11] Some are more specific, such as “SG.SC-12: Use of Validated Cryptography.”[12] In using this catalog as a checklist, it is clear that most interactions only need or reflect a small set of these requirements, such as:

- "Access to the mapping database for updates must use authentication - SG.CM-3: Configuration Change Control”

[11] *See* Volume 1, §3.11.
[12] *See* Volume 1, §3.24.

- "Cryptographic algorithms shall be current, publicly vetted, and government approved - SG.SC-11: Cryptographic Key Establishment and Management".

9.2.3 Step 1: Reviewing the Document Scope

When the SGCC receives a request to review a document, the SGCC reviews the scope and purpose of the requested review document, and notes any assumptions as to the domain and type of document. If the document should or does contain cybersecurity requirements, then the document is assessed for cybersecurity completeness and correctness. The SGCC Standards Subgroup usually requests an expert on the document to participate and answer questions on the context or purpose of cybersecurity items.

9.2.4 Step 2: NISTIR 7628 High Level Cybersecurity Requirements

After assessing the overall scope of the document, the SGCC starts a detailed review of the cybersecurity contents of the document, assessing them against the High-Level Security Requirements from the NISTIR 7628. (See Volume 1, Chapter 3) During this assessment, some requirements and interactions may not have direct correlations with the NISTIR 7628 high-level cybersecurity requirements. This will lead to a potential recommendation of:

- The NISTIR 7628 high-level cybersecurity requirements may need to be updated to include them, or the requirement may be so specific that the requirements is not needed in the NISTIR 7628.
- If there is a NISTIR 7628 cybersecurity family that is not referenced within the review document and the cybersecurity family can apply to the review document, then a gap is documented by the SGCC and a potential recommendation is documented for the review document.

9.2.5 Step 3: Recommendations on Standard

During the assessment, cybersecurity concerns or issues are noted and often discussed with the owners of the document. Recommendations for improvement on cybersecurity issues are provided so that the document owners may choose to update the document or underake additional documents to address these recommendations.

If the standard meets all major requirements, the SGCC recommends inclusion in the SGIP Catalog of Standards. If some requirements are not met, the SGCC may recommend conditional approval pending the correction or mitigation of the cybersecurity concern.

9.3 SGCC Standards Assessment Concepts

The following provides the background and concepts used in assessing standards:

9.3.1 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

First, communication standards for the Smart Grid are designed to meet many different requirements at many different "layers" in the reference model. Two commonly used reference

models are the International Organization for Standardization (ISO) / Open Systems Interconnection model (OSI) 7-layer reference model[13] and the GridWise Architecture Council (GWAC) Stack[14] (see Figure 9-1), where the OSI 7-layer model maps to the Technical levels of the GWAC Stack. Some standards address the lower layers of the reference models, such as wireless media, fiber optic cables, and power line carrier. Others address the "transport" layers for getting messages from one location to another. Still others cover the "application" layers, the semantic structures of the information as it is transmitted between software applications. In addition, there are communication standards that are strictly abstract models of information – the relationships of pieces of information with each other. Cybersecurity is a cross-cutting issue and should be reflected in requirements at all levels: cybersecurity policies and procedures mainly cover the GWAC Stack Organizational and Informational levels, while cybersecurity technologies generally address those requirements at the Technical level.

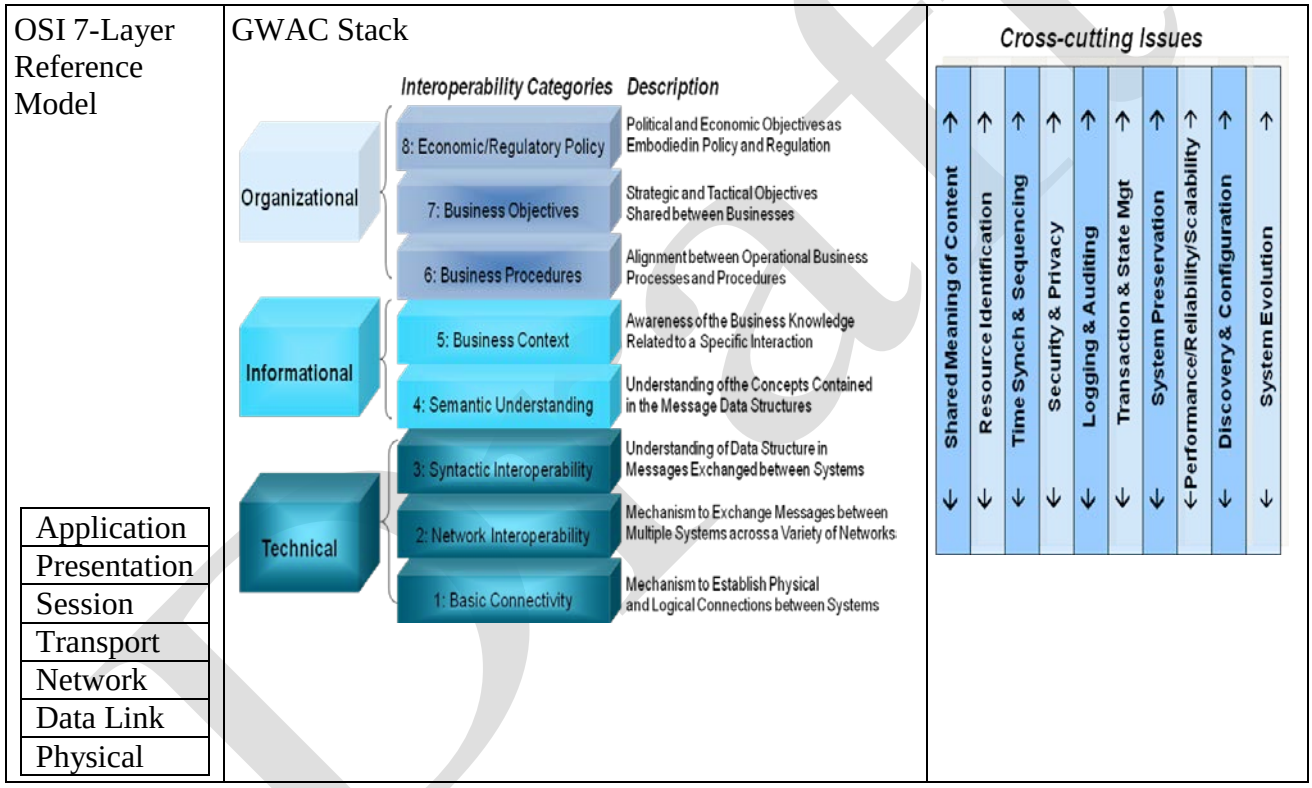


Figure 9-1 ISO/OSI 7-Layer Reference Model and GWAC Stack Reference Model

Second, regardless of what communications standards are used, cybersecurity must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. In addition, cybersecurity must address those aspects outside of the communications system in the upper GWAC Stack layers that may be functional requirements or may rely on procedures rather than technologies, such as authenticating the users and software applications, and screening

[13] ISO 7498-1:1994, Information technology-Open Systems Interconnection-Basic Reference Model: The Basic Model.

[14] The GWAC Stack is available at http://www.gridwiseac.org/ in the *GridWise Interoperability Context-Setting Framework*.

personnel. Cybersecurity must also address how to cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis.

Third, the cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself - how and where a standard is used must establish the levels and types of cybersecurity needed. Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data. Standards related to the upper layers of the GWAC Stack may address issues of data importance.

Fourth, some standards do not mandate their provisions using "shall" statements, but rather use statements such as "should," "may," or "could." Some standards also define their provisions as being "normative" or "informative." Normative provisions often are expressed with "shall" statements. Various standards organizations use different terms (e.g., standard, guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the "shall," "should," "may," and/or "could" statements, "normative," or "informative" language with which they are expressed.

Therefore, cybersecurity must be viewed as a stack or "profile" of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of policy, procedural, and communication standards designed to provide specific services. Ultimately cybersecurity, as applied to the information exchange standards, should be described as profiles of technologies and procedures which can include both "power system" methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cybersecurity technologies. For instance, if Transmission Control Protocol (TCP)/Internet Protocol (IP) is being used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then transport layer security (TLS) should be used.

In the following discussions of information exchange standard being reviewed, these caveats should be taken into account.

9.3.2 Correlation of Cybersecurity Requirements with Physical Security Requirements

Correlating cybersecurity requirements with specific physical security requirements is very complex since they generally address very different aspects of a system. Although both cyber and physical security requirements seek to prevent or deter deliberate or inadvertent attackers from accessing a protected facility, resource, or information, physical security solutions and procedures are vastly different from cybersecurity solutions and procedures, and involve very different expertise. Each may be used to help protect the other, while compromises of one can definitely compromise the other.

Physical and environmental security that encompasses protection of physical assets from damage is addressed by the NISTIR 7628 only at a high level. Therefore, assessments of standards that cover these non-cyber issues must necessarily also be at a general level.

9.3.3 Standardization Cycles of Information Exchange Standards

Information exchange standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as "appropriate security technologies and procedures should be implemented."

With the advent of the Smart Grid, cybersecurity has become increasingly important within the utility sector. However, since the development cycles of communication standards and cybersecurity standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references can be added, as appropriate.

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

9.3.4 References and Terminology

References to NISTIR 7628 security requirements refer to Volume 1, Chapter 3, High-Level Security Requirements, of this document.

References to "government-approved cryptography" refer to the list of approved cryptography suites identified in Volume 1, Chapter 4, Cryptography and Key Management, of this document. Summary tables of the approved cryptography suites are provided in Volume 1, §4.3.2.

The terms "approved", "acceptable", and "deprecated" are defined as the following:[15]

- Approved is used to mean that an algorithm is specified in a FIPS or NIST Recommendation (published as a NIST Special Publication).
- Acceptable is used to mean that the algorithm and key length is safe to use; no security risk is currently known.
- Deprecated means that the use of the algorithm and key length is allowed, but the user must accept some risk. The term is used when discussing the key lengths or algorithms that may be used to apply cryptographic protection to data (e.g., encrypting or generating a digital signature).

As noted, standards have different degrees for expressing requirements, and the security requirements must match these degrees. For these standards assessments, the following terminology is used to express these different degrees[16]:

[15] The definitions are obtained from NIST Special Publication 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.

- Requirements are expressed by "…shall…," which indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (shall equals is required to).
- Recommendations are expressed by "…should…," which indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (should equals is recommended that).
- Permitted or allowed items are expressed by "…may…," which is used to indicate a course of action permissible within the limits of the standard (may equals is permitted to).
- Ability to carry out an action is expressed by "…can …," which is used for statements of possibility and capability, whether material, physical, or causal (can equals is able to).
- The use of the word must is deprecated, and should not be used in these standards to define mandatory requirements. The word must is only used to describe unavoidable situations (e.g. "All traffic in this lane must turn right at the next intersection.")

9.4 SGCC Standards Assessment Template

The following subsections present the standards assessment template, including the template structure and questions, used by the Standards Subgroup to report findings from their standards review effort.

9.4.1 Description of Document

9.4.2 Assumptions

9.4.3 Assessment of Cybersecurity Content

9.4.3.1 Does the standard address cybersecurity? If not, should it?

9.4.3.2 What aspects of cybersecurity does the standard address and how well (correctly) does it do so?

Table 9-1: Correlations between Standard being Assessed and the NISTIR Security Requirements

Reference in Standard	Applicable NISTIR 7628 High Level Security Requirements	Comments including how NISTIR HLR Requirements Are or Are Not Completely Met

9.4.3.3 What aspects of cybersecurity does the standard not address? Which of these aspects should it address? Which should be handled by other means?

[16] The first clause of each terminology definition comes from the International Electrotechnical Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after "which") comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

9.4.3.4 What work, if any, is being done currently or is planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

9.4.3.5 Recommendations

The SGCC recommends {specific recommendations from the SGCC on the standard}

9.4.3.6 List any references to other standards and whether they are normative or informative

9.5 STANDARDS REVIEW LIST

The standards reviewed by the SGCC, if so recommended, are included in the SGIP Catalog of Standards after completing the full SGIP approval process.

CHAPTER 10
KEY POWER SYSTEM USE CASES FOR SECURITY REQUIREMENTS

The focus of this chapter is to identify the key Use Cases that are "architecturally significant" with respect to security requirements for the Smart Grid. This identification is neither exhaustive nor complete. New Use Cases may be added to this appendix in future versions of this report as they become available. The Use Cases presented in this appendix will be employed in evaluating Smart Grid characteristics and associated cybersecurity objectives; the high-level requirements of confidentiality, integrity, and availability, (CI&A); and stakeholder concerns. The focus here is more on operational functions rather than "back office" or corporate functions, since it is the automation and control aspects of power system management that are relatively unique and certainly stretch the security risk assessment, security controls, and security management limits.

Many interfaces and "environments"—with constraints and sensitive aspects—make up the information infrastructure that monitors and controls the power system infrastructure. This chapter does not directly capture those distinctions, but leaves it up to the implementers of security measures to take those factors into account.

10.1 USE CASE SOURCE MATERIAL

The Use Cases listed in this chapter were derived "as-is" from a number of sources and put into a common format for evaluation. The resulting list presented in this appendix does not constitute a catalog of recommended or mandatory Use Cases, nor are the listed Use Cases intended for architecting systems or identifying all the potential scenarios that may exist. The full set of Use Cases presented in this chapter was derived from the following sources:

- **IntelliGrid Use Cases**: Over 700 Use Cases are provided by this source, but only the power system operations Use Cases and Demand Response (DR) or Advanced Metering Infrastructure (AMI) cases are of particular interest for security. The Electric Power Research Institute (EPRI) IntelliGrid project developed the complete list of Use Cases. *See* IntelliGrid Web site, Complete List of Power System Functions.

- **AMI Business Functions**: Use Cases were originally extracted from Appendix B of the Advanced Metering Infrastructure Security (AMI-SEC) System Security Requirements document (published by the AMI-SEC Task Force) by the Transmission and Distribution Domain Expert Working Group (T&D DEWG), and the Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee (SGIP-SGCC) has now also posted this material on the SGIP TWiki).

  Before the revision of this document, the CSWG/SGCC AMI Subgroup revised the AMI use cases to better reflect actual AMI deployments.

- **Benefits and Challenges of Distribution Automation**: Use Case Scenarios (White Paper for Distribution on T&D DEWG), extracted from a California Energy Commission (CEC) document which has 82 Use Cases; now posted on the SGIP TWiki.

- **EPRI Use Case Repository**: A compilation of IntelliGrid and Southern California Edison (SCE) Use Cases, plus others. *See* EPRI Web site, Use Case Repository.

- **SCE Use Cases**: Developed by Southern California Edison with the assistance of EnerNex. *See* SCE.com Web site, Open Innovation.

A certain amount of overlap is found in these sources, particularly in the new area of AMI. However, even the combined set (numbering over 1000 Use Cases) does not address all requirements. For example, for one operation—the connect/disconnect of meters—originally 6 utilities developed more than 20 use case variations to meet their diverse needs, often as a means to address different state regulatory requirements.

The collected Use Cases listed in this chapter were not generally copied verbatim from their sources but were oftentimes edited to focus on the security issues.

10.2 Key Security Requirements Considerations

The Use Cases listed in subsection 10.3 can be considered to have key security requirements that may vary in vulnerabilities and impacts, depending upon the actual systems, but that nonetheless can be generally assessed as having security requirements in the three principal areas addressed in subsections 10.2.1 through 10.2.3.

10.2.1 CIA Security Requirements

The following points briefly outline security requirements related to confidentiality, integrity, and availability.

Confidentiality is generally the least critical for power system reliability. However, this is important as customer information becomes more easily available in cyber form:

- Privacy of customer information is the most important,
- Electric market information has some confidential portions,
- General corporate information, such as human resources, internal decision making, etc.

Integrity is generally considered the second most critical security requirement for power system operations and includes assurance that—

- Data has not been modified without authorization,
- Source of data is authenticated,
- Time -tamp associated with the data is known and authenticated,
- Quality of data is known and authenticated.

Availability is generally considered the most critical security requirement, although the time latency associated with availability can vary:

- 4 milliseconds for protective relaying,
- Subseconds for transmission wide area situational awareness monitoring,
- Seconds for substation and feeder supervisory control and data acquisition (SCADA) data,
- Minutes for monitoring noncritical equipment and some market pricing information,
- Hours for meter reading and longer term market pricing information,

- Days/weeks/months for collecting long-term data such as power quality information.

10.2.2 Critical Issues for the Security Requirements of Power Systems

The automation and control systems for power system operations have many differences from most business or corporate systems. Some particularly critical issues related to security requirements include—

- Operation of the power system must continue 24×7 with high availability (e.g., 99.99% for SCADA and higher for protective relaying) regardless of any compromise in security or the implementation of security measures which hinder normal or emergency power system operations.
- Power system operations must be able to continue during any security attack or compromise (as much as possible).
- Power system operations must recover quickly after a security attack or compromised information system.
- The complex and many-fold interfaces and interactions across this largest machine of the world—the power system—makes security particularly difficult since it is not easy to separate the automation and control systems into distinct "security domains," and yet end-to-end security is critical.
- There is not a one-size-fits-all set of security practices for any particular system or for any particular power system environment.
- Testing of security measures cannot be allowed to impact power system operations.
- Balance is needed between security measures and power system operational requirements. Absolute security is never perfectly achievable, so the costs and impacts on functionality of implementing security measures must be weighed against the possible impacts from security breaches.
- Balance is also needed between risk and the cost of implementing the security measures.

10.2.3 Security Programs and Management

Development of security programs is critical to all Use Cases, including—

- Risk assessment to develop security requirements based on business rational (e.g. impacts from security breaches of ICIA) and system vulnerabilities.
  - The likelihood of particular threat agents, which are usually included in risk assessments, should only play a minor role in the overall risk assessment, since the power system is so large and interconnected that appreciating the risk of these threat agents would be very difficult.
  - However, in detailed risk assessments of specific assets and systems, some appreciation of threat agent probabilities is necessary to ensure that an appropriate balance between security and operability is maintained.
- Security technologies that are needed to meet the security requirements:
  - Plan the system designs and technologies to embed the security from the start

- Implement the security protocols
- Add physical security measures
- Implement the security monitoring and alarming tools
- Establish role-based access control (RBAC) to authorize and authenticate users, both human and cyber, for all activities, including password/access management, certificate and key management, and revocation management
- Provide the security applications for managing the security measures

- Security policies, training, and enforcement to focus on the human side of security, including:
  - Normal operations
  - Emergency operations when faced with a possible or actual security attack
  - Recovery procedures after an attack
  - Documentation of all anomalies for later analysis and re-risk assessment.
- Conformance testing for both humans and systems to verify they are using the security measures and tools appropriately and not bypassing them:
  - Care must be taken not to impact operations during such testing
  - If certain security measures actually impact power system operations, the balance between that impact and the impact of a security compromise should be evaluated
- Periodic reassessment of security risks

10.3 USE CASE SCENARIOS

The following subsections present the key Use Cases deemed architecturally significant with respect to security requirements for the Smart Grid, with the listing grouped according to 10 main categories: AMI, Demand Response, Customer Interfaces, Electricity Market, Distribution Automation, Plug-in Hybrid Electric Vehicles (PHEV), Distributed Resources, Transmission Resources, Regional Transmission Operator / Independent System Operator (RTO/ISO) Operations, and Asset Management.

10.3.1 AMI Security Use Cases

In this chapter basic use cases are described which can be used as building blocks for more complex use cases that users of this guideline and AMI security profile may be interested in. Dozens of use cases can be constructed from these basic functions. A few short examples are provided below that demonstrate a more detailed process of combining the basic building blocks in the AMI security profile.

There are other functions not specified below which can be composed from these defined functions. The absence of a function on the list of use cases should not be taken as indication those functions are less important, but as an indication those functions are combinations of basic functions with the possible addition of out-of-scope and/or business process behaviors. Some examples:

- Revenue Protection: Revenue protection with respect to AMI consists of a number of business processes combined with AMI functions. For example, theft of service can be identified by comparing meter reads (Meter Sends Information function) of power line branch meter with the sum of meter reads of each of the subscribers on that branch (a specific non-AMI business process). A discrepancy on the total can indicate theft of service.

- Meter Removal: Detection of meter removal can occur in a number of different ways including "Meter Sends Information" where the exception case indicates no contact with the meter or "Meter Sends Alarm" where the self-protection capability of the meter notes a tamper event. Additionally, meter not communicating (disassociated from network) where a meter that has been associated or registered on the network is no longer performing necessary activities to maintain registration.

- Meter Bypass: Generically, detection of meter bypass is a back office business process dependent on information received from the field. One way of detecting meter bypass is historical analysis of consumption data and comparison of that data to other similar subscribers in the region.

- Outage Detection and Restoration: This is not directly an AMI function, but information for the process can be acquired from the AMI meter field through the "Meter Sends Information" function and the "Meter Sends Alarm" function. Depending on the needs of restoration, "Utility Sends Operational Command" may also occur. The specific set of functions for detection and restoration will most likely be different with each outage event and may differ based on the Utility and its practices.

- Pre-paid Metering: Depending on the specific mechanism for pre-paid metering (e.g. payment at the meter, payment to the utility, emergency power enable button) this can end up being the combination of any or all AMI functions. At the simplest, the setting of a consumption limit on a meter based on some business process decision by the utility would be a "Utility Sends Operational Command". Information about consumption rates as well as warnings about credit exhaustion will flow back to the utility via "Meter Sends Information" and "Meter Sends Alarm".

The 6 basic functions listed below were chosen because they mostly represent the same level of control plane and they involve only AMI elements. As utilities flesh out their set of use cases which involve (but are not necessarily limited to) AMI elements, they should use this set of functions to describe the AMI portion of the use case.

Category: AMI	Overall Use Case #1

Scenario: Meter sends information

Category Description

AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third-party systems that are interfaced to the AMI systems.

Scenario Description

A meter sends automated energy usage information to the Utility (e.g. meter read (usage data)). The automated send of energy usage information is initiated by the meter and is sent to the Advanced metering Infrastructure (AMI) Head End System (HES). The Head End system message flows to the meter Reading and Control (MRC). The MRC evaluates the message. The MRC archives the automated energy usage information and forwards the information onto the meter Data Management Systems (MDMS).

- Meter configuration information
- Periodic meter Reading
- On-Demand meter Reading
- Net metering for distributed energy resources (DER) and plug in electric vehicle (PEV)

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Enables new products, services and markets • Optimizes asset utilization and operate efficiently	• Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database to avoid serious breaches of privacy and potential legal repercussions • Integrity of meter data is important, but the impact of incorrect data is not large • Availability of meter data is not critical in real-time	• Customer data access • Customer data privacy and security • Reliable data for billing • Third party or party acting as an agent of the utility access to energy usage information for market and/or consumer services • Third party or party acting on behalf of the utility reliable data

3733

Category: AMI	Overall Use Case #2
Scenario: Utility sends operational command to meter	

Category Description

AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third-party systems that are interfaced to the AMI systems.

Scenario Description

A Utility requires an operational command be sent to the meter, such as a disconnect or reconnect of an electric smart meter. The command flows to the meter Reading and Control (MRC) that looks up the meter associated with the customer and then instructs the Advanced metering Infrastructure (AMI) Head End system (HES) to communicate the command to the meter. The HES evaluates current conditions and, if suitable (e.g. reconnects are not executed if the system is in a rolling black out state), sends the command to the meter. When the meter receives the command and parameters, the meter evaluates the command as to whether it is permitted. If the command is permitted, the meter executes the command and sends the result to the HES. If the command is not permitted, the meter sends the result to the HES. The HES evaluates the result (whether the action was successful or not and why) and relays that to the MRC. The MRC records the command result and notifies the appropriate actors.

- Configuration request
- Calibration request
- Connect / Disconnect request
- Prepaid metering configuration/setup

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Operates resiliently against attack and natural disasters	• Confidentiality requirements of the meter command is generally not very important • Integrity of control commands to the meter is critical to avoid dangerous/unsafe conditions. • Availability is not important with the exception of emergency situations such as fire or medical emrgency for remote connect/disconnect.	• Customer Safety • Third party or party acting as an agent of the utility access to energy usage information for market and/or consumer services

3734
3735

3736

Category: AMI	Overall Use Case #3
Scenario: Field tool sends instruction to the meter	

Category Description

AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third-party systems that are interfaced to the AMI systems.

Scenario Description

A field tool requires onsite maintenance of an electric smart meter. The Field Tool connects directly to an electric smart meter, then the command flows to the smart meter. When the meter receives the command and parameters, the meter evaluates the command as to whether it is permitted. If the command is permitted, the meter executes the command and sends the result back to the field tool. This use case is a closed loop, as stated in the preconditions.

- Meter calibration update
- Meter configuration update

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Enables new products, services and markets	• Confidentiality is not important unless some maintenance activity involves personal information • Integrity of meter maintenance repairs and updates are essential to prevent malicious intrusions and integrity of billing data to prevent high utility bills • Availability is important, because field tool requires real time interaction with the meter.	• Customer data privacy and security • Third party or party acting as an agent of the utility having access to customer & Utility information

3737
3738

Category: AMI	Overall Use Case #4
Scenario: Utility sends non-operational instruction to meter (peer-to-peer)	

Category Description

AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third-party systems that are interfaced to the AMI systems.

Scenario Description

This use case describes the Utility sending a non-operational instruction send to meter as a peer-to-peer transaction. A Utility requires actions from a set of meter which may or may not result in a change to the power state of the grid. These include at least meter reading, and certain configuration changes. The meter Reading and Control (MRC) determines the need to send instruction(s) to a meter. MRC looks up the meter associated with the customer and then instructs the Advanced metering Infrastructure (AMI) Head End system (HES) to queue up and execute the instruction(s). The AMI Head End can determine the instruction needs to be split into packets, schedules the sending of the packets and continues to send the packets to the meter until all instruction packets have been sent. The meter receives the instruction(s) and determines if the instruction is permitted. After execution, the meter sends the instruction result to the HES. The HES will then send the instruction result to the MRC. If the instruction result is energy usage information, the MRC will then forward the energy usage information onto the meter Data Management System (MDMS). If the MDMS receives energy usage information, then the MDMS forwards the energy usage information onto other actors for other actions.

- Meter calibration validation
- Connectivity validation
- Geolocation of meter
- Smart meter battery management

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Operates resiliently in response to natural and manmade events • Increases the timeliness, availability, and granularity of information for billing	• Confidentiality may or may not be an issue depending on whether information is public (date, time) or private (password change, Personal Identifiable Information). Some items must be confidential due to laws and regulations; confidentiality of other items may be left up to local policy, such as firmware or GPS coordinates. • Integrity of meter maintenance repairs and updates is essential to prevent malicious intrusions • Availability is important, but only in terms of hours or maybe days to provide synchronization and coherence of devices on the network, i.e. all devices acting together for entire population	• Customer data privacy and security • Third party or party acting as an agent of the utility having access to customer & Utility information • Third party access to electrical distribution system, e.g. separation of duties & authority (regulatory impact) • Vendor product quality

3739

Category: AMI	Overall Use Case #5
Scenario: Utility sends batch instruction to meters (group multicast transaction)	

Category Description

AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third-party systems that are interfaced to the AMI systems.

Scenario Description

This use case describes a batch instruction send to meters as a multicast transaction in an open loop situation. The open loop situation means that Advanced metering Infrastructure (AMI) Head End System (HES) does not expect a response for each packet sent to a meter. A Utility requires actions from a set of meters which may or may not result in a change to the power state of the grid. These include at least meter reading, and certain configuration changes. The meter Reading and Control (MRC) determines the need to send batch instructions to more than one meter. MRC looks up the meter associated with the customer and then instructs the Advanced metering Infrastructure (AMI) Head End system (HES) to queue up and execute the instructions. The AMI Head End can determine the instruction needs to be split into packets, schedules the sending of the packets and continues to send the packets to the meters until all instruction packets have been sent. The meter(s) receive the instruction(s) and determines if the instruction is permitted. After execution, the meter(s) send the instruction result to the HES. The HES will then send the instruction result to the MRC. If the instruction result is energy usage information, the MRC will then forward the energy usage information onto the meter Data Management System (MDMS). If the MDMS receives energy usage information, then the MDMS forwards the energy usage information onto other actors for other actions.

- Firmware update
- Key management update

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Enables new products, services and markets • Reduces cost of operations	• Confidentiality is not important unless some maintenance activity involves personal information • Integrity of meter maintenance repairs and updates are essential to prevent malicious intrusions • Availability is important, but only in terms of hours or maybe days	• Confirmation (if required) of update status. • Customer data privacy and security • Third party or party acting as an agent of the utility access to energy usage information for market and/or consumer services

3740
3741

Category: AMI	Overall Use Case #6
Scenario: Meter sends alarm or unsolicited and unscheduled request to the utility	
Category Description AMI systems consist of the hardware, software, and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third-party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third-party systems that are interfaced to the AMI systems.	
Scenario Description A meter sends an alarm or unsolicited and unscheduled request to the Utility (e.g. Physical tamper detection, Network join request, or HAN device / direct load control device enrollment request (proxy for customer). The message is initiated by the meter and sends the messages to the Advanced metering Infrastructure (AMI) Head End System (HES). The HES message flows to the meter Reading and Control (MRC). The MRC evaluates the message. The MRC records the command result and notifies the appropriate actors.	

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Optimizes asset utilization and operate efficiently • Operates resiliently against attack and natural disasters	• Confidentiality is not important unless alarm contains private information or exposes an attempt to obtain security information stored in the meter • Integrity - Protect against energy theft • Protect inetgrity of meter configuration • protect integrity of reporting • To protect the integrity of the network (authorized devices) • Availabilty is important to capture last gasp detecting, join detection, and reporting	• Network Service Providers • Customer may receive outage notification through third party • Billing service provider • Transmission & Distribution service provider

3742

3743

10.3.2 Demand Response Security Use Cases

Category: Demand Response (DR)	Overall Use Case #7
Scenario: Real-Time Pricing (RTP) for Customer Load and DER/PEV	
Category Description Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. RTP inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.	
Scenario Description Use of RTP for electricity is common for very large customers, affording them an ability to determine when to use power and minimize the costs of energy for their business. The extension of RTP to smaller industrial and commercial customers and even residential customers is possible with smart metering and in-home displays. Aggregators or customer energy management systems must be used for these smaller consumers due to the complexity and 24×7 nature of managing power consumption. Pricing signals may be sent via an AMI system, the Internet, or other data channels.	

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• Integrity, including nonrepudiation, of pricing information is critical, since there could be large financial and possibly legal implications • Availability, including nonrepudiation, for pricing signals is critical because of the large financial and possibly legal implications • Confidentiality is important mostly for the responses that any customer might make to the pricing signals	• Customer data privacy and security • Retail Electric Supplier access • Customer data access

3745

Category: Demand Response	Overall Use Case #8
Scenario: Time of Use (TOU) Pricing	

Category Description

Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed TOU pricing may be manually handled once the customer is aware of the time periods and the pricing.

Scenario Description

TOU creates blocks of time and seasonal differences that allow smaller customers with less time to manage power consumption to gain some of the benefits of real-time pricing. This is the favored regulatory method in most of the world for dealing with global warming.

Although RTP is more flexible than TOU, it is likely that TOU will still provide many customers will all of the benefits that they can profitably use or manage.

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• Integrity is not critical since TOU pricing is fixed for long periods and is not generally transmitted electronically • Availability is not an issue • Confidentiality is not an issue, except with respect to meter reading	• Customer data privacy and security • Retail Electric Supplier access • Customer data access

3746

3747

3748

Category: Demand Response	Overall Use Case #9
Scenario: Net Metering for DER and PEV	

Category Description

Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.

Scenario Description

When customers have the ability to generate or store power as well as consume power, net metering is installed to measure not only the flow of power in each direction, but also when the net power flows occurred. Often TOU tariffs are employed.

Today larger commercial and industrial (C&I) customers and an increasing number of residential and smaller C&I customers have net metering installed for their photovoltaic systems, wind turbines, combined heat and power (CHP), and other DER devices. As PEVs become available, net metering will increasingly be implemented in homes and small businesses, even parking lots.

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• Integrity is not very critical since net metering pricing is fixed for long periods and is not generally transmitted electronically • Availability is not an issue • Confidentiality is not an issue, except with respect to meter reading	• Customer data privacy and security • Retail Electric Supplier access • Customer data access

3749
3750

3751

Category: Demand Response	Overall Use Case #10
Scenario: Feed-In Tariff Pricing for DER and PEV	
Category Description Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.	
Scenario Description Feed-in tariff pricing is similar to net metering except that generation from customer DER/PEV has a different tariff rate than the customer load tariff rate during specific time periods.	

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically • Availability is not an issue • Confidentiality is not an issue, except with respect to meter reading	• Customer data privacy and security • Retail Electric Supplier access • Customer data access

3752
3753

3754

Category: Demand Response	Overall Use Case #11
Scenario: Critical Peak Pricing	

Category Description

Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.

Scenario Description

Critical Peak Pricing builds on TOU pricing by selecting a small number of days each year where the electric delivery system will be heavily stressed and increasing the peak (and sometime shoulder peak) prices by up to 10 times the normal peak price. This is intended to reduce the stress on the system during these days.

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically • Availability is not an issue • Confidentiality is not an issue, except with respect to meter reading	• Customer data privacy and security • Retail Electric Supplier access • Customer data access

3755

3756

3757

Category: Demand Response	Overall Use Case #12
Scenario: Mobile Plug-In Electric Vehicle Functions	

Category Description

Demand response is a general capability that could be implemented in many different ways. The primary focus is to provide the customer with pricing information for current or future time periods so they may respond by modifying their demand. This may entail just decreasing load or may involve shifting load by increasing demand during lower priced time periods so that they can decrease demand during higher priced time periods. The pricing periods may be real-time based or may be tariff based, while the prices may also be operationally based or fixed or some combination. Real-time pricing inherently requires computer-based responses, while the fixed time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.

Scenario Description

In addition to customers with PEVs participating in their home-based Demand Response functions, they will have additional requirements for managing the charging and discharging of their mobile PEVs in other locations:

Customer connects PEV at another home

Customer connects PEV outside home territory

Customer connects PEV at public location

Customer charges the PEV

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically • Availability is not an issue • Confidentiality is not an issue, except with respect to meter reading	• Customer data privacy and security • Retail Electric Supplier access • Customer data access

3758

10.3.3 Customer Interfaces Security Use Cases

Category: Customer Interfaces	Overall Use Case #13
Scenario: Customer's In Home Device is Provisioned to Communicate With the Utility	
Category Description Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in-home displays, computers, and mobile devices). In addition to real-time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.	
Scenario Description This scenario describes the process to configure a customer's device to receive and send data to utility systems. The device could be an information display, communicating thermostat, load control device, or smart appliance.	

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• To protect passwords • To protect key material • To authenticate with other devices on the AMI system	• Customer device standards • Customer data privacy and security

Category: Customer Interfaces	Overall Use Case #14
Scenario: Customer Views Pricing or Energy Data on Their In-Home Device	
Category Description Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in-home displays, computers, and mobile devices). In addition to real-time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.	
Scenario Description This scenario describes the information that should be available to customers on their in-home devices. Multiple communication paths and device functions will be considered.	

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• To validate that information is trustworthy (integrity)	• Customer device standards • Customer data privacy and security

Category: Customer Interfaces	Overall Use Case #15
Scenario: In-Home Device Troubleshooting	

Category Description

Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in-home displays, computers, and mobile devices). In addition to real-time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.

Scenario Description

This alternate scenario describes the resolution of communication or other types of errors that could occur with in-home devices. Roles of the customer, device vendor, and utility will be discussed.

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• To avoid disclosing customer information • To avoid disclosing key material and/or passwords	• Customer device standards • Customer data privacy and security

3762

Category: Customer Interfaces	Overall Use Case #16
Scenario: Customer Views Pricing or Energy Data via the Internet	

Category Description

Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in -home displays, computers, and mobile devices). In addition to real-time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.

Scenario Description

In addition to a utility operated communications network (i.e., AMI), the Internet can be used to communicate to customers and their devices. Personal computers and mobile devices may be more suitable for displaying some types of energy data than low cost specialized in-home display devices. This scenario describes the information that should be available to the customer using the Internet and some possible uses for the data.

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• To protect customer's information (privacy) • To provide accurate information	• Customer device standards • Customer data privacy and security

3763

Category: Customer Interfaces	Overall Use Case #17
Scenario: Utility Notifies Customers of Outage	

Category Description

Customers want to understand how their energy consumption habits affect their monthly energy bills and to find ways to reduce their monthly energy costs. Customers should have the ability to receive information on their usage and the price of energy on a variety of devices (in-home displays, computers, and mobile devices). In addition to real-time and historical energy data, customers should be able to receive messages from the utility notifying them about outages.

Scenario Description

When an outage occurs the utility can notify affected customers and provide estimated restoration times and report when power has been restored. Smart Grid technologies can improve the utility's accuracy for determination of affected area and restoration progress.

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• To validate that the notification is legitimate • Customer's information is kept private	• Customer device standards • Customer data privacy and security

3764

Category: Customer Interfaces	Overall Use Case #18
Scenario: Customer Access to Energy-Related Information	

Category Description

Customers with home area networks (HANs) and/or building energy management (BEM) systems will be able to interact with the electric utilities as well as third-party energy services providers to access information on their own energy profiles, usage, pricing, etc.

Scenario Description

Customers with HANs and/or BEM systems will be able to interact with the electric utilities as well as third-party energy services providers. Some of these interactions include:

Access to real-time (or near-real-time) energy and demand usage and billing information

Requesting energy services such as move-in/move-out requests, prepaying for electricity, changing energy plans (if such tariffs become available), etc.

Access to energy pricing information

Access to their own DER generation/storage status

Access to their own PEV charging/discharging status

Establishing thermostat settings for demand response pricing levels

Although different types of energy related information access is involved, the security requirements are similar.

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• Integrity, including non-repudiation, is critical since energy and pricing data will have financial impacts • Availability is important to the individual customer, but will not have wide-spread impacts • Confidentiality is critical because of customer privacy issues	• Customer data privacy and security • Retail Electric Supplier access • Customer data access

3765

10.3.4 Electricity Market Security Use Cases

Category: Electricity Market	Overall Use Case #19	
Scenario: Bulk Power Electricity Market		
Category Description The electricity market varies significantly from state to state, region to region, and at local levels. The market is still evolving after some initial setbacks and is expected to expand from bulk power to retail power and eventually to individual customer power as tariffs are developed to provide incentives. Demand response, handled in subsection 10.3.2, is a part of the electricity market.		
Scenario Description The bulk power market varies from region to region, and is conducted primarily through RTOs and ISOs. The market is handled independently from actual operations, although the bids into the market obviously affect which generators are used for what time periods and which functions (base load, regulation, reserve, etc.). Therefore there are no direct operational security impacts, but there are definitely financial security impacts.		
Smart Grid Characteristics • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	**Cyber Security Objectives/Requirements** • Integrity for pricing and generation information is critical • Availability for pricing and generation information is important within minutes to hours • Confidentiality for pricing and generation information is critical	**Potential Stakeholder Issues** • Customer data privacy and security • Retail Electric Supplier access • Customer data access

Category: Electricity Market	Overall Use Case #20
Scenario: Retail Power Electricity Market	
Category Description The electricity market varies significantly from state to state, region to region, and at local levels. The market is still evolving after some initial setbacks and is expected to expand from bulk power to retail power and eventually to individual customer power as tariffs are developed to provide incentives. Demand response, handled in subsection 10.3.2, is a part of the electricity market.	
Scenario Description The retail power electricity market is still minor, but growing, compared to the bulk power market but typically involves aggregators and energy service providers bidding customer-owned generation or load control into both energy and ancillary services. Again it is handled independently from actual power system operations. Therefore there are no direct operational security impacts, but there are definitely financial security impacts. (The aggregator's management of the customer-owned generation and load is addressed in the Demand Response subsection (see 10.3.2).)	

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• Integrity for pricing and generation information is critical • Availability for pricing and generation information is important within minutes to hours • Confidentiality for pricing and generation information is critical	• Customer data privacy and security • Retail Electric Supplier access • Customer data access

3768

Category: Electricity Market	Overall Use Case #21
Scenario: Carbon Trading Market	
Category Description The electricity market varies significantly from state to state, region to region, and at local levels. The market is still evolving after some initial setbacks and is expected to expand from bulk power to retail power and eventually to individual customer power as tariffs are developed to provide incentives. Demand response, handled in subsection 10.3.2, is a part of the electricity market.	
Scenario Description The carbon trading market does not exist yet, but the security requirements will probably be similar to the retail electricity market.	

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets	• Integrity for pricing and generation information is critical • Availability for pricing and generation information is important within minutes to hours • Confidentiality for pricing and generation information is critical	• Customer data privacy and security • Retail Electric Supplier access • Customer data access

3769

10.3.5 Distribution Automation Security Use Cases

Category: Distribution Automation (DA)	Overall Use Case #22
Scenario: DA within Substations	

Category Description

A broad definition of "distribution automation" includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.

No one approach is optimal for a utility or its customers. Certain DA functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other DA functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.

Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

Distribution automation within substations involves monitoring and controlling equipment in distribution substations to enhance power system reliability and efficiency. Different types of equipment are monitored and controlled:

Distribution supervisory control and data acquisition (SCADA) system monitors distribution equipment in substations

Supervisory control on substation distribution equipment

Substation protection equipment performs system protection actions

Reclosers in substations

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality for the range of needs in a digital economy • Optimizes asset utilization and operating efficiency • Anticipates and responds to system disturbances in a self-correcting manner	• Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently • Availability for control is critical, while monitoring individual equipment is less critical • Confidentiality is not very important	• Customer safety • Device standards • Cyber Security

3771

Category: Distribution Automation	Overall Use Case #23
Scenario: DA Using Local Automation	

Category Description

A broad definition of “distribution automation” includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.

No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.

Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

Local automation of feeder equipment consists of power equipment that is managed locally by computer-based controllers that are preset with various parameters to issue control actions. These controllers may just monitor power system measurements locally, or may include some short range communications to other controllers and/or local field crews. However, in these scenarios, no communications exist between the feeder equipment and the control center.

Local automated switch management

Local volt/VAR control

Local Field crew communications to underground network equipment

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently • Availability for control is critical, while monitoring individual equipment is less critical • Confidentiality is not very important	• Customer safety • Customer device standards • Demand response acceptance by customers

3772
3773

3774

Category: Distribution Automation	Overall Use Case #24
Scenario: DA Monitoring and Controlling Feeder Equipment	

Category Description

A broad definition of "distribution automation" includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.

No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.

Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

Operators and distribution applications can monitor the equipment on the feeders and determine whether any actions should be taken to increase reliability, improve efficiency, or respond to emergencies. For instance, they can—

Remotely open or close automated switches

Remotely switch capacitor banks in and out

Remotely raise or lower voltage regulators

Block local automated actions

Send updated parameters to feeder equipment

Interact with equipment in underground distribution vaults

Retrieve power system information from smart meters

Automate emergency response

Provide dynamic rating of feeders

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently • Availability for control is critical, while monitoring individual equipment is less critical • Confidentiality is not very important	• Customer safety • Customer device standards • Demand response acceptance by customers

3775
3776

3777

Category: Distribution Automation	Overall Use Case #25

Scenario: Fault Detection, Isolation, and Restoration

Category Description

A broad definition of “distribution automation” includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.

No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.

Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

AMI smart meters and distribution automated devices can detect power outages that affect individual customers and larger groups of customers. As customers rely more fundamentally on power (e.g., PEV) and become used to not having to call in outages, outage detection, and restoration will become increasingly critical.

The automated fault location, isolation, and restoration (FLIR) function uses the combination of the power system model with the SCADA data from the field on real-time conditions to determine where a fault is probably located by undertaking the following steps:

Determines the faults cleared by controllable protective devices:

Determines the faulted sections based on SCADA fault indications and protection lockout signals

Estimates the probable fault locations based on SCADA fault current measurements and real-time fault analysis

Determines the fault-clearing non-monitored protective device

Uses closed-loop or advisory methods to isolate the faulted segment

Once the fault is isolated, it determines how best to restore service to unfaulted segments through feeder reconfiguration.

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity of outage information is critical • Availability to detect large-scale outages usually involve multiple sources of information • Confidentiality is not very important	• Customer safety • Customer device standards • Demand response acceptance by customers

3778
3779

3780

Category: Distribution Automation	Overall Use Case #26
Scenario: Load Management	

Category Description

A broad definition of “distribution automation” includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.

No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.

Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

Load management provides active and passive control by the utility of customer appliances (e.g. cycling of air conditioner, water heaters, and pool pumps) and certain C&I customer systems (e.g., plenum precooling, heat storage management).

Direct load control and load shedding

Demand side management

Load shift scheduling

Curtailment planning

Selective load management through HANs

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity of load control commands is critical to avoid unwarranted outages • Availability for load control is important – in aggregate (e.g. > 300 MW), it can be critical • Confidentiality is not very important	• Customer safety • Customer device standards • Demand response acceptance by customers

3781
3782

3783

Category: Distribution Automation	Overall Use Case #27

Scenario: Distribution Analysis using Distribution Power Flow Models

Category Description

A broad definition of “distribution automation” includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.

No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.

Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

The brains behind the monitoring and controlling of field devices are the DA analysis software applications. These applications generally use models of the power system to validate the raw data, assess real-time and future conditions, and issue the appropriate actions. The applications may be distributed and located in the field equipment for local assessments and control, and/or may be centralized in a distribution management system (DMS) for global assessment and control.

Local peer-to-peer interactions between equipment

Normal distribution operations using the Distribution System Power Flow (DSPF) model

Emergency distribution operations using the DSPF model

Study-Mode DSPF model

DSPF/DER model of distribution operations with significant DER generation/storage

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity is critical to operate the distribution power system reliably, efficiently, and safely • Availability is critical to operate the distribution power system reliably, efficiently, and safely • Confidentiality is not important	• Customer safety • Customer device standards • Demand response acceptance by customers

3784

Category: Distribution Automation	Overall Use Case #28
Scenario: Distributed Energy Resources Management	

Category Description

A broad definition of “distribution automation” includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected DER, and automated interfaces with end-users.

No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.

Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

In the future, more and more of generation and storage resources will be connected to the distribution network and will significantly increase the complexity and sensitivity of distribution operations. Therefore, the management of DER generation will become increasingly important in the overall management of the distribution system, including load forecasts, real-time monitoring, feeder reconfiguration, virtual and logical microgrids, and distribution planning.

Direct monitoring and control of DER

Shut-down or islanding verification for DER

PEV management as load, storage, and generation resource

Electric storage fill/draw management

Renewable energy DER with variable generation

Small fossil resource management, such as backup generators to be used for peak shifting

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity is critical for any management/ control of generation and storage • Availability requirements may vary depending on the size (individual or aggregate) of the DER plant • Confidentiality may involve some privacy issues with customer-owned DER	• Customer safety • Customer device standards • Demand response acceptance by customers

3785

Category: Distribution Automation	Overall Use Case #29
Scenario: Distributed Energy Resource Management	

Category Description

A broad definition of “distribution automation” includes any automation which is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources, and automated interfaces with end-users.

No one approach is optimal for a utility or its customers. Certain distribution automation functions, such as optimal volt/VAR control, can be more beneficial to one utility or even a few feeders in one utility, while other distribution automation functions, such as fault detection, isolation, and service restoration, could be far more beneficial in other utilities.

Increasingly, distribution automation will entail closed-loop control, where distribution algorithms, applied to real-time models of the distribution system, will increase reliability and/or efficiency of the distribution system without direct operator involvement.

Scenario Description

Distribution planning typically uses engineering systems with access only to processed power system data that is available from the control center. It is therefore relatively self-contained.

Operational planning

Assessing planned outages

Storm condition planning

Short-term distribution planning

Short term load forecast

Short term DER generation and storage impact studies

Long term distribution planning

Long term load forecasts by area

Optimal placements of switches, capacitors, regulators, and DER

Distribution system upgrades and extensions

Distribution financial planners

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity not critical due to multiple sources of data • Availability is not important • Confidentiality is not important	• Cyber security

3786

10.3.6 PHEV Security Use Cases

Category: Plug In Hybrid Electric Vehicles (PHEV)	Overall Use Case #30	
Scenario: Customer Connects PHEV to Energy Portal		
Category Description Plug in electric vehicles will have a significant impact on the future electric system and challenge the utility and customer to manage vehicle connection and charging. As adoption rates of electric vehicles increase, the utility will have to handle the new load imposed on the electrical system. Scenarios will consider customer payment issues regarding mobility, load shifting vehicle charging, and the use of electric vehicles as a distributed resource.		
Scenario Description This scenario discusses the simple case of a customer plugging in an electric vehicle at their premise to charge its battery. Variations of this scenario will be considered that add complexity: a customer charging their vehicle at another location and providing payment or charging at another location where the premise owner pays.		
Smart Grid Characteristics • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently	**Objectives/Requirements** • The customer's information is kept private • Billing information is accurate	**Potential Stakeholder Issues** • Vehicle standards • Customer safety • Customer device standards • Demand response acceptance by customers

Category: Plug In Hybrid Electric Vehicles	Overall Use Case #31
Scenario: Customer Connects PHEV to Energy Portal and Participates in ”Smart” (Optimized) Charging	
Category Description Plug in electric vehicles will have a significant impact on the future electric system and challenge the utility and customer to manage vehicle connection and charging. As adoption rates of electric vehicles increase, the utility will have to handle the new load imposed on the electrical system. Scenarios will consider customer payment issues regarding mobility, load shifting vehicle charging, and the use of electric vehicles as a distributed resource.	
Scenario Description In addition to simply plugging in an electric vehicle for charging, in this scenario the electric vehicle charging is optimized to take advantage of lower rates or help prevent excessive load peaks on the electrical system.	

Smart Grid Characteristics	**Objectives/Requirements**	**Potential Stakeholder Issues**
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently	• Customer information is kept private	• Vehicle standards • Customer safety • Customer device standards • Demand response acceptance by customers

3789

Category: Plug In Hybrid Electric Vehicles	Overall Use Case #32
Scenario: PHEV or Customer Receives and Responds to Discrete Demand Response Events	

Category Description

Plug in electric vehicles will have a significant impact on the future electric system and challenge the utility and customer to manage vehicle connection and charging. As adoption rates of electric vehicles increase, the utility will have to handle the new load imposed on the electrical system. Scenarios will consider customer payment issues regarding mobility, load shifting vehicle charging, and the use of electric vehicles as a distributed resource.

Scenario Description

An advanced scenario for electric vehicles is the use of the vehicle to provide energy stored in its battery back to the electrical system. Customers could participate in demand response programs where they are provided an incentive to allow the utility to request power from the vehicle at times of high system load.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently	• Improved system stability and availability • To keep customer information private • To insure DR messages are accurate and trustworthy	• Vehicle standards • Customer safety • Customer device standards • Demand response acceptance by customers

3790

Category: Plug In Hybrid Electric Vehicles	Overall Use Case #33
Scenario: PHEV or Customer Receives and Responds to Utility Price Signals	

Category Description

Plug in electric vehicles will have a significant impact on the future electric system and challenge the utility and customer to manage vehicle connection and charging. As adoption rates of electric vehicles increase, the utility will have to handle the new load imposed on the electrical system. Scenarios will consider customer payment issues regarding mobility, load shifting vehicle charging, and the use of electric vehicles as a distributed resource.

Scenario Description

In this scenario, the electric vehicle is able to receive and act on electricity pricing data sent from the utility. The use of pricing data for charging is primarily covered in another scenario. The pricing data can also be used in support of a distributed resource program where the customer allows the vehicle to provide power to the electric grid based on market conditions.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently	• Improved system stability and availability • Pricing signals are accurate and trustworthy • Customer information is kept private	• Vehicle standards • Customer safety • Customer device standards • Demand response acceptance by customers

3791

3792 **10.3.7 Distributed Resources Security Use Cases**

Category: Distributed Resources	Overall Use Case #34	
Scenario: Customer Provides Distributed Resource		
Category Description Traditionally, distributed resources have served as a primary or emergency backup energy source for customers that place a premium on reliability and power quality. Distributed resources include generation and storage devices that can provide power back to the electric power system. Societal, policy, and technological changes are increasing the adoption rate of distributed resources, and Smart Grid technologies can enhance the value of these systems.		
Scenario Description This scenario describes the process of connecting a distributed resource to the electric power system and the requirements of net metering.		
Smart Grid Characteristics • Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently	**Objectives/Requirements** • Customer information is kept private • Net metering is accurate and timely	**Potential Stakeholder Issues** • Safety • Customer data privacy and security

3793

Category: Distributed Resources	Overall Use Case #35
Scenario: Utility Controls Customer's Distributed Resource	

Category Description

Traditionally, distributed resources have served as a primary or emergency backup energy source for customers that place a premium on reliability and power quality. Distributed resources include generation and storage devices that can provide power back to the electric power system. Societal, policy, and technological changes are increasing the adoption rate of distributed resources, and Smart Grid technologies can enhance the value of these systems.

Scenario Description

Distributed generation and storage can be used as a demand response resource where the utility can request or control devices to provide energy back to the electrical system. Customers enroll in utility programs that allow their distributed resource to be used for load support or to assist in maintaining power quality. The utility programs can be based on direct control signals or pricing information.

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
• Enables active participation by consumers • Accommodates all generation and storage options • Enables new products, services and markets • Provides power quality for the digital economy • Optimizes asset utilization and operate efficiently	• Commands are trustworthy and accurate • Customer's data is kept private • DR messages are received timely	• Safety • Customer data privacy and security

3794

10.3.8 Transmission Resources Security Use Cases

Category: Transmission Operations	Overall Use Case #36
Scenario: Real-Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data	
Category Description Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.	
Scenario Description Transmission normal real-time operations involve monitoring and controlling the transmission system using the SCADA and EMS. The types of information exchanged include— Monitored equipment states (open/close), alarms (overheat, overload, battery level, capacity), and measurements (current, voltage, frequency, energy) Operator command and control actions, such as supervisory control of switching operations, setup/options of EMS functions, and preparation for storm conditions Closed-loop actions, such as protective relaying tripping circuit breakers upon power system anomalies Automation system controls voltage, VAR, and power flow based on algorithms, real-time data, and network linked capacitive and reactive components	
Smart Grid Characteristics • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	**Cyber Security Objectives/Requirements** • Integrity is vital to the safety and reliability of the transmission system • Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s) • Confidentiality is not important
	Potential Stakeholder Issues • Customer safety • Customer device standards • Demand response acceptance by customers

Category: Transmission Operations	Overall Use Case #37
Scenario: EMS Network Analysis Based on Transmission Power Flow Models	

Category Description

Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.

Scenario Description

EMS assesses the state of the transmission power system using the transmission power system analysis models and the SCADA data from the transmission substations

EMS performs model update, state estimation, bus load forecast

EMS performs contingency analysis, recommends preventive and corrective actions

EMS performs optimal power flow analysis, recommends optimization actions

EMS or planners perform stability study of network

Exchange power system model information with RTOs/ISOs and/or other utilities

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity is vital to the reliability of the transmission system • Availability is critical to react to contingency situations via operator commands (e.g. one second) • Confidentiality is not important	• Cyber Security

3797

Category: Transmission Operations	Overall Use Case #38
Scenario: Real-Time Emergency Transmission Operations	

Category Description

Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.

Scenario Description

During emergencies, the power system takes some automated actions and the operators can also take actions:

Power System Protection: Emergency operations handles under-frequency load/generation shedding, under-voltage load shedding, load tap changer (LTC) control/blocking, shunt control, series compensation control, system separation detection, and wide area real-time instability recovery

Operators manage emergency alarms

SCADA system responds to emergencies by running key applications such as disturbance monitoring analysis (including fault location), dynamic limit calculations for transformers and breakers based on real-time data from equipment monitors, and pre-arming of fast acting emergency automation

SCADA/EMS generates signals for emergency support by distribution utilities (according to the T&D contracts):

Operators performs system restorations based on system restoration plans prepared (authorized) by operation management

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity is vital to the safety and reliability of the transmission system • Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s) • Confidentiality is not important	• Customer safety • Customer device standards • Demand response acceptance by customers

3798
3799

3800

Category: Transmission Operations	Overall Use Case #39
Scenario: Wide Area Synchro-Phasor System	

Category Description

Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.

Scenario Description

The wide area synchrophasor system provides synchronized and time-tagged voltage and current phasor measurements to any protection, control, or monitoring function that requires measurements taken from several locations, whose phase angles are measured against a common, system-wide reference. Present day implementation of many protection, control, or monitoring functions is hobbled by not having access to the phase angles between local and remote measurements. With system-wide phase angle information, they can be improved and extended. The essential concept behind this system is the system-wide synchronization of measurement sampling clocks to a common time reference.

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	• Integrity is vital to the safety and reliability of the transmission system • Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s) • Confidentiality is not important	• Cyber Security • Customer data privacy and security

3801

10.3.9 RTO/ISO Operations Security Use Cases

Category: RTO/ISO Operations	Overall Use Case #40	
Scenario: RTO/ISO Management of Central and DER Generators and Storage		
Category Description TBD		
Scenario Description RTOs and ISOs manage the scheduling and dispatch of central and distributed generation and storage. These functions include— Real-time scheduling with the RTO/ISO (for nonmarket generation/storage) Real-time commitment to RTO/ISO Real-time dispatching by RTO/ISO for energy and ancillary services Real-time plant operations in response to RTO/ISO dispatch commands Real-time contingency and emergency operations Black start (system restoration after blackout) Emissions monitoring and control		
Smart Grid Characteristics • Provides power quality • Optimizes asset utilization • Anticipates and responds to system disturbances	**Cyber Security Objectives/Requirements** • Integrity is vital to the safety and reliability of the transmission system • Availability is critical to operator commands (e.g. one second) • Confidentiality is not important	**Potential Stakeholder Issues** • Cyber Security • Customer data privacy and security

10.3.10 Asset Management Security Use Cases

Category: Asset Management	Overall Use Case #41
Scenario: Utility Gathers Circuit and/or Transformer Load Profiles	

Category Description

At a high level, asset management seeks a balance between asset performance, cost, and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies, and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain, and protect utility assets.

For our purposes we will establish the scope for the asset management category to be the use of specific applications and devices by utility staff, such as condition monitoring equipment, protection equipment, event recorders, computer-based maintenance management systems (CMMS), display applications, ratings databases, analysis applications, and data marts (historians).

Scenario Description

Load profile data is important for the utility planning staff and is also used by the asset management team that is monitoring the utilization of the assets and by the SCADA/EMS and system operations team. This scenario involves the use of field devices that measure loading, the communications network that delivers the data, the historian database, and the load profile application and display capability that is either separate or an integrated part of the SCADA/EMS.

Load profile data may also be used by automatic switching applications that use load data to ensure new system configurations do not cause overloads.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
• Provides power quality for the range of needs in a digital economy • Optimizes asset utilization and operating efficiency • Anticipates and responds to system disturbances in a self-correcting manner	• Data is accurate (integrity) • Data is provided timely • Customer data is kept private	• Customer data privacy and security • Cyber Security

3807

Category: Asset Management	Overall Use Case #42
Scenario: Utility Makes Decisions on Asset Replacement Based on a Range of Inputs Including Comprehensive Offline and Online Condition Data and Analysis Applications	

Category Description

At a high level, asset management seeks a balance between asset performance, cost, and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies, and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain, and protect utility assets.

For our purposes we will establish the scope for the asset management category to be the use of specific applications and devices by utility staff such as condition monitoring equipment, protection equipment, event recorders, CMMS, display applications, ratings databases, analysis applications and data marts (historians).

Scenario Description

When decisions on asset replacement become necessary, the system operator, asset management, apparatus engineering, and maintenance engineering staff work closely together with the objective of maximizing the life and utilization of the asset while avoiding an unplanned outage and damage to the equipment.

This scenario involves the use of online condition monitoring devices for the range of assets monitored, offline test results, mobile work force technologies, the communications equipment used to collect the online data, data marts (historian databases) to store and trend data as well as condition analysis applications, CMMS applications, display applications, and SCADA/EMS.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
• Provides power quality for the range of needs in a digital economy • Optimizes asset utilization and operating efficiency • Anticipates and responds to system disturbances in a self-correcting manner	• Data provided is accurate and trustworthy • Data is provided timely	• Cyber Security • Customer data privacy and security

3808

3809

Category: Asset Management	Overall Use Case #43
Scenario: Utility Performs Localized Load Reduction to Relieve Circuit and/or Transformer Overloads	

Category Description

At a high level, asset management seeks a balance between asset performance, cost, and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies, and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain, and protect utility assets.

For our purposes we will establish the scope for the asset management category to be the use of specific applications and devices by utility staff, such as condition monitoring equipment, protection equipment, event recorders, CMMS, display applications, ratings databases, analysis applications, and data marts (historians).

Advanced functions that are associated with asset management include dynamic rating and end of life estimation.

Scenario Description

Transmission capacity can become constrained due to a number of system-level scenarios and result in an overload situation on lines and substation equipment. Circuit and/or transformer overloads at the distribution level can occur when higher than anticipated customer loads are placed on a circuit or when operator or automatic switching actions are implemented to change the network configuration.

Traditional load reduction systems are used to address generation shortfalls and other system-wide issues. Localized load reduction can be a key tool enabling the operator to temporarily curtail the load in a specific area to reduce the impact on specific equipment. This scenario describes the integrated use of the AMI system, the demand response system, other load reduction systems, and the SCADA/EMS to achieve this goal.

Smart Grid Characteristics	**Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality for the range of needs in a digital economy • Optimizes asset utilization and operating efficiency • Anticipates and responds to system disturbances in a self-correcting manner	• Load reduction messages are accurate and trustworthy • Customer's data is kept private • DR messages are received and processed timely	• Demand response acceptance by customers • Customer data privacy and security • Retail Electric Supplier access • Customer data access

3814

Category: Asset Management	Overall Use Case #44
Scenario: Utility System Operator Determines Level of Severity for an Impending Asset Failure and Takes Corrective Action	
Category Description At a high level, asset management seeks a balance between asset performance, cost, and risk to achieve the utilities business objectives. A wide range of conventional functions, models, applications, devices, methodologies, and tools may be deployed to effectively plan, select, track, utilize, control, monitor, maintain, and protect utility assets. For our purposes we will establish the scope for the asset management category to be the use of specific applications and devices by utility staff, such as condition monitoring equipment, protection equipment, event recorders, CMMS, display applications, ratings databases, analysis applications, and data marts (historians).	
Scenario Description When pending asset failure can be anticipated, the system operator, asset management, apparatus engineering, and maintenance engineering staff work closely together with the objective of avoiding an unplanned outage while avoiding further damage to the equipment. This scenario involves the use of online condition monitoring devices for the range of assets monitored, offline test results, mobile workforce technologies, the communications equipment used to collect the online data, data marts (historian databases) to store, and trend data, as well as condition analysis applications, CMMS applications, display applications, and SCADA/EMS.	

Smart Grid Characteristics	**Objectives/Requirements**	**Potential Stakeholder Issues**
• Provides power quality for the range of needs in a digital economy • Optimizes asset utilization and operating efficiency • Anticipates and responds to system disturbances in a self-correcting manner	• Asset information provided is accurate and trustworthy • Asset information is provided timely	• Cyber security • Customer data privacy and security

3815
3816
3817

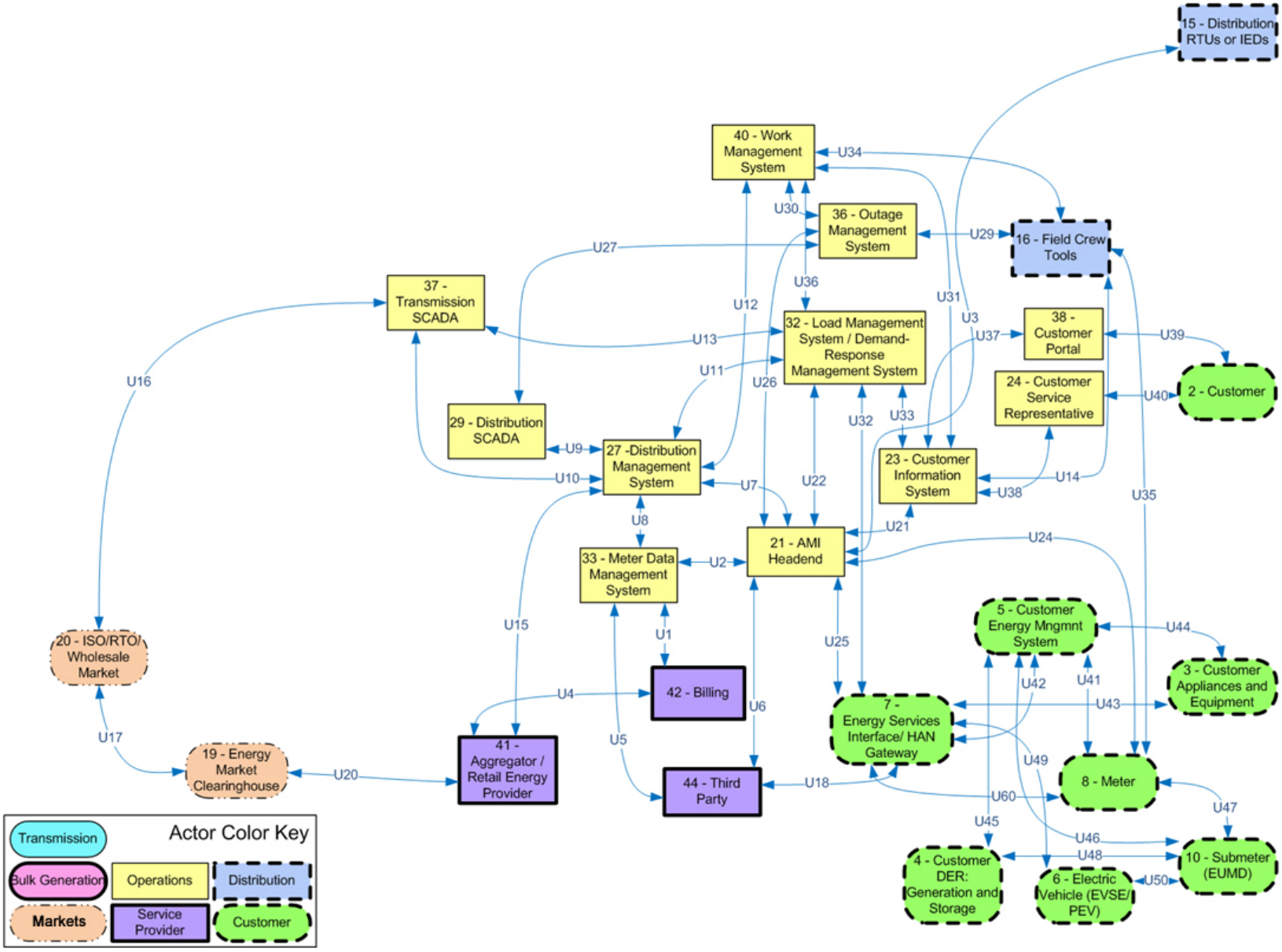
APPENDIX H
LOGICAL ARCHITECTURE AND INTERFACES OF THE SMART GRID

The following subsection refers to detailed logical interfaces including both diagrams and tables that allocate the logical interfaces to one of the logical interface categories.[17]

H.1 ADVANCED METERING INFRASTRUCTURE

The advanced metering infrastructure (AMI) consists of the communications hardware and software, together with the associated system and data management software, that creates a bi-directional network between advanced metering equipment and utility business systems, enabling collection and distribution of information to customers and other parties, such as competitive retail suppliers or the utility itself. AMI provides customers with real-time (or near-real-time) pricing of electricity and may help utilities achieve necessary load reductions. Figure H-1 diagrams the AMI, and Table H-1 lists the AMI logical interfaces by category.

[17] Please note that during development, logical interface 23 was deleted. Subsequent interfaces were not renumbered due to the amount of development already done at that time. It is expected that this will be resolved in the next version of this document.



3832
3833

Figure 10-1 Advanced Metering Infrastructure

3834 **Table 10-1 AMI Logical Interfaces by Logical Interface Category**

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant	U3, U28
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	
5. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	U9, U27
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U7, U10, U13, U16
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U2, U22, U26, U31
8. Interface between back office systems not under common management authority, for example: • Between a third-party billing system and a utility meter data management system	U1, U6, U15
9. Interface with B2B[18] connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U17, U20
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U12, U30, U33, U36

[18] B2B – Business To Business

Logical Interface Category	Logical Interfaces
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	None
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U8, U21, U25, U32
14. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV[19]	U43, U44, U45, U49
16. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U18, U19, U37, U38, U39, U40
17. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	U14, U29, U34, U35
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U24, U41, U46, U47, U50
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
20. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	U11
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	U5, U132

[19] PEV-Plug in Electric Vehicle

Logical Interface Category	Logical Interfaces
22. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	None

H.2 DISTRIBUTION GRID MANAGEMENT

Distribution grid management (DGM) focuses on maximizing the performance of feeders, transformers, and other components of networked distribution systems and integrating with transmission systems and customer operations. As Smart Grid capabilities such as AMI and demand response are developed, and as large numbers of distributed energy resources and plug-in electric vehicles (PEVs) are deployed, the automation of distribution systems becomes increasingly more important to the efficient and reliable operation of the overall power system. The anticipated benefits of DGM include increased reliability, reductions in peak loads and improved capabilities for managing distributed sources of renewable energy. Figure H-2 diagrams the DGM, and Table H-2 lists the DGM logical interfaces by category.

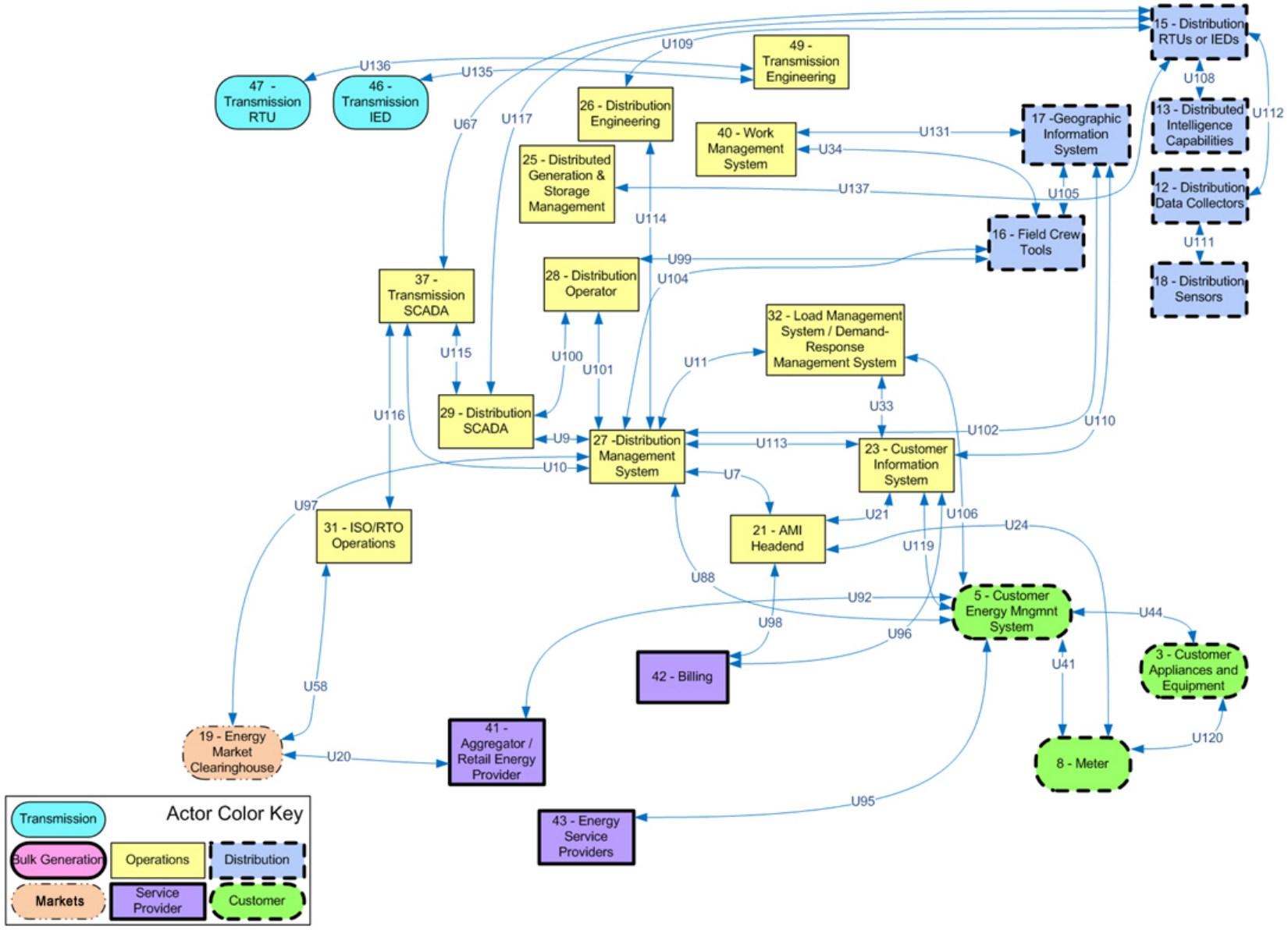


Figure 10-2 Distribution Grid Management

3847 **Table 10-2 DGM Logical Interfaces by Logical Interface Category**

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant	U102, U117, U135, U136
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	
5. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	U9, U11
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U7, U10, U115, U116
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U96, U98, U110
8. Interface between back office systems not under common management authority, for example: • Between a third-party billing system and a utility meter data management system	None
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U20, U58, U97
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U33, U106, U113, U114, U131
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	U111
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	U108, U112

Logical Interface Category	Logical Interfaces
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U95, U119
14. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U44, U120
16. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U88, U92, U100, U101
17. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	U99, U104, U105
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U24, U41
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
20. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	U109
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
22. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	None

3848

H.3 ELECTRIC STORAGE

Electric storage (ES) is the means of storing energy either directly or indirectly. The significant bulk of energy storage technology available today is pumped hydro-electric storage hydroelectric technology. New storage capabilities, especially in the area of distributed storage, would benefit the entire grid in many aspects. Figure H-3 shows the ES diagram, and Table H-3 lists the associated ES logical interfaces by category.

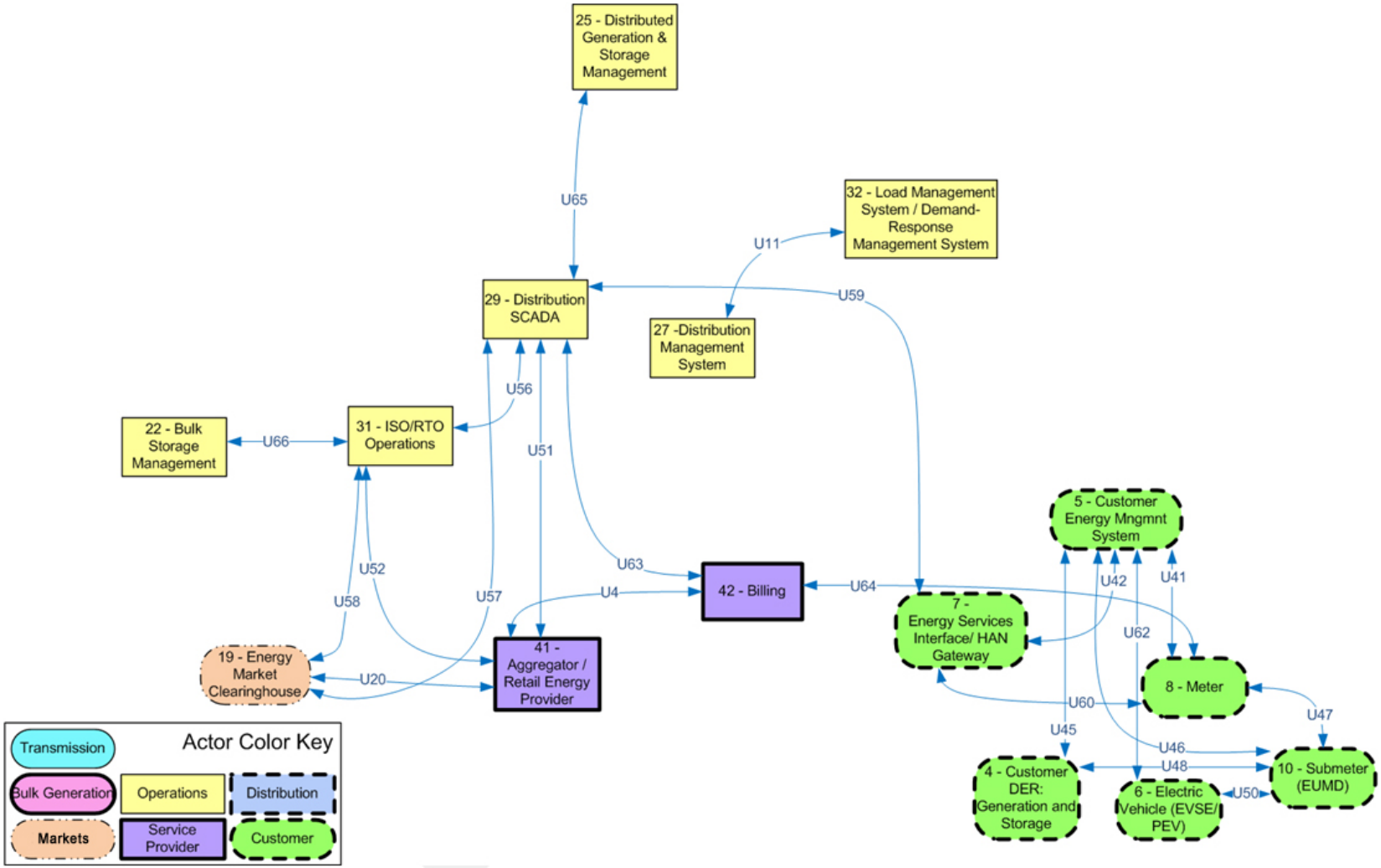


Figure 10-3 Electric Storage

3859 **Table 10-3 ES Logical Interfaces by Logical Interface Category**

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant	None
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	
5. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	U65, U66
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U56
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U63
8. Interface between back office systems not under common management authority, for example: • Between a third-party billing system and a utility meter data management system	None
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U4, U20, U51, U57, U58
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U59
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	None
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None

Logical Interface Category	Logical Interfaces
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	None
14. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U42, U45, U62
16. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U19
17. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	None
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U41, U46, U47, U48, U50, U64
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
20. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	None
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
22. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	None

H.4 ELECTRIC TRANSPORTATION

Electric transportation (ET) refers primarily to enabling large-scale integration of PEVs. Electric transportation will significantly reduce U.S. dependence on foreign oil, increase the use of renewable sources of energy, and dramatically reduce the nation's carbon footprint. Figure H-4 and Table H-4 address the ET logical interfaces.

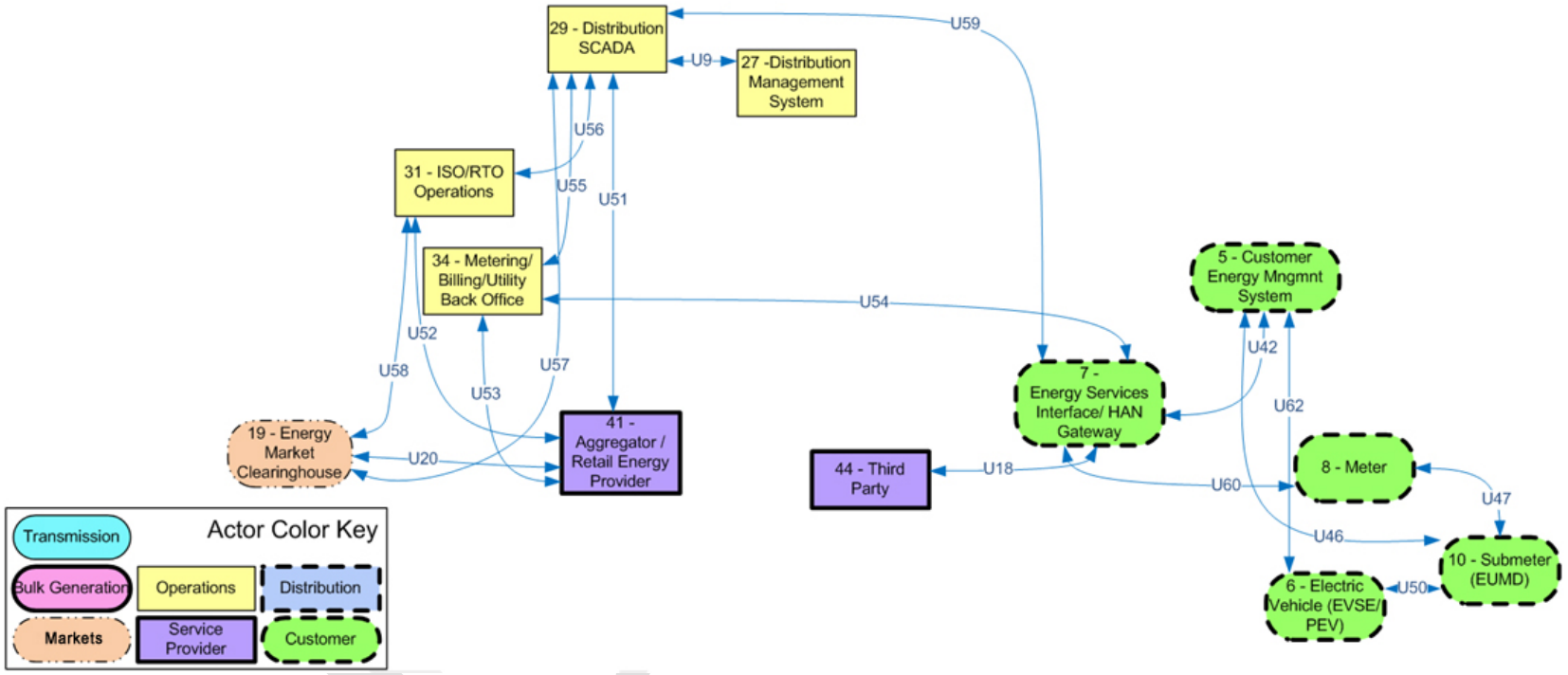


Figure 10-4 Electric Transportation

3873 **Table 10-4 ET Logical Interfaces by Logical Interface Category**

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant	None
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	
5. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	None
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U56
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	None
8. Interface between back office systems not under common management authority, for example: • Between a third-party billing system and a utility meter data management system	U55
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U20, U51, U52, U53, U57, U58
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U59
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	None

Logical Interface Category	Logical Interfaces
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	None
14. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U62
16. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U18, U19
17. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	None
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U46, U47, U50, U54, U60
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
20. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	None
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
22. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	None

3874
3875

H.5 CUSTOMER PREMISES

The customer premises address demand response (DR) and consumer energy efficiency. This includes mechanisms and incentives for utilities, business, industrial, and residential customers to cut energy use during times of peak demand or when power reliability is at risk. Demand response is necessary for optimizing the balance of power supply and demand. Figure H-5 diagrams the customer premises and Table H-5 provides the companion list of customer premises.

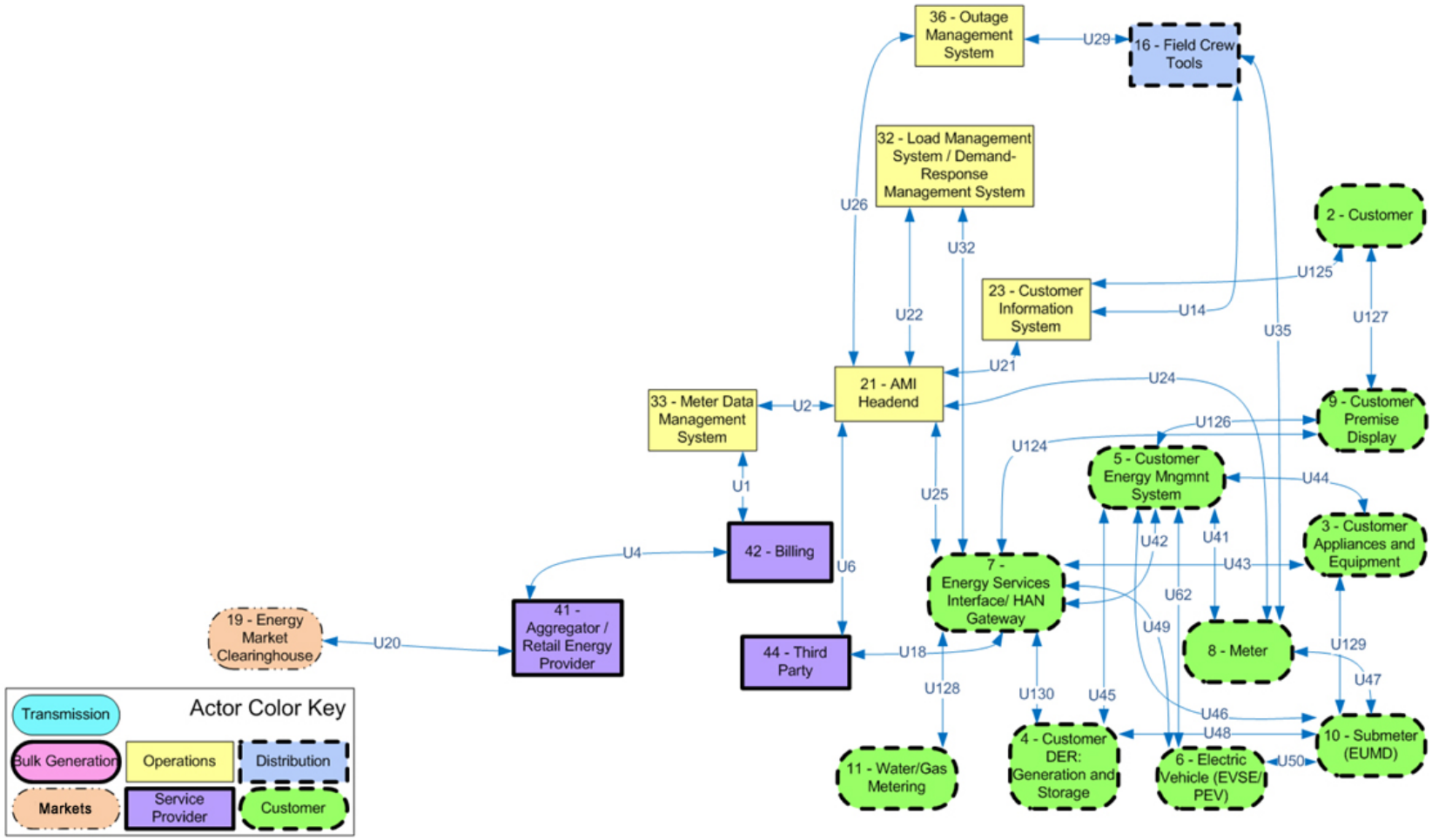


Figure 10-5 Customer Premises

3888 **Table 10-5 Customer Premises by Logical Interface Category**

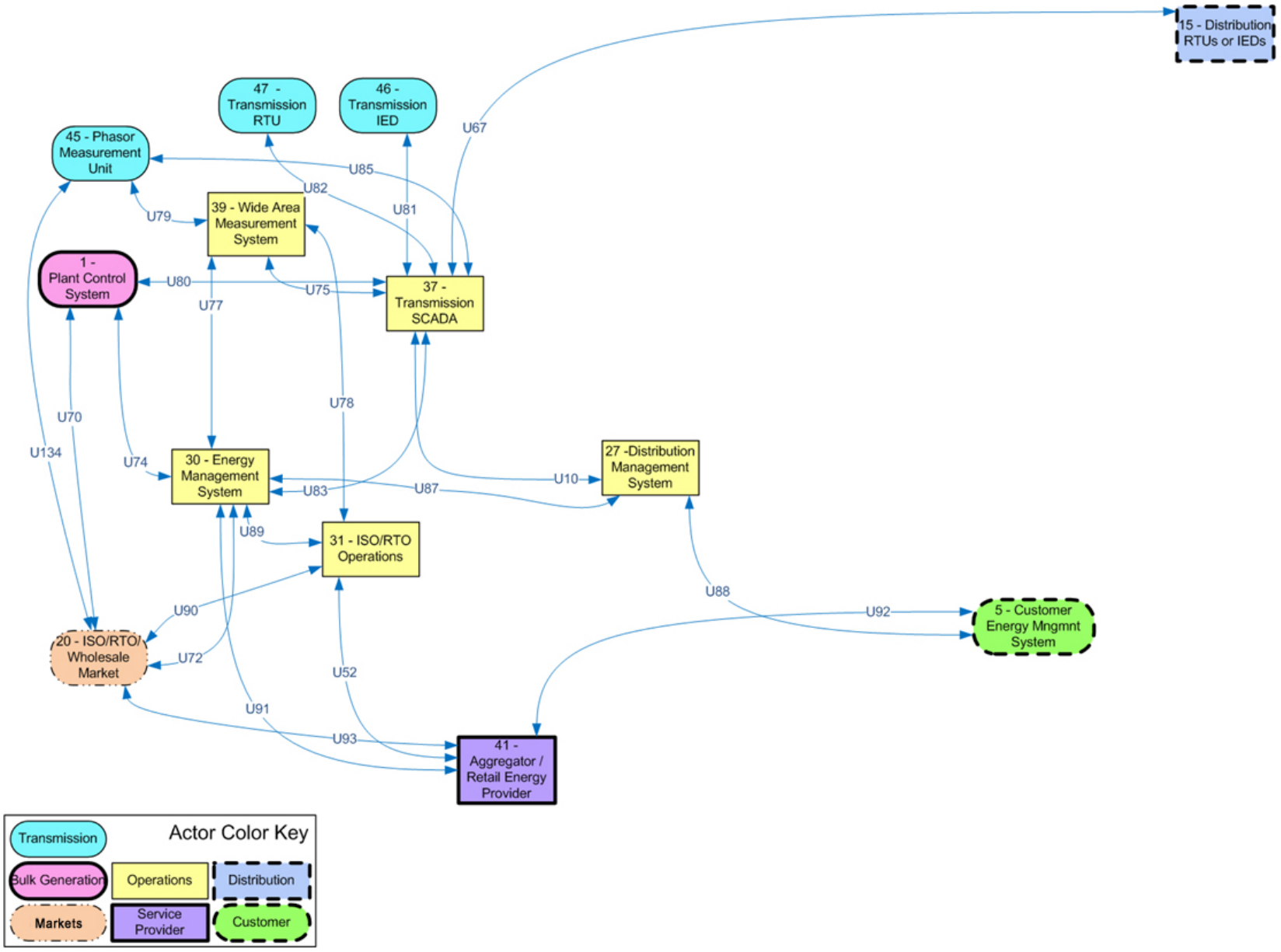
Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant	None
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	
5. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	None
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	none
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U2, U22, U26
8. Interface between back office systems not under common management authority, for example: • Between a third-party billing system and a utility meter data management system	U1
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U4, U20
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	None
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	None
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None

Logical Interface Category	Logical Interfaces
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U25, U32, U130
14. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U42, U43, U44, U45, U49, U62, U124, U126, U127
16. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U18, U19, U125
17. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	U14, U29, U35
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U24, U41, U46, U47, U48, U50, U128, U129
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	None
20. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	None
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
22. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	None

3889
3890

H.6 WIDE AREA SITUATIONAL AWARENESS

Wide area situational awareness (WASA) includes the monitoring and display of power system components and performance across interconnections and over large geographic areas in near real time. The goals of situational awareness are to understand and ultimately optimize the management of power-network components, behavior, and performance, as well as to anticipate, prevent, or respond to problems before disruptions can arise. Figure H-6 shows the diagram for the WASA logical interfaces and associated Table H-6 lists the logical interfaces by category.



3898
3899

Figure 10-6 Wide Area Situational Awareness

3900 **Table 10-6 WASA Logical Interfaces by Logical Interface Category**

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant	U67, U79, U81, U82, U85
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	
5. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	None
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U10, U74, U80, U83, U87
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	None
8. Interface between back office systems not under common management authority, for example: • Between a third-party billing system and a utility meter data management system	None
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U72, U93
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U75, U91
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	None

Logical Interface Category	Logical Interfaces
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	None
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	None
14. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	None
16. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U88, U92
17. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	None
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	None
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	U77, U78
20. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	None
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	None
22. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	None

3901

APPENDIX I
ANALYSIS MATRIX OF LOGICAL INTERFACE CATEGORIES

A set of Smart Grid key attributes was defined and allocated to each logical interface category. These key attributes included requirements and constraints that were used in the selection of security requirements for the logical interface category.

This analysis was one of the tools that was used in the determination of the CI&A impact levels for each logical interface category and in the selection of security requirements. The attribute table was used as a guide for selecting unique technical requirements and determining the impact level for confidentiality, integrity, and availability. The set of attributes allocated to each logical interface category is not intended to be a comprehensive set, or to exclude interfaces that do not include that attribute. For example, a Smart Grid information system may include logical interface category 1, but not ATR-11, legacy information protocols. The goal was to define typical attributes for each logical interface category.

Table I-1 provides additional descriptions of each attribute.

Table I-1 Interface Attributes and Descriptions

Interface Attributes	Descriptions
ATR-1a: Confidentiality requirements	Strong requirement that information should not be viewed by unauthorized entities
ATR-1b: Privacy concerns	Strong requirement that information should not be viewed by unauthorized entities
ATR-2: Integrity requirements	Strong requirement that information should not be modified by unauthorized entities, and should be validated for accuracy and errors. Higher level integrity may require additional technical controls.
ATR-3: Availability requirements	Strong requirement that information should be available within appropriate time frames. Often this necessitates redundancy of equipment, communication paths, and or information sources.
ATR-4: Low bandwidth of communications channels	Severely-limited bandwidth may constrain the types of security technologies that should be used across an interface while still meeting that interface's performance requirements.
ATR-5: Microprocessor constraints on memory and compute capabilities	Severely-limited memory and/or compute capabilities of a microprocessor-based platform may constrain the types of security technologies, such as cryptography, that may be used while still allowing the platform to meet its performance requirements.
ATR-6: Wireless media	Wireless media may necessitate specific types of security technologies to address wireless vulnerabilities across the wireless path.
ATR-7: Immature or proprietary protocols	Immature or proprietary protocols may not be adequately tested either against inadvertent compromises or deliberate attacks. This may leave the interface with more vulnerabilities than if a more mature protocol were used.

Interface Attributes	Descriptions
ATR-8: Inter-organizational interactions	Interactions which cross organizational domains, including the use of out-sourced services and leased networks, can limit trust and compatibility of security policies and technologies. Therefore, these vulnerabilities should be taken into account.
ATR-9: Real-time operational requirements with low tolerance for latency problems	Real-time interactions may entail short acceptable time latencies, and may limit the security technology choices for mitigating on-going attacks.
ATR-11: Legacy communication	Older communication technologies may limit the types, thoroughness, or effectiveness of different security technologies which may be employed. This sensitivity to security technologies should be taken into account.
ATR-10: Legacy end-devices and systems protocols	Older end-devices and protocols may constrain the types, thoroughness, or effectiveness of different security technologies which may be employed.
ATR-12: Insecure, untrusted locations	Devices or systems in locations which cannot be made more secure due to their physical environment or ownership, pose additional security challenges. For instance, hardware-based cryptography may be necessary.
ATR-13: Key management for large numbers of devices	Key management for large numbers of devices without direct access to certificate management may limit the methods for deploying, updating, and revoking cryptographic keys.
ATR-14: Patch and update management constraints for devices including scalability and communications	Patch management constraints may limit the frequency and processes used for updating security patches.
ATR-15: Unpredictability, variability, or diversity of interactions	Unpredictable interactions may complicate the decisions on the types and severity of security threats and their potential impacts
ATR-16: Environmental and physical access constraints	Access constraints may limit the types of security technologies that could be deployed. For instance, if appliances are in a customer's house, access could be very limited.
ATR-17 Limited power source for primary power	Devices with limited power, such as battery-run appliances which "go to sleep" between activities, may constrain the types of security technologies to those that do not require continuous power.
ATR-18: Autonomous control	Autonomous control of devices that may not be centrally monitored could lead to undetected security threats.

Table I-2 provides the analysis matrix of the security-related logical interface categories (rows) against the attributes (ATR) that reflect the interface categories (columns).

3921 **Table I-2 Analysis Matrix of Security-Related Logical Interface Categories, Defined by Attributes**

Attributes / Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17 Limited power source for primary power	ATR-18: Autonomous control
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints			X	X	X	X	X	X		X	X	X	X	X	X		X		X
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints			X		X	X	X	X		X	X	X	X	X	X		X	X	X

Attributes / Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17 Limited power source for primary power	ATR-18: Autonomous control
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints			X	X			X	X		X	X	X	X	X	X		X		X
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints			X				X	X		X	X	X	X	X	X	X	X		X
5. Interface between control systems within the same organization			X	X						X		X			X				X
6. Interface between control systems in different organizations			X	X					X	X		X			X				

Attributes / Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17 Limited power source for primary power	ATR-18: Autonomous control
7. Interface between back office systems under common management authority	X	X	X												X				
8. Interface between back office systems not under common management authority	X	X	X						X						X				
9. Interface with B2B connections between systems usually involving financial or market transactions	X	X	X	X					X	X						X			
10. Interface between control systems and non-control/ corporate systems	X	X	X	X				X	X						X	X			

Attributes / Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17 Limited power source for primary power	ATR-18: Autonomous control
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements					X	X	X	X		X	X	X	X				X	X	
12. Interface between sensor networks and control systems			X		X	X	X	X		X	X	X		X			X	X	X
13. Interface between systems that use the AMI network	X	X	X		X	X	X	X	X				X	X	X	X	X		
14. Interface between systems that use the AMI network for functions that require high availability	X	X	X	X	X	X	X	X	X				X	X	X	X	X		

Attributes / Logical Interface Categories	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17 Limited power source for primary power	ATR-18: Autonomous control
15. Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs	X	X	X	X		X	X	X	X	X			X	X		X	X		X
16. Interface between external systems and the customer site	X	X	X			X		X	X				X	X		X			
17. Interface between systems and mobile field crew laptops/equip-ment			X	X	X		X	X					X	X	X		X		
18. Interface between metering equipment	X	X	X		X	X	X	X	X		X	X	X	X	X		X		

Logical Interface Categories \ Attributes	ATR-1a: Confidentiality requirements	ATR-1b: Privacy concerns	ATR-2: Integrity requirements	ATR-3: Availability requirements	ATR-4: Low bandwidth of communications channels	ATR-5: Microprocessor constraints on memory and compute capabilities	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8: Inter-organizational interactions	ATR-9: Real-time operational requirements with low tolerance for latency problems	ATR-10: Legacy end-devices and systems	ATR-11: Legacy communication protocols	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large numbers of devices	ATR-14: Patch and update management constraints for devices including scalability and communications	ATR-15: Unpredictability, variability, or diversity of interactions	ATR-16: Environmental and physical access constraints	ATR-17 Limited power source for primary power	ATR-18: Autonomous control
19. Interface between operations decision support systems			X	X					X	X									
20. Interface between engineering/ maintenance systems and control equipment			X		X	X					X	X	X	X	X		X		
21. Interface between control systems and their vendors for standard maintenance and service			X						X				X	X	X		X		
22. Interface between security/network/ system management consoles and all networks and systems	X	X	X	X						X	X	X		X	X	X	X		

APPENDIX J
MAPPINGS TO THE HIGH-LEVEL SECURITY REQUIREMENTS

J.1 R&D TOPICS

The following table is a mapping of research and development topics [See §8] to the High-Level Security Requirements Families.

Table J-1 Mapping of R&D Topics to the High-Level Requirements Families

		Smart Grid Security Requirements Families																	
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Device Level	Improve Cost - Effective Higher Tamper Resistant & Survivable Device Architectures					X		X										X		
	Intrusion Detection with Embedded Processors			X				X					X			X				
Novel Mechanisms	Topics in Cryptographic Key Management			X			X			X							X	X		

		Smart Grid Security Requirements Families																		
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
	Advanced Topics in Cryptography									X							X	X		
Systems Level Topics	Scalability				X												X	X		X
	Architecting for bounded recovery and reaction					X		X					X			X				X
	Architecting Real-time security	X					X								X		X	X		
	Calibrating assurance and timeliness trade-offs		X										X		X	X				
	Legacy system integration				X												X		X	X
	Resiliency Management and Decision Support		X	X		X		X					X			X				
	Efficient Composition of Mechanisms																X			

		Smart Grid Security Requirements Families																		
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
	Risk Assessment and Management				X	X		X						X	X	X				
Networking	Safe use of COTS/Publicly Available Systems and Networks																X			
	Advanced Networking																X			
	IPv6																X		X	X
Other Security Issues in the Smart Grid Context	Privacy and Access Control in Federated Systems	X		X			X													
	Auditing and Accountability			X																
	Infrastructure Interdependency Issues					X		X					X			X				
	Cross-Domain (Power/Electrical					X		X					X			X				

		Smart Grid Security Requirements Families																		
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Other Security Issues in the Smart Grid Context	to Cyber/Digital) Security Event Detection, Analysis, and Response																			
	Covert Channels in the Smart Grid: Creation, Characterization, Detection and Elimination					X		X									X			
	DoS/DDoS Resiliency	X				X	X	X									X	X		
	Cloud Security	X					X		X	X							X			
	Security Design & Verification Tools (SD&VT)				X															X
	Distributed versus Centralized security	X			X	X	X	X							X		X	X	X	
	System Segmentation and Virtualization	X			X					X							X	X		X

		Smart Grid Security Requirements Families																	
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
	Vulnerability Research	X	X		X		X			X	X	X		X			X	X	X	X
	Vulnerability Research Tools	X			X		X			X	X	X		X			X	X		X
	Data Provenance			X	X		X			X							X	X		X
	Security and Usability		X												X	X				
	Cybersecurity Issues for Electric Vehicles	X		X			X			X							X	X		X
	Detecting Anomalous Behavior Using Modeling			X	X			X									X	X		

3928
3929

J.2 VULNERABILITY CLASSES

The following is a mapping of vulnerability classes [See §6] to the High-Level Security Requirements Families.

Table J-2 Mapping of Vulnerability Classes to High-Level Security Requirements Families

			Smart Grid Security Requirements Families																	
			Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
People, Policy and Procedure	Training	Insufficient Trained Personnel		X			X		X							X					
		Inadequate Security Training and Awareness Program		X			X		X							X					
	Policy and Procedure	Insufficient Identity Validation, Background Checks	X					X				X	X			X					X
		Inadequate Security Policy	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
		Inadequate Privacy Policy													X	X					
		Inadequate Patch Management Process	X			X	X	X	X							X			X	X	
		Inadequate Change and Configuration Management				X										X				X	

			Smart Grid Security Requirements Families																	
			Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
People, Policy and Procedure		Unnecessary System Access	X			X		X			X	X	X			X					
	Risk Management	Inadequate Periodic Security Audits			X											X					
		Inadequate Security Oversight by Management		X	X							X	X		X	X					
		Inadequate Continuity of Operations or Disaster Recovery Plan					X							X	X	X	X				
		Inadequate Risk Assessment Process														X					
		Inadequate Incident Response Process				X			X				X	X		X	X				
		Code Quality Vulnerability		X								X				X		X	X	X	X
		Authentication Vulnerability		X	X			X								X			X	X	X
		Authorization Vulnerability		X	X			X								X			X	X	X

			Smart Grid Security Requirements Families																	
			Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Platform Software/ Firmware Vulnerabilities	Software Development	Cryptographic Vulnerability		X												X				X	X
		Environmental Vulnerability	X	X				X				X				X		X		X	X
		Error Handling Vulnerability		X												X			X	X	X
		Business Logic Error		X												X				X	X
		Input and Output Validation		X												X			X	X	X
		Logging and Auditing Vulnerability		X				X								X				X	X
		Password Management Vulnerability	X	X				X								X				X	X
		Path Vulnerability		X												X				X	X
		Protocol Errors		X												X				X	X
		Range and Type Error Vulnerability		X												X				X	X

			Smart Grid Security Requirements Families																	
			Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Platform Software/ Firmware Vulnerabilities	Software Development	Sensitive Data Protection Vulnerability		X						X						X				X	X
		Session Management Vulnerability		X												X				X	X
		Concurrency, Synchronization and Timing Vulnerability		X												X				X	X
		Insufficient Safeguards for Mobile Code		X												X				X	X
		Buffer Overflow		X												X				X	X
		Mishandling of Undefined, Poorly Defined, or "Illegal" Conditions		X												X				X	X
		Use of Insecure Protocols		X												X		X		X	X
		Weakness that Affect Files and Directories		X												X				X	X

			Smart Grid Security Requirements Families																		
			Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Platform Vulnerabilities	API Usage & Implementation	API Abuse		X												X				X	X
		Use of Dangerous API		X												X				X	X
	Design	Use of Inadequate Security Architecture and Designs	X	X	X		X	X	X			X		X		X	X	X	X	X	X
		Lack of External or Peer Review for Security Design	X	X	X		X	X	X			X		X		X	X	X	X	X	X
	Implementation	Whitelisting			X	X															X
		File Integrity Monitoring								X	X								X	X	X
		Inadequate Malware Protection		X	X		X		X					X			X	X	X	X	
		Installed Security Capabilities Not Enables by Default	X	X	X	X		X						X			X	X	X	X	
		Absent or Deficient Equipment Implementation	X	X	X	X		X						X		X	X	X		X	

			Smart Grid Security Requirements Families																		
			Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
		Guidelines																			
	Operational	Lack of Prompt Security Patches from Software Vendors			X		X		X									X	X	X	
		Unneeded Services Running		X	X	X								X			X	X	X	X	
		Insufficient Log Management	X	X	X	X	X	X	X		X			X			X	X	X	X	
	Poorly configured security equip.	Inadequate Anomaly Tracking	X	X	X		X	X	X			X	X	X			X	X	X	X	
Network		Inadequate Integrity Checking				X									X	X			X	X	X
		Inadequate Network Segregation				X									X			X	X	X	X
		Inappropriate Protocol Selection				X									X	X		X	X	X	X

		Smart Grid Security Requirements Families																	
		Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
	Weakness in Authentication Process or Authentication Keys				X														X	X
	Insufficient Redundancy	X			X		X				X	X		X	X					X
	Physical Access to the Device	X			X		X				X	X		X	X				X	X

3933

J.3 BOTTOM-UP TOPICS

The following is a mapping of topics identified in the Bottom-up chapter [See §7] to the High-Level Security Requirements Families.

Table J-3 Mappling of Bottom-Up Topics to the High-Level Security Requirements Families

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Openness and Accessibility of Smart Grid Standards														X					
Authenticating and Authorizing Users to Substation IEDs						X													
Authenticating and Authorizing Users to Outdoor Field Equipment						X													
Authenticating and Authorizing Maintenance Personnel to Meters						X													
Authenticating and Authorizing Consumers to Meters						X													
Authenticating Meters to/from AMI Head Ends						X													
Authenticating HAN Devices to/from HAN Gateways						X													

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Authenticating Meters to/from AMI Networks						X													
Securing Serial SCADA Communications																X			
Securing Engineering Dial-up Access																X			
Secure End-to-End Meter to Head End Communication																X			
Access Logs for IEDs			X																
Remote Attestation of Meters																X	X		X
Protection of Routing Protocols in AMI Layer 2/3 Networks																X	X		
Key Management for Meters																X			
Protection of Dial-up Meters																X			
Outsourced WAN Links																X			
Insecure Firmware Updates																	X	X	
Side Channel Attacks on Smart Grid Field Equipment						X										X			
Securing and Validating Field Device Settings	X					X										X			

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Absolute & Accurate Time Information			X			X										X			
Security Protocols																			
Synchrophasors																			
Certificates																			
Event Logs and Forensics																			
Personnel Issues In Field Service Of Security Technology																			
Weak Authentication of Devices In Substations						X					X								
Weak Security for Radio-Controlled Distribution Devices						X										X			
Weak Protocol Stack Implementations																X			
Insecure Protocols																			
License Enforcement Functions																			
IT vs. Smart Grid Security																			
Patch Management																	X		

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Authentication	X			X		X													
System Trust Model																X			
User Trust Model																X			
Security Levels																			
Distributed vs. Centralized Model of Management																			
Local Autonomy of Operation																			
Intrusion Detection for Power Equipment				X		X											X		
Network and System and Management for Power Equipment	X			X		X											X		
Security Event Management					X		X										X		X
Cross-Utility / Cross-Corporate Security																			
Trust Management																			
Management of Decentralized Security Controls																			
Password Management	X					X													
Cipher Suite																X			

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Authenticating Users to Control Center Devices and Services						X													
Authentication of Devices to Users						X													
Entropy																			
Tamper Evidence	X										X					X			
Challenges with Securing Serial Communications																			
Legacy Equipment with Limited Resources																X		X	X
Costs of Patch and Applying Firmware Updates	X	X		X		X					X						X		
Forensics and Related Investigations			X		X		X										X		
Roles and Role Based Access Control	X					X													
Limited Sharing of Vulnerability and/or Incident Information														X					
Data Flow Control Vulnerability Issues																			

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Use of Shared/Dedicated and Public/Private Cyber Resources																			
Traffic Analysis						X										X	X		
Poor Software Engineering Practices																	X		
Attribution of Faults to the Security System																			
Need for Unified Requirements Model																			
Broad Definition of Availability																			
Utility Purchasing Practices																		X	
Cyber Security Governance																			
Key Management Issues																			
Summarized Issues with PKI																			
Key Management Systems for Smart Grid																X			
Computational Constraints																			

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Channel Bandwidth																			
Connectivity																			
Certificate Life Cycles																X			
Local Autonomy of Operation																			
Availability																			
Trust Roots																			
Algorithms and Key Lengths																			
Selection and Use of Cryptographic Techniques																X			
Elliptic Curve Cryptography (ECC)														X					
Break Glass Authentication																			
Cryptographic Module Upgradeability																			
Password Complexity Rules	X					X													
Authentication						X													
Network Access Authentication and Access Control	X					X													

	Access Control (SG.AC)	Awareness and Training (SG.AT)	Audit and Accountability (SG.AU)	Configuration Management (SG.CM)	Continuity of Operations (SG.CP)	Identification and Authentication (SG.IA)	Incident Response (SG.IR)	Information and Document Management (SG.ID)	Media Protection (SG.MP)	Personnel Security (SG.PS)	Physical and Environmental Security (SG.PE)	Strategic Planning (SG.PL)	Security Assessment and Authorization (SG.CA)	Security Program Management (SG.PM)	Planning (SG.PL)	Smart Grid Information System and Communication Protection (SG.SC)	Smart Grid Information System and Information Integrity (SG.SI)	Smart Grid Information System and Services Acquisition (SG.SA)	Smart Grid Information System Development and Maintenance (SG.MA)
Random Number Generation & Entropy																			
Single Sign On (SSO)																			

3937

3938

APPENDIX K
GLOSSARY AND ACRONYMS

3DES	Triple Data Encryption Standard (168 Bit)
AAA	Authentication, Authorization, and Accounting
Active Directory	A technology created by Microsoft that provides a variety of network services and is a central component of the Windows Server platform. The directory service provides the means to manage the identities and relationships that make up network environments.
ADA	Americans with Disabilities Act
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AGA	American Gas Association
AGC	Automatic Generation Control. A standalone subsystem that regulates the power output of electric generators within a prescribed area in response to changes in system frequency, tie-line loading, and the relation of these to each other. This maintains the scheduled system frequency and established interchange with other areas within predetermined limits.
Aggregation	Practice of summarizing certain data and presenting it as a total without any PII identifiers
AICPA	American Institute of Certified Public Accountants. The national, professional organization for all Certified Public Accountants.
AMI	Advanced Metering Infrastructure
AMI-SEC	AMI Security [Task Force]
Anonymize	• To organize data in such a way as to preserve the anonymity or hide the personal identity of the individual(s) to whom the data pertains • A process of transformation or elimination of PII for purposes of sharing data
ANSI	American National Standards Institute
API	Application Programming Interface
ASAP-SG	Advanced Security Acceleration Project – Smart Grid
ASTM	American Society for Testing and Materials
Asymmetric cipher	Cryptography solution in which separate keys are used for encryption and decryption, where one key is public and the other is private.
ATR	Attribute
B2B	Business to Business
BAN	Building Area Network
BEM	Building Energy Management

Block cipher	A symmetric key cipher operating on fixed-length groups of bits, called blocks, with an unvarying transformation—in contrast to a stream cipher, which operates on individual digits one at a time and whose transformation varies during the encryption. A block cipher, however, can effectively act as a stream cipher when used in certain modes of operation.
Botnet	Robot Network. A large number of compromised computers also called a "zombie army," that can be used to flood a network with messages as a denial of service attack. A thriving botnet business consists in selling lists of compromised computers to hackers and spammers.
C&I	Commercial and Industrial
CA	Certificate Authority
CALEA	Communications Assistance for Law Enforcement Act
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing
CBC	Cipher Block Chaining
CEC	California Energy Commission
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CHP	Combined Heat and Power
CI&A	Confidentiality, Integrity, and Availability
CIM	Common Information Model. A structured set of definitions that allow different Smart Grid domain representatives to communicate important concepts and exchange information easily and effectively.
CIMA	Chartered Institute of Management Accountants
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPA	Children's Internet Protection Act
CIS	Cryptographic Interoperability Strategy
CIS	Customer Information System
CISO	Chief Information Security Officer
CMMS	Computer-based Maintenance Management Systems
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSCTG	Cyber Security Coordination Task Group
CSO	Chief Security Officer
CSP	Critical Security Parameters
CSR	Certificate Signing Request

CSR	Customer Service Representative
CSSWG	Control Systems Security Working Group
CSWG	Cyber Security Working Group
CRT	Cathode Ray Tube
CTR mode	Counter mode. A block cipher mode of operation also known as Integer Counter Mode (ICM) and Segmented Integer Counter (SIC) mode.
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DA	Distribution Automation
DARPA	Defense Advanced Research Projects Agency
DCS	Distributed Control System. A computer-based control system where several sections within the plants have their own processors, linked together to provide both information dissemination and manufacturing coordination.
DDoS	Distributed Denial of Service
De-identify	A form of anonymization that does not attempt to control the data once it has had PII identifiers removed, so it is at risk of re-identification.
DER	Distributed Energy Resources
DES	Data Encryption Standard
DEWG	Domain Expert Working Group
DFR	Digital Fault Recorder
DGM	Distribution Grid Management
DHS	Department of Homeland Security
Diffie-Hellman	A cryptographic key exchange protocol first published by Whitfield Diffie and Martin Hellman in 1976. It allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
Distinguished names	String representations that uniquely identify users, systems, and organizations.
DMS	Distribution Management System
DN	Distinguished Name
DNP	Distributed Network Protocol
DNS	Domain Name Service
DoD	Department of Defense
DOE	Department of Energy
DoS	Denial of Service
DR	Demand Response
DRBG	Deterministic Random Bit Generators

DRM	Digital Rights Management. A generic term for access control technologies used by standards providers, publishers, copyright holders, manufacturers, etc. to impose limitations on the usage of digital content and devices. The term is used to describe any technology that inhibits the use of digital content in a manner not desired or intended by the content provider.
DRMS	Distribution Resource Management System
DSL	Digital Subscriber Line
DSPF	Distribution System Power Flow
DSS	Digital Signature Standard
EAP	Extensible Authentication Protocol
EAX mode	• A mode of operation for cryptographic block ciphers. It is an AEAD algorithm designed to simultaneously provide both authentication and privacy of the message with a two-pass scheme, one pass for achieving privacy and one for authenticity for each block. • A mixed authenticated encryption mode of operation of a block cipher in order to reduce the area overhead required by traditional authentication schemes.
EAX'	A modification of the EAX mode used in the ANSI C12.22 standard for transport of meter-based data over a network.
ECC	Elliptic Curve Cryptography (encryption)
ECDH	Elliptic Curve Diffie-Hellman. A key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel.
ECDSA	Elliptic Curve Digital Signature Algorithm
ECPA	Electronic Communications Privacy Act
EEO	Equal Employment Opportunity
EEPROM	Electrically Erasable Programmable Read-Only Memory
EISA	Energy Independence and Security Act
EKU	Extended Key Usage
EMS	Energy Management System
EMSK	Extended Master Session Key
Entropy	In the case of transmitted messages, a measure of the amount of information that is missing before reception.
Ephemeral Unified Model	A ECDH scheme where each party generates an ephemeral key pair to be used in the computation of the shared secret.
EPIC	Electronic Privacy Information Center
EPRI	Electric Power Research Institute
EPSA	Electric Power Supply Association
ES	Electric Storage
ESI	Energy Services Interface

ESP	Energy Service Provider
ET	Electric Transportation
EUMD	End Use Measurement Device
EV	Electric Vehicle
EV/PHEV	Electric Vehicle/Plug-in Hybrid Electric Vehicles. Cars or other vehicles that draw electricity from batteries to power an electric motor. PHEVs also contain an internal combustion engine.
EvDO	Evolution Data Optimized
EVSE	Electric Vehicle Service Element
FACTA	Fair and Accurate Credit Transactions Act
FAQ	Frequently Asked Questions
FERC	Federal Energy Regulatory Commission
FERPA	Family Educational Rights and Privacy Act
FIPS	Federal Information Processing Standards
FIPS 140-2	Publication 140-2 is a U.S. government computer security standard used to accredit cryptographic modules. NIST issued the FIPS 140 Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware and software components.
FLIR	Fault Location, Isolation, Restoration
FTP	File Transfer Protocol
G&T	Generations and Transmission
GAPP	Generally Accepted Privacy Principles. Privacy principles and criteria developed and updated by the AICPA and Canadian Institute of Chartered Accountants to assist organizations in the design and implementation of sound privacy practices and policies.
GIC	Group Insurance Commission
GIS	Geographic Information System
GLBA	Gramm-Leach Bliley Act
GPRS	General Packet Radio Service
GPSK	Generalized Pre-Shared Key
Granularity	The extent to which a system contains separate components, e.g., the fineness or coarseness with which data fields are subdivided in data collection, transmission, and storage systems. The more components in a system, the more flexible it is. In more general terms, the degree to which a volume of information is finely detailed.
GRC	Governance, Risk, and Compliance
GWAC	GridWise Architecture Council

Hacker	In common usage, a hacker is a person who breaks into computers and/or computer networks, usually by gaining access to administrative controls. Proponents may be motivated by diverse objectives from the shear entertainment value they find in the challenge of circumventing computer/network security to political or other ends. Hackers are often unconcerned about the use of illegal means to achieve their ends. Out-and-out cyber-criminal hackers are often referred to as "crackers."
HAN	Home Area Network. A network of energy management devices, digital consumer electronics, signal-controlled or -enabled appliances, and applications within a home environment that is on the home side of the electric meter.
Hash	Any well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serve as an index to an array. The values returned by a hash function are called hash values, hash codes, hash sums, checksums, or simply hashes.
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HMAC	Hash Message Authentication Code
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
Hz	hertz
IBE	Identity-Based Encryption
ICS	Industrial Control Systems
ID	Identification
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFAC	International Federation of Accountants
IKE	Internet Key Exchange. Protocol used to set up a security association in the IPsec protocol suite.
INL	Idaho National Laboratory
IP	Internet Protocol
IPP	Independent Power Producer
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System

IPSec	Internet Protocol Security
IS	Information Security
ISA	International Society of Automation
ISAKMP	Internet Security Association and Key Management Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO	Independent System Operator
ISO/IEC27001	International Organization for Standardization/International Electrotechnical Commission Standard 27001. A auditable international standard that specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It uses a process approach for protection of critical information.
IT	Information Technology
ITGI	IT Governance Institute
ITL	Information Technology Laboratory
IVR	Interactive Voice Response
JNI	Java Native Interface
JTC	Joint Technical Committee
KDC	Key Distribution Center
KEK	Key Encryption Key
Kerberos	A computer network authentication protocol, developed by the Massachusetts Institute of Technology, which allows nodes communicating over a nonsecure network to prove their identity to one another in a secure manner. It is also a suite of free software published by MIT that implements this protocol.
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LMS	Load Management System
LTC	Load Tap Changer
MAC	Message Authentication Code
MAC address	Media Access Control address. The unique serial number burned into Ethernet and Token Ring adapters that identifies that network card from all others.
MAC protection	Message Authentication Code protection. In cryptography, a short piece of information used to authenticate a message. The MAC value protects data integrity and authenticity of the tagged message by allowing verifiers (who also possess the secret key used to generate the value) to detect any changes to the message content.
MDMS	Meter Data Management System

min	minute
MIT	Massachusetts Institute of Technology
MITM	Man in the Middle
ms	millisecond (10^{-3} second)
MTBF	Mean Time Before Failure
MW	megawatt (10^{6} watts)
NAN	Neighborhood Area Network
NERC	North American Electric Reliability Corporation
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NMAP	Networked Messaging Application Protocol
NRECA	National Rural Electric Cooperative Association
NSA	National Security Agency
NSA Suite B	A set of cryptographic algorithms promulgated by the National Security Agency to serve as an interoperable cryptographic base for both unclassified information and most classified information.
NSF	National Science Foundation
NVD	National Vulnerability Database
OCSP	Online Certificate Status Protocol
OE	Office of Electricity Delivery and Energy Reliability
OECD	Organisation for Economic Cooperation and Development. A global governmental forum of 30+ market democracies for comparison of policy experiences, good practices, and coordination of domestic and international policies. It is one of the world's largest and most reliable sources of comparable statistical, economic and social data.
OID	Object Identifier
OMS	Outage Management System
One-Pass Diffie-Hellman	A key-agreement scheme in which an ephemeral key pair generated by one party is used together with the other party's static key pair in the computation of the shared secret.
OWASP	Open Web Application Security Project
PANA	Protocol for carrying Authentication for Network Access
PAP	Priority Action Plan
PC	Personal Computer
PDA	Personal Digital Assistant
PDC	Phasor Data Concentrator

PE	Protocol Encryption
PE mode	• An encryption mode combining CTR mode and ECB mode developed for streaming SCADA messages. It relies on the SCADA protocol's ability to detect incorrect SCADA messages. • Position Embedding mode. A cryptographic mode designed specifically for low latency integrity protection on low-speed serial links.
Personal Information	Information that reveals details, either explicitly or implicitly, about a specific individual's household dwelling or other type of premises. This is expanded beyond the normal "individual" component because there are serious privacy impacts for all individuals living in one dwelling or premise. This can include items such as energy use patterns or other types of activities. The pattern can become unique to a household or premises just as a fingerprint or DNA is unique to an individual.
PEV	Plug-In Electric Vehicle
PFS	Perfect Forward Secrecy
PHEV	Plug In Hybrid Electric Vehicle
PIA	Privacy Impact Assessment. A process used to evaluate the possible privacy risks to personal information, in all forms, collected, transmitted, shared, stored, disposed of, and accessed in any other way, along with the mitigation of those risks at the beginning of and throughout the life cycle of the associated process, program or system.
PII	Personally Identifiable Information
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PKMv2	Privacy Key Management version 2
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PQ	Power Quality
Public-key cryptography	A cryptographic approach that involves the use of asymmetric key algorithms instead of or in addition to symmetric key algorithms. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver.
PUC	Public Utilities Commission
QoS	Quality of Service
R&D	Research and Development
RA	Registration Authority
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RBAC	Role-Based Access Control

Retail Access	Competitive retail or market-based pricing offered by energy services companies or utilities to some or all of their customers under the approval/regulation of state public utilities departments.
RF	Radio Frequency
RFC	Request for Comments
RNG	Random Number Generator
RP	Relying Party
RSA	Widely used in electronic commerce protocols, this algorithm for public-key cryptography is named for Rivest, Shamir, and Adleman who were first to publicly described it. This was the first algorithm known to be suitable for signing as well as encryption and represents a great advance in public key cryptography.
RSA algorithm	RSA is public key cryptography algorithm named for its co-inventors: Ron Rivest, Adi Shamir, and Len Adleman.
RTO	Regional Transmission Operator
RTP	Real-Time Pricing
RTU	Remote Terminal Unit
s	second
S/MIME	Secure/Multipurpose Internet Mail Extensions
SA	Security Association
SAM	Security Authentication Module
SCADA	Supervisory Control and Data Acquisition
SCE	Southern California Edison
SDLC	Software Development Life Cycle
SDO	Standard Developing Organization
SEL	Schweitzer Engineering Laboratories
SEM	Security Event Management
SEP	Smart Energy Profile
SGIP	Smart Grid Interoperability Panel
SGIP TWiki	An open collaboration site for the Smart Grid community to work with NIST in developing a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems and is part of a robust process for continued development and implementation of standards as needs and opportunities arise and as technology advances.
SGIP-CSWG	SGIP – Cyber Security Working Group
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard

Single sign-on	A property of access control of multiple, related, but independent software systems. With this property a user/device logs in once and gains access to all related systems without being prompted to log in again at each of them.
SNMP	Simple Network Management Protocol
Social Engineering	The act of manipulating people into performing actions or divulging confidential information. The term typically applies to trickery or deception being used for purposes of information gathering, fraud, or computer system access.
SP	Special Publication
SPOF	Signal Point of Failure
SSH	Secure Shell. A protocol for secure remote login and other secure network services over an insecure network.
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSL/TLS	Secure Socket Layer / Transport Layer Security
SSN	Social Security Number
SSO	Single Sign-On
SSP	Sector-specific Plans
Symmetric cipher	Cryptography solution in which both parties use the same key for encryption and decryption, hence the encryption key must be shared between the two parties before any messages can be decrypted.
T&D	Transmission and Distribution
T&D DEWG	T&D Domain Expert Working Group
TA	Trust Anchor
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TCPA	Telephone Consumer Protection Act
TCS	Trouble Call System
Telnet	Teletype network. A network protocol used on the Internet or local area networks to provide a bidirectional interactive communications facility. The term telnet may also refer to the software that implements the client part of the protocol.
TEMPEST	A codename referring to investigations and studies of conducted emissions. Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.
TLS	Transport Layer Security
TNC	Trusted Network Connect
TOCTOU	Time of Check, Time of Use

TPI	Two-Person Integrity
TRSM	Tamper Resistant Security Modules
Trust anchor	In cryptography, an authoritative entity represented via a public key and associated data. When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor. The public key (of the trust anchor) is used to verify digital signatures and the associated data.
TWiki	A flexible, open source collaboration and Web application platform (i.e., a structured Wiki) typically used to run a project development space, a document management system, a knowledge base, or any other groupware tool on an intranet, extranet, or the Internet to foster information flow between members of a distributed work group.
UCAIug	UtiliSec Working Group
UDP/IP	User Datagram Protocol/Internet Protocol
Upsell	Marketing term for the practice of suggesting higher priced products or services to a customer who is considering a purchase.
URL	Universal Resource Locator
USRK	Usage-Specific Root Key
Van Eck phreaking	Named after Dutch computer researcher Wim van Eck, phreaking is the process of eavesdropping on the contents of a CRT and LCD display by detecting its electromagnetic emissions. Because of its connection to eavesdropping, the term is also applied to exploiting telephone networks.
VAR	Volts-Amps-Reactive
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAMS	Wide Area Measurement System
WAN	Wide Area Network
WASA	Wide Area Situational Awareness
WG	Working Group
Wi-Fi	Term often used as a synonym for IEEE 802.11 technology. Wi-Fi is a trademark of the Wi-Fi Alliance that may be used with certified products that belong to a class of WLAN devices based on the IEEE 802.11 standards.
WiMAX	• Worldwide Interoperability for Microwave Access. A telecommunications protocol that provides fixed and fully mobile Internet access. • Wireless digital communications system, also known as IEEE 802.16, which is intended for wireless "metropolitan area networks."
WLAN	Wireless Local Area Network
WMS	Work Management System
XML	Extensible Markup Language

3941

3942

APPENDIX L
SGIP-CSWG AND SGIP 2.0-SGCC MEMBERSHIP

This list is a combination of all participants in the Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP–CSWG, including all of the subgroups) and the SGIP 2.0 Smart Grid Cybersecurity Committee. Some of the organizations listed have changed over time, but these reflect the organizational affiliation of the members during their time of membership.

Name	Organization
Aber, Lee	OPOWER
Ackerman, Eric	Edison Electric Institute
Ahmad, Wadji	General Electric
Ahmadi, Mike	GraniteKey
Ahsan, Naeem	DNV KEMA Energy and Sustainability
Aikman, Megan	FERC
Akyol, Bora	Pacific Northwest National Laboratory
Alcaraz, Cristina	NIST
Alexander, Michael	Underwriters Laboratories Inc.
Alexander, Rob	Ember Corporation
Alexander, Roger	Eka Systems, Inc.
Allitt, Ed	IPKeys
Al-Mukdad, Wendy	California PUC
Alrich, Tom	ENCARI
Ambady, Balu	Sensus
Anderson, Casey	Tendril, Inc.
Anderson, Dwight	Schweitzer Engineering Labs
Anderson, Ken	Information and Privacy Commissioner's Office of Ontario
Andreou, Demos	Cooper Industries
Andrews, Joseph	Western Electricity Coordinating Council
Antonacopoulos, Glenn	Northrop Grumman Corp.
Arensman, Will	SouthWest Research Institute
Arneja, Vince	Arxan Technologies, Inc.
Artz, Sharla	Schweitzer Engineering Laboratories
Arunachalam, Arun	Southern California Edison
Ascough, Jessica	Harris Corporation
Ashton, Skip	Ember Corporation
Bacik, Sandy	Enernex
Baiba Grazdina	Duke Energy
Baker, Fred	Cisco Systems, Inc.
Balsam, John	Georgia Tech Research Institute
Banerjee, Aditi	Texas Instruments
Barber, Mitch	Industrial Defender, Inc.

Barclay, Steve	ATIS
Barnes, Frank	University of Colorado at Boulder
Barnett, Bruce	GE Global Research
Barr, Michael	L-3 Communications Nova Engineering
Bartol, Nadya	Utilities Telecom Council
Barton, Michael	SunPower Corporation
Bass, Len	Software Engineering Institute Carnegie Mellon University
Basu, Sourjo	General Electric Energy
Bates, Shirley	Siemens
Batz, David	Edison Electric Institute
Beale, Steven	Future of Privacy Forum
Behrens, Stephen	KEMA, Inc.
Beinert, Rolf	OpenADR
Belanger, Phil	Oak Tree Consulting
Belgi, Subodh	MIEL e-Security Private Limited
Bell, Ray	Grid Net
Bell, Will	Grid Net
Bemmel, Vincent	Trilliant
Bender, Klaus	Utilities Telecom Council
Benn, Jason	Hawaiian Electric Company
Benoit, Jacques	Cooper Power Systems
Berkowitz, Don	S&C Electric Company
Beroset, Ed	Elster Group
Berrett, Dan E.	DHS Standards Awareness Team (SAT)
Berrey, Adam	General Catalyst Partners
Bertholet, Pierre-Yves	Ashlawn Energy, LLC
Besko, Geoff	Seccuris, Inc.
Beyene, Tsegereda	Cisco Systems, Inc.
Bezecny, Steve	CenterPoint Energy
Bhaskar, Mithun M.	National Institute of Technology, Warangal
Biggs, Doug	Infogard
Biggs, Les	Infogard
Bilow, Steve	The Bilow Group
Bitter, David	SMUD
Blomgren, Paul	SafeNet Inc.
Blossom, Michael	SmartSynch
Bobba, Rakesh	University of Illinois, Urbana-Champaign
Bochman, Andy	IBM
Bockenek, Richard	Verizon
Boivie, Rick	IBM T. J. Watson Research Center
Boulez, Kris	Ascure

Brackney, Dick	Microsoft
Bradley, Steven	Virginia State Corporation Commission
Braendle, Markus	ABB
Branco, Carlos	Northeast Utilities
Brennan, Jim	New Hampshire PUC
Brent, Richard	FriiPwrLtd
Brenton, Jim	Ercot
Brewer, Tanya	NIST
Brigati, David	NitroSecurity
Brinskele, Ed	Vir2us Inc.
Brooks, Thurston	3e Technologies International, Inc.
Brown, Bobby	Consumers Energy / EnerNex Corporation
Brown, Peter	Progress Energy
Brozek, Mike	Westar Energy, Inc.
Brunnetto, Michael	
Bryan, Clifford	Examiner.com
Brydl, Jerry	Steffes Corporation
Bucciero, Joe	Buccerio Consulting
Buffo, Lydia	Dominion
Bump, William	Booz, Allen, Hamilton
Burnham, Laurie	Dartmouth College
Butler, Greg	
Butterworth, Jim	Guidance Software
Byrum, Drake	Cigital, Inc.
Camilleri, John	Green Energy Corp
Camm, Larry	Schweitzer Engineering Laboratories, Inc.
Campagna, Matt	Certicom Corp.
Cam-Winget, Nancy	Cisco Systems, Inc.
Caprio, Daniel	McKenna Long & Aldridge LLP
Cardenas, Alvaro A.	Fujitsu
Carlson, Chris	Puget Sound Energy
Carpenter, Matthew	
Cavoukian, Ann	Office of the Information and Privacy Commissioner of Ontario
Chan, Rida	Deloitte & Touche, LLP
Chaney, Mike	Securicon
Charbonneau, Sylvain	Hydro-Quebec
Chasko, Stephen	Landis+Gyr
Chason, Glen	EPRI
Chaudhry, Hina	Argonne National Labs
Chhabra, Rahul	Burns & McDonnell Engineering

Chibba, Michelle	Office of the Information and Privacy Commissioner of Ontario
Choubey, TN	Southern California Edison
Chow, Edward	U of Colorado at Colorado Springs
Chow, Richard	PARC
Chris Starr	General Dynamics
Christopher, Jason	FERC
Chudgar, Raj	Sungard
Chung, Raymond	National Technical Systems, Inc.
Churchill, Alex	Duke Energy
Cioni, Mark V.	MV Cioni Associates, Inc.
Clark, Jamie	OASIS
Claypoole, Ted	Womble Carlyle Sandridge & Rice, PLLC
Clements, Abraham	Sandia National Laboratories
Clements, Sam	Pacific Northwest National Laboratory
Cleveland, Frances	Xanthus Consulting International
Cohen, Michael	Mitre
Cohen, Yossi	
Collier, Albert	Alterium, LLC
Coney, Lillie	Electronic Privacy Information Center
Coomer, Mark	ITT Defense and Information Solutions
Coop, Mike	ThinkSmartGrid
Cornish, Kevin	Enspiria
Cortes, Sarah	Inman Technology IT
Cosio, George	Florida Power and Light
Cox, William	Cox Software Architects
Cragie, Robert	Jennic LTD
Crane, Melissa	Tennessee Valley Authority
Crljenica, Igor	State of Michigan
Cuen, Lita	LC RISQ & Associates
Cui, Stephen	Microchip Technology
Czaplewski, John	Northrup Grumman Corp.
Dagle, Jeff	Pacific Northwest National Laboratory
Dalva, Dave	Stroz Friedberg
Danahy, Jack	Bochman & Danahy Research
Danezis, George	Microsoft
Dangler, Jack	
Das, Subir	Applied Communication Sciences
Davis, Scott	Sensus
Davison, Brian	Public Utility Commission of Texas
De Petrillo, Nick	Industrial Defender
Delenela, Ann	Ercot

DeLoach, Tim	IBM Global Business Services
DePeppe, Doug	i2IS Cyberspace Solutions
di Sabato, Mark	
Dieffenbach, Dillon	Ernst & Young
Dienhart, Mary	Xcel Energy
Dierking, Tim	Aclara Power-Line Systems, Inc.
Dillon, Terry	APS
Dinges, Sharon	Trane
Dion, Thomas	Dept of Homeland Security
Do, Tam	Southwest Research Institute
Dodd, David	pbnetworks
Dodson, Greg	Dominion Resources Services, Inc.
Don-Arthur, George	Alterium LLC
Doreswamy, Rangan	Verisign, Inc.
Doring, Ernest	Pacific Gas & Electric
Dorn, John	Accenture
Dougherty, Steven	IBM
Downum, Wesley	Telcordia
Dransfield, Michael	National Security Agency
Drgon, Michele	DataProbity
Drozinski, Timothy	Florida Power & Light Company
Drummond, Rik	Drummond Group
Dubrawsky, Ido	Itron
Duffy, Paul	Cisco Systems
Duggan, Pat	ConEd
Dulaney, Mike	Arxan Technologies, Inc.
Dunfee, Rhonda	Department of Energy
Dunphy, Mary	
Dunton, Benjamin	NYS Department of Public Service
Dupper, Jeff	Ball Aerospace & Technologies
Duren, Michael	Protected Computing
Dutta, Prosenjit	Utilities AMI Practice
Earl, Frank	Earl Consulting
Eastham, Bryant	Panasonic Electric Works Laboratory of America (PEWLA)
Edgar, Tom	Pacific Northwest National Laboratory
Eggers, Matthew	U.S. Chamber of Commerce
Eigenhuis, Scott M	
Ellison, Mark	DTE Energy
Emelko, Glenn	ESCO
Engels, Mark	Dominion Resources Services, Inc.
Ennis, Greg	Wi-Fi Alliance

Enstrom, Mark	NeuStar
Eraker, Liz	Samuelson Clinic at UC Berkeley
Erickson, Dave	California Public Utility Commission
Ersue, Mehmet	Nokia Siemens Networks
Estefania, Maria	ATIS
Eswarahally, Shrinath	Infineon Technologies NA
Evans, Bob	Idaho National Laboratory
Ewing, Chris	Schweitzer Engineering Labs
Fabela, Ronnie	Lockheed Martin
Fabian, Michael	Wurldtech Security Technologies
Faith, Doug	MW Consulting
Faith, Nathan	American Electric Power
Famolari, David	Telcordia Technologies
Faure, Jean-Philippe	Progilon Co.
Fennell, Kevin	Landis+Gyr
Fenner, Philip	American Electric Power, Inc.
Fischer, Ted	Norwich University Applied Research Institutes (NUARI)
Fisher, Jim	Noblis
Fishman, Aryah	Edison Electric Institute
Fitzpatrick, Gerald	NIST
Flickinger, Derek	ThinkSmartGrid, LLC
Flowers, Tom	Control Center Solutions, LLC
Foglesong, Anna	Pacific Gas & Electric
Ford, Guy	New Hampshire Electric Cooperative
Foster, William	Lumi Wireless Technologies
Francis, Daniel	AEP
Franklin, Troy	FriiPwrLtd
Franz, Matthew	SAIC
Fraser, Barbara	Cisco
Fredebeil, Karlton	Tennessee Valley Authority
Frederick, Jennifer	Direct Energy
Fredrickson, Dan	Tendril Inc.
Freund, Mark	Pacific Gas and Electric Company
Friedman, Dan	
Frogner, Bjorn	
Fulford, Ed	
Fuloria, Shailendra	Cambridge University
Fulton, Joel	
Futch, Matt	IBM Energy and Utilities
Gailey, Mike	CSC
Galli, Stefano	ASSIA, Inc.

Garrard, Ken	Aunigma Network Solutions Corp.
Gassko, Irene	Florida Power & Light
Gaulding, Win	Northrop Grumman Information Systems
Gerber, Josh	San Diego Gas and Electric
Gerbino, Nick	Dominion Resources Services, Inc.
Gering, Kip	Itron
Gerney, Arkadi	OPOWER
Gerra, Arun	University of Colorado, Boulder
Ghansah, Isaac	California State University Sacramento
Gibbs, Derek	SmartSynch
Gilchrist, Grant	EnerNex
Gill, Jeff	RuggedCom Inc.
Gillmore, Matt	CMS Energy
Givens, Beth	Privacy Rights Clearinghouse
Glassey, Todd	Certichron Inc.
Glavin, Kevin	Cigital
Glenn, Bill	Westar Energy, Inc.
Goff, Ed	Progress Energy
Gokul, Jay	Technology Crest Corp.
Golla, Ramprasad	Grid Net
Gomez, Aaron	Drummond Group
Gonzalez, Efrain	Southern California Edison
Gooding, Jeff	Southern California Edison
Goodson, Paul	ISA
Gorog, Christopher	Atmel Corporation
Grainger, Steven	General Dynamics
Grazdina, Baiba	Duke Energy
Greenberg, Alan M.	
Greenfield, Neil	American Electric Power, Inc.
Greer, David	University of Tulsa
Griffin, Slade	Enernex
Grochow, Jerrold	MIT
Gulick, Jessica	SAIC
Gunter, Carl	U. of Illinois
Gupta, Rajesh	UC San Diego
Gupta, Sarbari	Electrosoft
Gutierrez, Julio	Florida Power & Light
Habre, Alex	PJM
Hague, David	
Halasz, Dave	Aclara
Halbgewachs, Ronald D.	Sandia National Laboratories
Hall, Tim	Mocana

Hallman, Georgia	Guidance Software
Hambrick, Gene	Carnegie Mellon University
Hanley, James	General Electric
Hardjono, Thomas	MIT
Harkins, Dan	Aruba Networks
Harper, John	American Electric Power, Inc.
Harris, Greg	Harris Corporation
Harris, Therese	Public Utility Commission of Texas
Harrison, Becky	GridWise Alliance
Hartman, Darren	ICSA Labs
Hartmann, Chad	Xcel Energy
Hashimoto, Mikio	Toshiba
Hastings, Nelson	NIST
Hawk, Carol	Department of Energy
Hayden, Ernest	Verizon
He, Donya	BAE Systems
Heger, Mary	Ameren Services
Heiden, Rick	Pitney Bowes
Heidner, Dennis	
Helm, Donny	Oncor
Henderson, Lynn	Northrop Grumman Information Systems
Hensel, Hank	CSC
Herold, Rebecca	Privacy Professor Rebecca Herold & Associates, LLC
Heron, George L.	BlueFin Security
Herrell, Jonas	University of California, Berkeley
Hertzler, Megan	Xcel Energy
Hertzog, Christine	Smart Grid Library
Hieta, Karin	California Public Utility Commission
Higgins, Moira	TSRI
Highfill, Darren	SCE
Hilber, Del	Constellation Energy
Histed, Jonathan	Novar | Honeywell
Hoag, John C.	Ohio University
Holland, Clayton	DHS / Missing Link Security
Hollenbaugh, Greg	Electrosoft Inc.
Holstein, Dennis	OPUS Consulting Group
Hoofnagle, Chris	University of California, Berkeley
Hooper, Emmanuel	Harvard University
Hornung, Lynette	
House, Joshua	Future of Privacy
Houseman, Doug	Capgemini Consulting
Howie, Sarah	NextEnergy Center

Huber, Robert	Critical Intelligence
Hudson, John	CenterPoint Energy
Hughes, Joe	EPRI
Humphrey, Robert	Duke Energy
Humphries, Scott	SmartSynch
Hunt, Chuck	
Hunteman, William	Department of Energy
Hurley, Jesse	Shift Research, LLC
Hussey, Laura	Schweitzer Engineering Laboratories, Inc.
Hutson, Jeff	Accenture
Huzmezan, Mihai	General Electric
Ibrahim, Erfan	EPRI
Iga, Yoichi	Renesas Electronics Corp.
Ilic, Jovan	
Ilic, Marija	Carnegie-Mellon University
Inaba, Atsushi	GlobalSign
Iorga, Michaela	NIST
Ivers, James	SEI
Jacobs, Leonard	Xcel Energy
Jaffray, Travis	
Jaokar, Ajit	Futuretext
Jarrett, Terry	Missouri Public Service Commission
Jeirath, Nakul	Southwest Research Institute
Jepson, Robert	Lockheed Martin Energy Solutions
Jin, Chunlian	Pacific Northwest National Laboratory
Joffe, Rodney	NeuStar
Johnson, Freemon	NIST
Johnson, Oliver	Tendril
Jones, Barry	Sempra
Jones, Derrick	Enteredge Technology, LLC
Jones, Derrick	Merlin International, Inc.
Joshi, Makarand	
Kahl, Steve	North Dakota
Kahn, Ely	FriiPwrLtd
Kaiser, Lisa	Department of Homeland Security
Kalbfleisch, Roderick	Northeast Utilities
Kanda, Mitsuru	Toshiba
Kashatus, Jennifer	Womble Carlyle Sandridge & Rice, PLLC
Kassakhian, Ken	Colorado Dept. of Regulatory Authorities
Kastner, Ryan	University of California at San Diego
Katz, Martha Lessman	Gordon, Feinblatt, Rothman, Hoffberger & Hollander, LLC

Kaufman, David R.	Honeywell International
Kavanagh, Mike	Constellation Energy
Kellogg, Shannon	EMC
Kelly, Lee	
Kenchington, Henry	U.S. Department of Energy
Kenney, Charlie	IBM
Kerber, Jennifer	Tech America
Khera, Rohit	S & C Electric Company
Khurana, Himanshu	Honeywell
Kiely, Sarah	NRECA
Kilbourne, Brett	Utilities Telecom Council
Kim, Jin	Risk Management Consulting, CRA International
Kim, Tae-Wan	NIST
Kimura, Randy	General Electric
King, Charlie	BAE Systems
Kirby, Bill	Aunigma Network Solutions Corp.
Kiss, Gabor	Telcordia
Kladko, Stan	Aspect Labs
Klein, Stanley A.	Open Secure Energy Control Systems, LLC
Klerer, Mark	
Kobayashi, Nobuhiro	Mitsubishi Electric
Kobes, Jason	Northrop Grumman Corp.
Koliwad, Ajay	General Electric
Kotting, Chris	ThinkSmartGrid, LLC
Koyuncu, Osman	Texas Instruments, Inc.
Kravitz, David	
Krishna, Karthik	Michigan Technological University
Krishnamurthy, Hema	ITT Information Assurance
Kube, Nate	Wurldtech
Kulkarni, Manoj	Mocana
Kursawe, Klaus	
Kuruganti, Phani Teja	EMC2
Kyle, Martin	Sierra Systems
Lackey, Kevin	Electric Reliability Council of Texas (ERCOT)
Lakshminarayanan, Sitaraman	General Electric
LaMarre, Mike	Austin Energy ITT
Lane, Anne	American Electric Power, Inc.
LaPorte, TJ	Landis+Gyr
Larsen, Harmony	Infogard
Lauriat, Nicholas A.	Network and Security Technologies
LaVoy, Lanse	DTE Energy

Lawrence, Bill	Lockheed Martin Corporation
Lawson, Barry	NRECA
Lebanidze, Evgeny	Cigital
Leduc, Jean	Hydro-Quebec
Lee, Annabelle	EPRI
Lee, Cheolwon	Electronics and Telecommunications Research Institute
Lee, Gunhee	Electronics and Telecommunications Research Institute
Lee, JJ	LS Industrial Systems
Lee, Travis	SMUD
Lee, Virginia	eComp Consultants
Legary, Michael	Seccuris, Inc.
Leggin, Nick	West Monroe
Lenane, Brian	SRA International
Leuck, Jason	Lockheed Martin Corporation
Levinson, Alex	Lockheed Martin Information Systems and Global Solutions
Levy, Roger	Lawrence Berkeley National Laboratory
Lewis, David	Hydro One
Lewis, Rob	Trustifiers Inc.
Li, Tony	CLP Power Hong Kong Lmtd
Libous, Jim	Lockheed Martin Systems Integration – Owego
Light, Matthew	NERC
Lilley, John	Sempra
Lima, Claudio	Sonoma Innovation
Lin, Yow-Jian	Telcordia Technologies
Lintzen, Johannes	Utimaco Safeware AG
Lipson, Howard	CERT, Software Engineering Institute
Locke, David	Verizon
Loomis, Joe	Southwest Research Institute
Lowe, Justin	PA Consulting Group
Lynch, Jennifer	University of California, Berkeley
Machado, Raphael	Inmetro – Instituto Nacional de Metrologia, Brazil
Maciel, Greg	Uniloc USA
Madden, Jason	MRIGlobal
Magda, Wally	Industrial Defender
Magnuson, Gail	
Mahmud, Shamun	DLT Solutions, Incorporated
Malashenko, Liza	California PUC
Malina, Alfred	SG-CG Smart Grid Information Security WG
Manjrekar, Madhav	Siemens
Manucharyan, Hovanes	LinkGard Systems

Maria, Art	AT&T
Markham, Tom	Honeywell
Marks, Larry	
Martin, Gordon	Alabama Power
Martinez, Catherine	DTE Energy
Martinez, Ralph	BAE Systems
Marty, David	University of California, Berkeley
Masch, Brian	Ernest & Young
Mashima, Daisuke	Fujitsu Lab of America
McBride, Sean	Critical Intelligence
McCaffree, Matt	OPOWER
McComber, Robert	Telvent
McCullough, Jeff	Elster Group
McDonald, Jeremy	Southern California Edison
McGinnis, Douglas	Exelon
McGrew, David	Cisco
McGuire, John	American Electric Power, Inc.
McGurk, Sean	Dept of Homeland Security
McKay, Brian	Booz Allen Hamilton
McKenna, Erin	
McKinnon, David	Pacific Northwest National Laboratory
McMahon, Liam	Bridge Energy Group
McMillin, Bruce	Missouri University of Science and Technology
McNay, Heather	Landis+Gyr
McQuade, Rae	NAESB
Medlar, Arthur	LocalPower
Melton, Ron	Pacific Northwest National Laboratory
Mennella, Jean-Pierre	SG-CG Smart Grid Information Security WG
Mertz, Michael	Southern California Edison
Metke, Tony	Motorola
Michail, David	Zuber & Taillieu LLP
Milbrand, Doug	Concurrent Technologies Corporation
Millard, David	Georgia Tech Research Institute
Miller, Joel	Merrion Group
Miller, Melvin	Nulink Wireless
Mirza, Wasi	Motorola
Mitsuru, Kanda	Toshiba
Mitton, David	Ambient Corp.
Modeste, Ken	Underwriters Laboratories, Inc.
Mohan, Apurva	Honeywell
Moise, Avy	Future DOS R&D Inc.
Molina, Jesus	Fujitsu Ltd.

Molitor, Paul	NEMA
Mollenkopf, Jim	CURRENT Group
Moniz, Paulo	
Monkman, Brian	ICSA Labs
Montgomery, Jason	American Electric Power, Inc.
Moody, Diane	American Public Power Association
Morese, Alex	State of Michigan
Morris, Tommy	Mississippi State University
Mosely, Donald	FriiPwrLtd
Moskowitz, Robert	ICSAlabs
Mulberry, Karen	Neustar
Munoz, Tony	Colorado Department of Regulatory Agencies
Nahas, John	ICF International
Nakamura, Masafumi	Mitsubishi Research Institute, Inc.
Navid, Nivad	Midwest ISO
Neergaard, Dude	Oak Ridge National Laboratory
Newhouse, Bill	NIST
Nguyen, Nhut	Samsung
Nidetz, Lee	TSRI
Nissim, Sharon Goott	Electronic Privacy Information Center
Noel, Paul	ASI
Norton, Dave	Entergy
Nutaro, James J.	Southern California Edison
O'Neill, Ivan	Southern California Edison
O'Sullivan, Mairtin	
Obregon, Eduardo	University of Texas at El Paso
Oduyemi, Felix	Southern California Edison
Ohba, Yoshihiro	Toshiba
Okunami, Peter M.	Hawaiian Electric Company, Inc.
Old, Robert	Siemens Building Technologies, Inc.
Oldak, Mike	Utilities Telecom Council
Olive, Kay	Olive Strategies
Ornelas, Efrain	PG&E
Overman, Thomas M.	Boeing
Owens, Andy	Plexus Research
Owens, Leslie	American Systems
Pabian, Michael	Exelon Legal Services
Pace, James	Silver Spring Networks
Pahl, Chris	Southern California Edison Company
Paine, Tony	Kepware Technologies
Pal, Partha	Raytheon BBN Technologies
Pales, Wayne	CLP Power Hong Kong Lmtd

Palmquist, Scott	Itron
Papa, Mauricio	University of Tulsa
Parthasarathy, Jagan	Business Integra
Patel, Chris	EMC Technology Alliances
Pearce, Thomas C. II	Public Utilities Commission of Ohio
Pederson, Perry	U.S. Nuclear Regulatory Commission
Peralta, Rene	NIST
Peters, Mike	FERC
Peterson, Thomas	Boeing
Phillips, Matthew	Electronic Privacy Information Center
Phillips, Michael	Centerpoint Energy
Phinney, Tom	
Phiri, Lindani	Elster Group
Pillitteri, Victoria	NIST
Pittman, James	Idaho Power
Pittman, Jason	DTE Energy
Planter-Pascal, Claudine	FERC
Polonetsky, Jules	The Future of Privacy Forum
Polulyakh, Diana	Aspect Labs
Polulyakh, Eugene	Aspect Labs
Pope, John	NeuStar
Porterfield, Keith	Georgia System Operations Corporation
Potter, Rick	Alliant Energy
Powell, Terry	L-3 Communications
Proctor, Brian	Sempra Energy Utilities
Prowell, Stacy	Oak Ridge National Laboratory
Puri, Anuj	IEEE
Pyle, Mike	Schneider Electric
Pyles, Ward	Southern Company
Qin, Andy	Cisco
Qin, Jason	Skywise Systems
Qiu, Bin	E:SO Global
Quinn, Steve	Sophos
Rader, Bodhi	FERC
Radgowski, John	Dominion Resources Services, Inc
Ragsdale, Gary L.	Southwest Research Institute
Raines, Tim	Black Hills, Corp.
Rakaczky, Ernest A.	Invensys Global Development
Rao, Josyula R	IBM
Ray, Indrakshi	Colorado State University
Reddi, Ramesh	Intell Energy
Reed, Rebecca	Texas PUC

Revill, David	Georgia Transmission Corp.
Rhéaume, Réjean	Hydro-Quebec
Richtsmeier, Dorann	Northrup Grumman Corp.
Rick Schantz	BBN
Riepenkroger, Karen	Sprint
Ristaino, Andre	
Rivaldo, Alan	Public Utility Commission of Texas
Rivero, Al	Telvent
Roberts, Don	Southern Company Transmission
Roberts, Jeremy	LonMark International
Robinson, Brandon	Balch & Bingham LLP
Robinson, Charley	International Society of Automation
Robinson, Eric	ITRON
Robinson, Louis	Constellation Energy
Rodriguez, Gene	IBM
Rothke, Ben	National Grid
Ruano, Julio	IBM
Rueangvivatanakij, Birdie	Missing Link Security
Rumery, Brad	Sempra
Rush, Bill	
Russell, Dave	Noveda Technologies
Rutfield, Craig	NTRU Cryptosystems, Inc.
Rutkowska, Joanna	Invisible Things
Rutkowski, Tony	Yaana Technologies
Sachs, Marcus	Verizon Communications
Sacre, Spiro	National Technical Systems, Inc.
Saint, Bob	National Rural Electric Cooperative Association
Sakane, Hiro	NIST
Sakr, Osman	National Technical Systems, Inc.
Salons, Deborah	
Sambasivan, Sam	AT&T
Sanders, William	University of Illinois
Saperia, Jon	
Sargent, Robert	Cisco Systems, Inc.
Saunders, Scott	SMUD
Scace, Caroline	NIST
Schaefer, Krystina	Ohio PUC
Schantz, Rick	Raytheon BBN Technologies
Scheff, Andrew	Scheff Associates
Schmitt, Laurent	SG-CG Smart Grid Information Security WG
Schneider, Brandon	SRA International
Schneider, Don	Duke Energy

Schoechle, Timothy	
Schomburg, Paul	Panasonic Corp. of North America
Schooler, Eve	Intel Labs
Schroeder, Joel	Inmarsat Inc.
Schulman, Ross	Center for Democracy and Technology
Schultz, Bill	Vanderbilt University
Schwarz, David	Department of Homeland Security
Sciacca, Sam	SCS Consulting, LLC
Sconzo, Mike	Electric Reliability Council of Texas
Scott, David	Accenture
Scott, Kat	EPIC
Scott, Richard	
Scott, Tom	Progress Energy
Searfoorce, Daniel	Pennsylvania Public Utility Commission
Searle, Justin	UtiliSec
Seewald, Mike	Cisco
Seo, Jeongtaek	Electronics and Telecommunications Research Institute
Sequino, David	Green Hills Software
Shah, Nihar	Information Law Group
Shakespeare, Jared	Western Electricity Coordinating Council
Shastri, Viji	MCAP Systems
Shavit, Juliet	SmartMark Communications, LLC
Shaw, Vishant	Enernex
Shein, Robert	EDS
Sheldon, Rick	Oakridge National Laboratory
Sherman, Sean	Triton
Shetty, Ram	General Electric
Shin, Mark	Infogard
Shipley, AJ	Wind River
Shorter, Scott	Electrosoft
Shpantzer, Gal	
Silverstone, Ariel	
Sinai, Nick	Federal Communications Commission
Singer, Bryan	Kenexis
Sisley, Elizabeth	University of Minnesota
Sitbon, Pascal	EDF Inc.
Skare, Paul	Pacific Northwest National Laboratory
Skidmore, Charlotte	Association of Home Appliance Manufacturers
Slack, Phil	Florida Power & Light Company
Smith, Brian	EnerNex
Smith, Charles	General Electric

Smith, Rhett	Schweitzer Engineering Laboratories, Inc.
Smith, Ron	ESCO Technologies Inc.
Smith, Zane	FriiPwrLtd
Sokker, Anan	Florida Power & Light Company
Sood, Kapil	Intel Labs
Sorebo, Gilbert	SAIC
Soriano, Erick	Garvey Schubert Barer
Souza, Bill	
Spirakis, Charles	Google
St Johns, Michael	Nth Permutation
Staggs, Kevin	Honeywell
Stallings, Amanda	Public Utility Commission of Ohio
Stammberger, Kurt	Mocana
Standifur, Thomas	KEMA Inc.
Starr, Christopher	General Dynamics Advanced Information Systems
Steiner, Michael	IBM Thomas J. Watson Research Center
Stepanovich, Amie	EPIC
Sterling, Joyce	NitroSecurity
Stevens, James	Software Engineering Institute
Stewart, Clinton	
Stitzel, Jon	Burns & McDonnell Engineering Company, Inc.
StJohns, Michael	Nth Permutation
Storey, Clay	Avista Corp.
Stouffer, Keith	NIST
Strickland, Tom	General Electric
Struik, Rene	Struik Security Consultancy
Struthers, Brent	NeuStar
Stuber, Micheal	Itron
Sturek, Don	Grid2Home
Sturm, John	Indiana State University
Stycos, Dave	Zocalo Data Systems, Ltd.
Suarez, Luis Tony	Tennessee Valley Authority
Suchman, Bonnie	Troutman Sanders LLP
Sullivan, Kevin	Microsoft
Sung, Lee	Fujitsu
Sushilendra, Madhava	EPRI
Swanson, Marianne	NIST
Sweet, Jeffrey	American Electric Power, Inc.
Tallent, Michael	Tennessee Valley Authority
Taylor, Dave	Siemens
Taylor, Malcolm	Carnegie Mellon University
Tengdin, John	OPUS Consulting

Thanos, Daniel	General Electric
Thaw, David	Hogan & Hartson
Thomas, Sarah	California Public Utility Commission
Thomassen, Tom	Symantec
Thompson, Catherine	Information and Privacy Commissioner's Office of Ontario
Thompson, Daryl L.	Thompson Network Consulting
Thompson, Mark	Aclara RF Systems, Inc.
Thomson, Matt	General Electric
Thrasher, Shelly	Office of the Information & Privacy Commissioner of Ontario
Tien, Lee	Electronic Freedom Foundation
Tiffany, Eric	Liberty Alliance
Tillman, Leonard	Balch & Bingham LLP
Tobin, Tim	Hogan Lovells US LLP
Toecker, Michael	Burns & McDonnell
Tolway, Rich	APS
Tom, Steve	Idaho National Laboratory
Tran, Lan	Tangible
Trapp, Bob	Booz Allen Hamilton
Trayer, Mark	Samsung
Trimble, Curtis D.	
Truskowski, Mike	Cisco System, Inc.
Tull, Laurie	Anakam, an Equifax Company
Tunney, Carrin	DTE Energy
Turgeon, Anyck	
Turke, Andy	Siemens Energy, Inc.
Turner, Patrick	Secure Works
Turner, Steve	International Broadband Electric Communications, Inc.
Uhrig, Rick	Electrosoft
Urban, Jennifer	Samuelson Clinic at UC Berkeley
Uzhunnan, Abdul	DTE Energy
Vader, Rob	DTE Energy
van Loon, Marcel	AuthenTec
Vankayala, Vidya	Cisco
Vayos, Daphne	Northeast Utilities
Veillette, Michel	Trilliant Inc.
Veltsos, Christophe	Minnesota State University
Venkatachalam, R. S.	Mansai Corporation
Vettoretti, Paul	SBC Global
Villarreal, Christopher	California Public Utilities Commission
Voje, Joe	Snohomish County PUD

Vollebregt, Paul	MobiComm Communications
Wacks, Kenneth P.	GridWise Architecture Council
Waddell, Dan	Tantus Tech
Waheed, Aamir	Cisco Systems, Inc.
Walia, Harpreet	Wave Strong Inc.
Wall, Perrin	CenterPoint Energy
Wallace, Donald	Itron
Walsh, Jack	ICSA Labs
Walters, Keith	Edison Electric Institute
Walters, Ryan	COO TerraWi Communications
Wang, Alex	Cisco Systems, Inc.
Wang, Longhao	Samuelson Clinic at UC Berkeley
Wang, Yongge	University of North Carolina-Charlotte
Ward, Mark	Pacific Gas & Electric Company
Warner, Christopher	Pacific Gas & Electric Company
Watson, Brett	NeuStar
Webb, Kyle	Deloitte & Touche LLP
Weber, Don	InGuardians
Wei, Dong	SIEMENS Corporation
Weimerskirch, Andre	Escrypt
Wepman, Joshua	SAIC Commercial Business Services
West, Andrew C	Invensys Process Systems
West, Troy	Cleco Corpo.
Weyer, John A.	John A. Weyer and Associates
Whitaker, Kari	LockDown, Inc.
White, Jim	Uniloc USA, Inc.
Whitney, Tobias	The Structure Group
Whitsitt, Jack	
Whyte, William	Ntru Cryptosystems, Inc.
Wiese, Sean	National Information Solutions Cooperative
Williams, Jeffrey	
Williams, Terron	Elster Electricity
Wilson, Chris	TechAmerica
Wilson, Jason	Duke Energy
Wingo, Harry	Google
Witnov, Shane	University of California, Berkeley
Wohnig, Ernest	Booz-Allen Hamilton
Wolf, Dana	RSA
Wollman, David	NIST
Worden, Michael	New York State Public Service Commission
Worthington, Charles	Federal Communications Commission
Wright, Andrew	N-Dimension Solutions

Wright, Christine	Texas PUC
Wright, Josh	Inguardians
Wu, Lei	Clarkson University
Wu, Richard	Nokia Siemens Networks, USA
Wyatt, Michael	ITT Advanced Technologies
Xia, Sharon	ALSTOM Grid Inc.
Yakobitis, John J.	Federal Energy Regulatory Commission
Yao, Taketsugu	Oki Electric Industry, Co., Ltd
Yap, Xiang Ling	MIT
Yardley, Tim	University of Illinois
Yodaiken, Ruth	Federal Trade Commission
Yoo, Kevin	Wurldtech
Zausner, Alan	
Zummo, Paul	American Public Power Association
Zurcher, John	SRA

3949