DRAFT NISTIR 7628

Smart Grid Cyber Security Strategy and Requirements

The Cyber Security Coordination Task Group
Annabelle Lee, Lead
Tanya Brewer, Editor
Advanced Security Acceleration Project – Smart Grid

September 2009

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

DRAFT NISTIR 7628

Smart Grid Cyber Security Strategy and Requirements

The Cyber Security Coordination Task Group

Annabelle Lee, Lead
Tanya Brewer, Editor
Computer Security Division
Information Technology Laboratory

Advanced Security Acceleration Project – Smart Grid

September 2009

U. S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director

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 analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report 7628 (draft)
236 pages (September 2009)

Acknowledgments

This document was developed by members of the Cyber Security Coordination Task Group (CSCTG). The group is lead by NIST. The members of the CSCTG have extensive technical expertise, knowledge, and commitment to addressing the cyber security needs of the Smart Grid. Members of the CSCTG and the workings groups of the CSCTG are listed in Appendix E of this document.

Another group has also been instrumental in the development of this document. The Advanced Security Acceleration Project – Smart Grid (ASAP-SG) developed the security profile for Advanced Metering Infrastructure (AMI) for the CSCTG and The UtiliSec Working Group (UCAIug). Many of the members of the ASAP-SG also participate in the CSCTG. Members of the ASAP-SG are also listed in Appendix E of this document.

Table of Contents

CHAPTER ONE

CYBER SECURITY RISK MANAGEMENT FRAMEWORK AND STRATEGY

1.1 OVERVIEW

With the Smart Grid's transformation of the electric system to a two-way flow of electricity and information, the information technology (IT) and telecommunications infrastructures have become critical to the energy sector infrastructure. Therefore, the management and protection of systems and components of these infrastructures must also be addressed by an increasingly diverse energy sector. To achieve this requires that security be designed in at the architectural level.

NIST has established a Smart Grid Cyber Security Coordination Task Group (CSCTG), which now has more than 200 volunteer members from the public and private sectors, academia, regulatory organizations, and federal agencies. Cyber security is being addressed in a complementary and integral process that will result in a comprehensive set of cyber security requirements. As explained more fully later in this chapter, these requirements are being developed using a high-level risk assessment process that is defined in the cyber security strategy for the Smart Grid. Cyber security requirements are implicitly recognized as critical in all of the particular priority application plans discussed in the *NIST Smart Grid Framework 1.0* document that is being published concurrent with the publication of this document.

Although still a work in progress, NIST is publishing this preliminary report, NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements[1] that describes the CSCTG's overall cyber security strategy for the Smart Grid. The preliminary report distills use cases collected to date, requirements and vulnerability classes identified in other relevant cyber security assessments and scoping documents, and other information necessary for specifying and tailoring security requirements to provide adequate protection for the Smart Grid. Anticipated to be published by the end of 2009 a subsequent draft will include the overall Smart Grid security architecture and security requirements.

The first installment of this in-process document also is being submitted for public review and comment in conjunction with *NIST Smart Grid Framework 1.0 document*. This roughly 240-page document is summarized below.

1.2 CYBER SECURITY AND THE ELECTRIC SECTOR

The critical role of cyber security in ensuring the effective operation of the Smart Grid is documented in legislation and in the Department of Energy (DOE) Energy Sector Plan as described below:

[1] The document is available at: http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7628 Comments may be submitted to: csctgdraftcomments@nist.gov.

The Energy Independence and Security Act of 2007 (P.L. 110-140) states that, "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:

1. Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
2. Dynamic optimization of grid operations and resources, with full cyber-security. ...."

DOE's *Energy Sector-Specific Plan*[2] "envisions a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government."

1.3 SCOPE, RISKS, AND DEFINITIONS

Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways. The need to address potential vulnerabilities has been acknowledged across the Federal government, including NIST, the Department of Homeland Security (DHS), DOE, and FERC.

Additional risks to the grid include:

- Increasing the complexity of the grid that could introduce vulnerabilities and increase exposure to potential attackers and unintentional errors;
- Interconnected networks can introduce common vulnerabilities;
- Increasing vulnerabilities to communication disruptions and introduction of malicious software that could result in denial of service or compromise the integrity of software and systems;
- Increased number of entry points and paths for potential adversaries to exploit; and
- Potential for compromise of data confidentiality, include the breach of customer privacy.

With the adoption and implementation of the Smart Grid, the IT and telecommunication sectors will be more directly involved. These sectors have existing cyber security standards to address vulnerabilities and assessment programs to identify known vulnerabilities in these systems. These same vulnerabilities need to be assessed in the context of the Smart Grid. In addition, the Smart Grid has additional vulnerabilities due to its complexity, large number of stakeholders, and highly time-sensitive operational requirements.

[2] Department of Energy, *Energy, Critical Infrastructure and Key Resources, Sector-Specific Plan as input to the National Infrastructure Protection Plan,* May 2007.

The following definitions of cyber infrastructure and cyber security from the National Infrastructure Protection Plan (NIPP) are included to ensure a common understanding.

- **Cyber Infrastructure:** Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.

For this document, cyber security is defined as follows:

- **Cyber Security**: The protection required to ensure confidentiality, integrity and availability of the electronic information communication system.

1.4 SMART GRID CYBER SECURITY STRATEGY

The overall cyber security strategy for the Smart Grid examines both domain-specific and common requirements when developing a mitigation strategy to ensure interoperability of solutions across different parts of the infrastructure.

Implementation of a cyber security strategy requires the development of an overall cyber security risk management framework for the Smart Grid. This framework is based on existing risk management approaches developed by both the private and public sectors. This risk management framework establishes the processes for combining impact, vulnerability, and threat information to produce an assessment of risk to the Smart Grid and to its domains and sub-domains, such as homes and businesses. Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated impacts. Because the Smart Grid includes systems and components from the IT, telecommunications, and energy sectors, the risk management framework is applied on an asset, system, and network basis, as applicable. The goal is to ensure that a comprehensive assessment of the systems and components of the Smart Grid is completed. Following the risk assessment, the next step is to select and tailor (as necessary) the security requirements.

The following documents were used in developing the risk management approach for the Smart Grid:

- National Institute of Standards and Technology (NIST) Special Publication (SP), 800-39, *DRAFT Managing Risk from Information Systems: An Organizational Perspective*, April 2008;
- Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006;

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004;
- North American Electric Reliability Corporation (NERC), *Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment*, 2002;
- *The National Infrastructure Protection Plan*, 2009;
- The IT, telecommunications, and energy sectors sector specific plans (SSPs), initially published in 2007 and updated annually;
- ANSI/ISA-99, *Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology*, 2007 and *Part 2: Establishing a Manufacturing and Control Systems Security Program*, 2009; and
- The *Advanced Metering Infrastructure (AMI) System Security Requirements*, 2008.

In a typical risk management process, assets, systems and networks are identified; risks are assessed (including vulnerabilities, impacts and threats); security requirements are specified; and security controls are selected, implemented, assessed for effectiveness, authorized,[3] and then monitored over the lifecycle of the system. The risk assessment process for the Smart Grid will be completed when the security requirements are specified. These requirements will be selected on the basis of a risk assessment and will apply to the Smart Grid as a whole. The requirements will not be allocated to specific systems, components, or functions of the Smart Grid. In specifying the security requirements, all gaps will be identified. The implementation, assessment and monitoring of security controls are applicable when a system is implemented in an operational environment. The output from the Smart Grid risk management process should be used in these steps. In addition, the full risk management process should be applied to legacy systems and when Smart Grid owners and operators implement new systems or augment/modify existing systems.

The tasks within the cyber security strategy for the Smart Grid are being performed by participants in the NIST led Cyber Security Coordination Task Group (CSCTG). Representatives from the private and public sectors, regulatory bodies, and federal agencies participate in the CSCTG. In addition, the CSCTG is coordinating activities with the Advanced Security Acceleration Project – Smart Grid. The ASAP-SG is a collaborative effort between EnerNex Corporation, multiple major North American utilities, the National Institute of Standards and Technology, and the United States Department of Energy (DOE), including resources from Oak Ridge National Laboratory and the Software Engineering Institute of Carnegie Mellon University. Following are the tasks that are being performed by the CSCTG in the implementation of the cyber security strategy. Also included are the deliverables for each task. Because of the timeframe for developing the document, the tasks listed below will be performed in parallel, with significant interactions among the groups addressing the tasks. . (These tasks are not listed in priority order - the first task is near completion, and the second and third tasks are being worked on in parallel.)

[3] Security authorization is the step where the designated official accepts the risk to the mission.

1.4.1 Selection of use cases with cyber security considerations.[4]

The use cases were selected from several existing sources, e.g., IntelliGrid, Electric Power Research Institute (EPRI), and Southern California Edison (SCE). The set of use cases provides a common framework for performing the risk assessment, developing the security architecture, and selecting and tailoring the security requirements. The Use Cases are included in Appendix A of this document.

1.4.2 Performance of a risk assessment of the Smart Grid, including assessing vulnerabilities, threats and impacts.

The risk assessment, including identifying vulnerabilities, impacts and threats will be done from both a high-level overall functional perspective and a focus on the six functional priority areas that are the focus of this framework and roadmap report. The output will be used in the selection of security requirements and the identification of security requirements gaps. The initial draft list of vulnerability classes[5] was developed using information from several existing documents and websites, e.g., NIST SP 800-82 and the Open Web Application Security Project (OWASP) vulnerabilities list. These vulnerability classes will be used in ensuring that the security controls address the identified vulnerabilities. The vulnerability classes may also be used by Smart Grid implementers, e.g., vendors and utilities in assessing their systems.

Both top-down and bottom-up approaches are being used in implementing the risk assessment. The top-down approach focuses on the use cases and the overall Smart Grid functionality. The bottom-up approach focuses on well-understood problems that need to be addressed, such as authenticating and authorizing users to substation IEDs, key management for meters, and intrusion detection for power equipment. Also, interdependencies among Smart Grid domains/systems will be considered when evaluating the impacts of a cyber or physical security incident. An incident in one infrastructure can cascade to failures in other domains/systems. The vulnerability categories are included in Appendix C of this document. The Bottom-Up Security Analysis of the Smart Grid is included in Appendix D of this document.

1.4.3 Development of a security architecture linked to the Smart Grid conceptual reference model

The first phase in this task was to assess and revise the six functional priority areas with logical interfaces. The information that is communicated across each interface was specified. Also, implementation constraints and issues were specified for each interface and the confidentiality, integrity, and availability impact levels were defined. After all the logical interfaces across all the priority areas were identified, each interface was allocated to one of the logical interface categories based on similarity of networks, constraints, and types of information. Some examples are: control systems with high data accuracy and high

[4] A use case is a method of documenting applications and processes for purposes of defining requirements.

[5] 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. A vulnerability class is a grouping of common vulnerabilities.

availability, as well as media and compute constraints; B2B connections, interfaces between sensor networks and controls systems; and interface to the customer site. For each logical interface category, constraints, issues, and impacts were selected using the information provided for each individual interface. This information will be used in the selection and tailoring of security requirements – defined in 1.4.4 below. The diagrams and interface categories are included in Section 3 of this document.

The Smart Grid conceptual reference model, described in chapter 3 of the *NIST Smart Grid Framework 1.0* document, provides a common view that is being used to develop the Smart Grid security architecture. The Smart Grid security architecture will overlay this conceptual architecture and security requirements will be allocated to specific domains, mission/business functions and/or interfaces included in the Smart Grid conceptual reference model. Alternatively, some security requirements, such as the policy requirements, will be allocated to the entire Smart Grid. (Note: this task has not been initiated; therefore, how the security requirements will be allocated has not been finalized.) The objective is to ensure that cyber security is addressed as a critical cross-cutting requirement of the Smart Grid.

1.4.4 Specification and tailoring of security requirements to provide adequate protection.

There are many requirements documents that may be applicable to the Smart Grid. Currently, only the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIPs) are mandatory for a specific domain of the Smart Grid. The following documents have been identified by members of the CSCTG as having security requirements relevant to one or more aspects of the smart grid.

The following standards are directly relevant to Smart Grid

- NERC CIP 002, 003-009
- IEEE 1686-2007, *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*
- AMI System Security Requirements, 2008
- *UtilityAMI Home Area Network System Requirements Specification*, 2008
- IEC 62351 1-8, Power System Control and Associated Communications - Data and Communication Security

The following documents are applicable to control systems:

- ANSI/ISA-99, *Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology* and *Part 2: Establishing a Manufacturing and Control Systems Security Program*
- NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009.
- NIST SP 800-82, *DRAFT Guide to Industrial Control Systems (ICS) Security*, Sept. 2008
- DHS Procurement Language for Control Systems
- ISA SP100, *Wireless Standards*

Because the impact of a security compromise may vary across the domains and interfaces of the Smart Grid, security requirements from different baselines in NIST SP 800-53 will be considered. For example, in the federal government, FIPS 199 identifies three impact levels; low, moderate and high. The impact is based on the potential impact of the security breach of confidentiality, integrity, and availability. FIPS 200 establishes the minimum security requirements for federal information and information systems. These minimum requirements are further defined by a set of baseline security controls in SP 800-53 that are based on the impact levels in FIPS 199.

The cyber security requirements in the documents listed above are not unique across the documents. To assist in assessing and selecting the requirements, a cross-reference matrix was developed and is included in Appendix B of this document. This matrix maps the requirements from the various documents listed above to the controls included in the *Catalog of Control Systems Security: Recommendations for Standards Developers*, published by the Department of Homeland Security in 2008. The security requirements included in the Catalog document are the base for the development of the specific cyber security controls for the Smart Grid. The requirements in the Catalog are at a high level and will need to be tailored for the specific needs of the Smart Grid. Included in this document are the AMI security requirements that were developed by the ASAP-SG project.

1.5 TIME LINE AND DELIVERABLES

This first draft of the NISTIR includes the initial risk assessment documents (vulnerability classes and bottom-up analysis), the security-relevant use cases, the cross-reference of security standards, the six functional priority areas diagrams and interfaces, the Advanced Metering Infrastructure (AMI) security requirements, and the interface categories with constraints, issues, and impacts. This document will be posted for public comment.

The second draft of the NISTIR will be revised based on the comments received from the first draft. In addition, the second draft will include the overall Smart Grid architecture and the security requirements. This draft will also be posted for public comment. This draft is scheduled to be published in December 2009.

The final version of the NISTIR is scheduled to be published in March 2010, and will address all comments received to that date. The document will have the final set of security controls and the final security architecture.

CHAPTER 2

PRIVACY AND THE SMART GRID

2.1 HIGH-LEVEL SMART GRID CONSUMER-TO-UTILITY PRIVACY IMPACT ASSESSMENT (PIA) REPORT

One of the working groups of the CSCTG addresses privacy. This working group consists of representatives from industry and information security and privacy experts and focuses on the privacy issues of the Smart Grid. With the extremely limited timeframe, the group was unable to perform an in-depth review of all possible information exchanges. However, the high-level assessment revealed many significant privacy concerns and issues.

This Privacy Impact Assessment (PIA) examines privacy implications and related information security safeguards within the planned U.S. Smart Grid, particularly issues involved with consumer-to-utility data items collected and how they are used. This analysis was performed in accordance with numerous U.S. federal data protection requirements and with Organization for Economic Cooperation and Development (OECD) privacy principles as outlined within the American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP).

The scope of this PIA includes a review of available documentation and information obtained from a variety of utility and industry contacts and experts.

2.2 SUMMARY OF PIA FINDINGS

The results of a high-level PIA of the consumer-to-utility metering data sharing portion of the Smart Grid reveal that significant areas of concern must be addressed within each localized region of the Smart Grid.

Most states have general laws in place regarding privacy protections. However, these laws are most often not specific to the electric utility industry. Furthermore, enforcement of state privacy related laws is often delegated to agencies other than public utility commissions, who have regulatory responsibility for electric utilities. Research indicates that, in general, state utility commissions currently lack formal privacy policies or standards related to the Smart Grid. Some, individual utility implementations of the Smart Grid are currently at an early stage, while others are more fully developed. Utilities at an early stage of implementation may have not yet documented or implemented privacy policies, standards, or procedures for the data collected throughout the Smart Grid. Comprehensive and consistent definitions of personally identifiable information (PII) do not typically exist at state utility commissions, at FERC, or within the utility industry.

The lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use creates a privacy risk that needs to be addressed.

2.3 PURPOSE OF A HIGH-LEVEL PIA

This document summarizes the results of a high-level PIA, performed during August 2009, of the consumer-to-utilities component of the planned Smart Grid. The PIA objectives were to determine if the risks to PII and associated privacy issues are mitigated appropriately, and that PII data is not inaccurate or out-of-date. Additional objectives were to determine if excessive PII was collected or used in unacceptable or unexpected ways beyond the control of data subjects.

The following preliminary set of principles was developed using the GAPP, which form the basis of most international, national, and local data protection laws. In addition, safeguards specified in the international information security standard ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements* (widely used for data protection regulatory compliance) were considered. The consumer-to-utility smart meter data gathering documentation included in the NIST Roadmap was reviewed against these principles in the development of this section. These principles can be used by authorities and organizations as a starting point for the development of appropriate protections for PII collected and/or used within the Smart Grid.

1. **Management and Accountability**: An organization should formally appoint personnel to ensure that information security and privacy policies and practices exist and are followed. Documented requirements for regular training and ongoing awareness activities should exist and be followed. Audit functions should be present to monitor all data accesses and modifications.

2. **Notice and Purpose**: A clearly-specified notice should exist to describe the purpose for the collection, use, retention, and sharing of PII. Data subjects should be told this information at or before the time of collection.

3. **Choice and Consent**: The organization should describe the choices available to individuals and obtain explicit consent if possible, or implied consent when this is not feasible, with respect to the collection, use, and disclosure of their PII.

4. **Collection and Scope**: Only PII that is required to fulfill the stated purpose should be collected from individuals. Treatment of the information must conform to fair information processing practices. Information should be collected directly from each individual person unless there are justifiable reasons why this is not possible.

5. **Use and Retention**: Information should only be used or disclosed for the purpose for which it was collected, and should only be divulged to those parties authorized to receive it. PII should be aggregated or anonymized wherever possible to limit the potential for computer matching of records. PII should only be kept as long as is necessary to fulfill the purposes for which it was collected.

6. **Individual Access**: Organizations should provide a process for PII data subjects to allow them to ask to see their corresponding PII and to request the correction of perceived

inaccuracies. PII data subjects must also be informed about parties with whom PII has been shared.

7. **Disclosure and Limiting Use**: PII should be used only for the purposes for which it was collected. PII should not be disclosed to any other parties except for those identified in the notice, or with the explicit consent of the individual.

8. **Security and Safeguards**: PII, in all forms, must be protected from loss, theft, unauthorized access, disclosure, copying, use, or modification.

9. **Accuracy and Quality**: Every effort should be made to ensure that the PII is accurate, complete, and relevant for the purposes identified in the notice, and remains accurate throughout the life of the PII while within the control of the organization.

10. **Openness, Monitoring and Challenging Compliance**: Privacy policies should be made available to PII data subjects. PII data subjects should be given the ability and process to challenge an organization's compliance with their state privacy policies as well as their actual privacy practices.

2.4 NIST SMART GRID DESCRIPTION

Some of the goals of the planned Smart Grid will require the use of digital technology to improve reliability, security, and efficiency of the nationwide electricity system from large generation power transmission, distribution, and management, through the delivery systems to electricity consumers and increasing numbers of distributed-generation and storage resources. As described in the July 2009 *Smart Grid System Report* from the U.S. Department of Energy[6]:

"Areas of the electric system that cover the scope of a smart grid include the following:

- *the delivery infrastructure (e.g., transmission and distribution lines, transformers, switches),*
- *the end-use systems and related distributed-energy resources (e.g., building and factory loads, distributed generation, storage, electric vehicles),*
- *management of the generation and delivery infrastructure at the various levels of system coordination (e.g., transmission and distribution control centers, regional reliability coordination centers, national emergency response centers),*
- *the information networks themselves (e.g., remote measurement and control communications networks, inter- and intra-enterprise communications, public Internet), and*
- *the financial and regulatory environment that fuels investment and motivates decision makers to procure, implement, and maintain all aspects of the system (e.g., stock and*

[6] Retrieved 08.27.09 from page iv at http://www.oe.energy.gov/DocumentsandMedia/SGSRMain_090707_lowres.pdf

bond markets, government incentives, regulated or non-regulated rate-of-return on investment)."

As work progresses on the Smart Grid, privacy concerns continue to be raised as a result of discussions and speculation about how data automatically collected from smart meters, and potentially distributed and utilized throughout the entire Smart Grid system, will be used and, more importantly for this review, how it may be protected.

The scope of this PIA is the consumer meter to local utility (consumer-to-utility) data flow and associated privacy issues. However, before looking specifically at the consumer-to-utility issues, one must first consider the wide breadth and significant depth of information flow throughout the entire Smart Grid network. As Figure 2.1 shows, the expanse is significant.

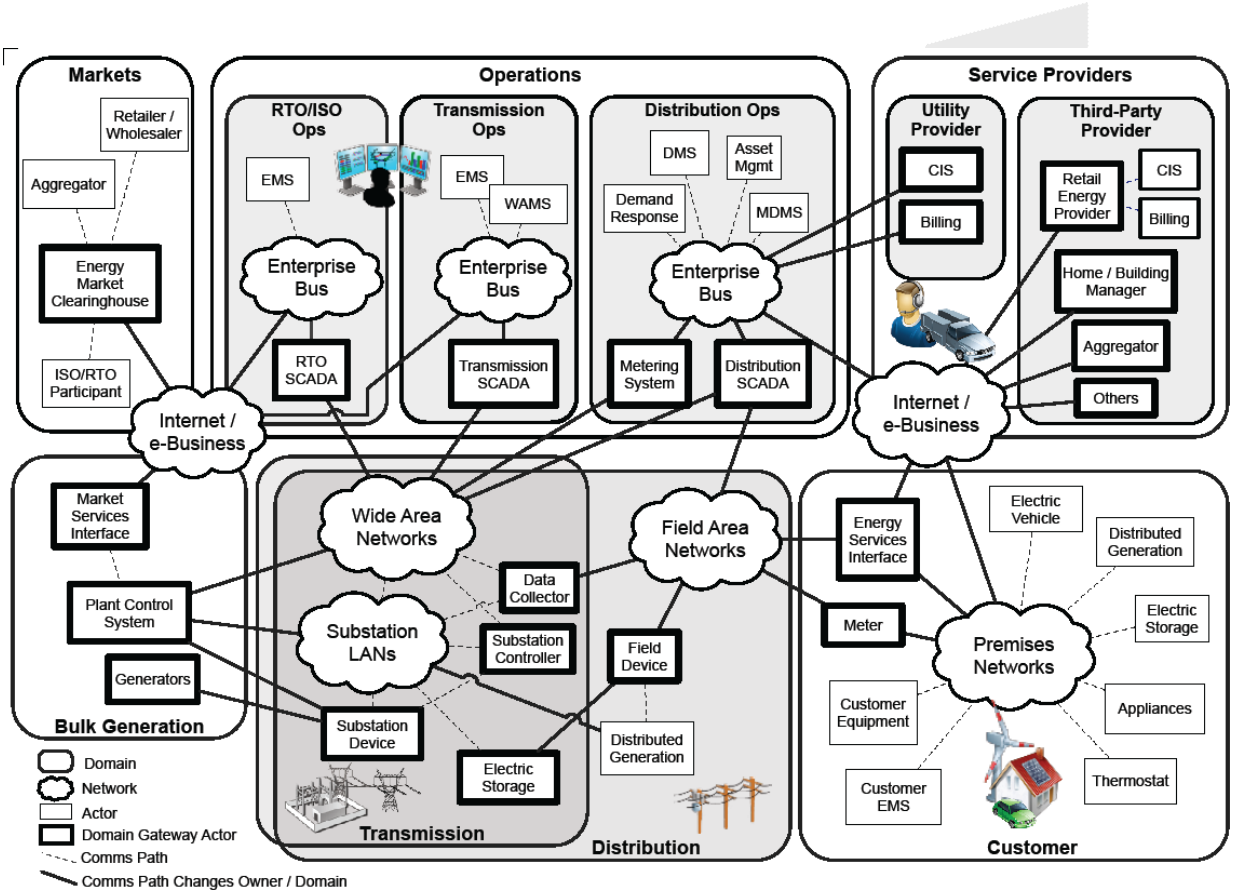


Figure 2.1 Information sharing components of the Smart Grid[7]

Data will flow between the many components within the Smart Grid. The bi-directional flow of data between utilities and customer premises will now be more similar to the types of data flows between commercial meters and utilities. While the data flows are similar, as the diagram in Figure 2.1 indicates, the specific data items involved, and the associated privacy issues, are very different. The data items collected from the Distributed Energy Resources (DERs) and smart meters will reveal different types of information about residential consumers and activities

[7] Diagram from NIST Smart Grid Framework 1.0 Sept 2009.

within the house than the information collected from commercial DERs and smart meters. The differences in potential impacts to individuals are significant.

The ability for smart grid devices to "roam" to other utility systems – for example, driving an electric vehicle (PEV) to visit family, and recharging it while there – creates the potential for additional flows of PII data (such as the PEV identifiers) between the roaming devices and their "host" utility if the "host" utility were in a position to bill the PEV's "home" utility for the PEV's recharge.

2.5 PRIVACY PRINCIPLES AND RELATIONSHIP TO THE SMART GRID

2.5.1 Management, Accountability and Training

At this time, the Privacy group could find no formally documented privacy responsibilities for Smart Grid management positions.

Documented requirements for regular privacy training and ongoing awareness activities for all utilities, vendors, and other entities with management responsibilities throughout the Smart Grid should be created and implemented, and compliance enforced.

2.5.2 Notice and Purpose for PII Use

The new smart meters and accompanying potential and actual uses create the need for utilities to be more transparent and clearly provide notice documenting the types of information items collected, and the purposes for collecting the data.

Within the Smart Grid implementation a clearly-specified notice must describe the purpose for the collection, use, retention, and sharing of PII. Data subjects should be told this information at or before the time of collection.

2.5.3 Choice & Consent to use PII

New smart meters create the need for utilities to give residents a choice about the types of data collected. Utilities should obtain consent from residents for using the collected data for other purposes, and as a requirement before data can be shared with other entities.

2.5.4 Collection of PII

In the current operation of the electric grid, data taken from meters consists of basic data usage readings required to create bills. Under a smart grid implementation, meters and will collect other types of data. Some of this additional data may be PII. Because of the associated privacy risks, only the minimum amount of data necessary for the utility companies to use for energy management and billing should be collected. However, the amount of information collected may vary, depending on whether or not power generation occurs on the premises. Home generation services will likely increase the amount of information created and shared.

2.5.5 Use and Retention of PII

In the current operation of the electric grid, data taken from meters is used to create residents' bills, determine energy use trends, and allow customers to control their energy usage both on-site

and remotely. The new smart meters, and the Smart Grid network, will have the capability to use the collected data in an unlimited number of ways.

Information should only be used or disclosed for the purpose for which it was collected, and should be divulged only to those parties authorized to receive it. PII should be aggregated or anonymized wherever possible to limit the potential for computer matching of records. PII should only be kept as long as is necessary to fulfill the purposes for which it was collected.

2.5.6 Individual access

In the current operation of the electric grid, data taken from the meters is obtainable by consumers from their own homes. The data collected in a Smart Grid implementation may be stored in multiple locations. Currently, there is no standardized process to allow residents to access to their own corresponding PII that may be stored throughout the Smart Grid. .

Currently, customers are able to access their account information through their monthly bill, utility websites, and annual terms and conditions statements. The utilities that comprise the Smart Grid should establish and provide to all customers a process to allow them to inspect their corresponding PII , and to request the correction of inaccuracies. Customers should also be informed about parties with whom PII data has been shared.

2.5.7 Disclosure and Limiting Use of PII

Significant privacy concerns and risks exist when PII is inappropriately shared without the knowledge and consent of the individuals to whom the PII applies. Data collected through smart meters should be used solely for the specific purposes for which it was collected. If utilities wish to use the data for other purposes, or share the data with other entities, they should notify consumers, clearly communicate their plans, and obtain consent to use and share the data as described.

2.5.8 Security and Safeguards

The data collected from smart meters may potentially be transmitted to and stored in multiple locations throughout the Smart Grid. Establishing strong security safeguards will be necessary to protect the PII from loss, theft, unauthorized access, disclosure, copying, use, or modification. (The AMI requirements are included in this draft and requirements for the entire Smart Grid will be included in the December draft of this document.)

2.5.9 Accuracy and Quality of PII

The data collected from smart meters and related equipment will potentially be stored in multiple locations throughout the Smart Grid. Meter data may be automatically collected in a variety of ways. The ability to inappropriately modify data could be significant in utilities where access controls are not appropriately set. Accordingly, establishing strong security safeguards will be necessary to protect the information. Since meter data may be stored in many locations, and therefore, accessed by many different individuals and entities and used for a very wide variety of purposes, PII data may be inappropriately modified. Automated Smart Grid decisions made for home energy use could be detrimental for residents (e.g., restricted power, thermostats turned to dangerous levels), while decisions about Smart Grid power use and activities could be based upon inaccurate information.

Every effort must be made to ensure that PII collected throughout the Smart Grid, and at all locations where it is stored, is accurate, complete and relevant for the purposes identified, and remains accurate throughout the life of the PII.

2.5.10 Openness, Monitoring and Challenging Compliance

In the current electric grid, utilities follow a wide variety of methods and policies for communicating to residents how PII will be used. Some utilities provide no privacy notices to residents. The data collected from new smart meters and related equipment will potentially be stored in multiple locations throughout the Smart Grid, possibly within multiple states. Privacy protections should be applied consistently and at the same level for all PII throughout the entire Smart Grid system to be effective.

2.6 COMPLIANCE

Privacy issues created by the Smart Grid have already begun to be addressed; for example, NARUC has adopted the *"Resolution Urging the Adoption of General Privacy Principles For State Commission Use in Considering the Privacy implications of the Use of Utility Customer Information."* (available at http://www.naruc.org/Resolutions/privacy_principles.pdf)

CHAPTER 3
LOGICAL INTERFACE ANALYSIS

One of the first tasks in the cyber security strategy for the Smart Grid is to assess the interface diagrams developed for the six functional priority areas. This analysis involved reviewing and revising the logical interface diagrams, identifying the logical data flows within each interface diagram, identifying the security constraints and issues for each interface, and specifying the confidentiality, integrity, and availability (CIA) impact levels of data compromises at each interface. The next step was to consolidate all the interfaces into one of the categories defined below. Finally, for each category, the security constraints, security issues, CIA impacts were specified. This information was consolidated from the individual interface specifications completed previously.

3.1 CATEGORIZATION OF THE LOGICAL INTERFACES

The logical interfaces in the six functional priority areas were allocated to one of the fifteen categories defined below. These categories were selected based on the similarity of networks, constraints, and types of information that is passed across the logical interface.

Category
1. Control systems with high data accuracy and high availability, as well as media and compute constraints • E.g. Between Supervisory Control and Data Acquisition (SCADA) and field equipment
2. Control systems with no bandwidth constraints wide area network (WAN) but are in different organizations • E.g. Between an Regional Transmission Organization/Independent System Operators (RTO/ISO) Energy Management System (EMS) and a utility energy management system
3. Control systems within the same organization with no bandwidth constraints • E.g. multiple Distribution Management System (DMS) systems belonging to the same utility
4. Back office systems under common management authority • E.g. Between a Customer Information System and a Meter Data Management System
5. Back office systems not under common management authority • E.g. Between a third party billing system and a utility meter data management system
6. B2B connections • E.g. Between a Retail aggregator and an Energy Clearinghouse
7. Interfaces between control systems and non-control systems • E.g. between a Geographic Information System (GIS) and a Load Management/Demand Response (DR) System

Category
8. Sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements • E.g. between temperature sensor on a transformer and its receiver
9. Interfaces between sensor networks and control systems • E.g. between a sensor receiver and the substation master
10. Interfaces that use the Advanced Metering Infrastructure (AMI) network • E.g. Between meter data management system (MDMS) and meters • Between Load Management System/Demand Response Management System (LMS/DRMS) and Customer EMS • Between DMS Applications and Customer distributed energy resources (DER) • Between DMS Applications and DA Field Equipment
11. Interfaces that use customer (residential, commercial, and industrial) site networks such as home area networks (HANs) and business area networks (BANs) • E.g. Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and Plug-in electric vehicle (PEV)
12. Interface to the Customer Site • E.g. Between Customer and Customer Information System (CIS) Web site • Between Third Party and HAN Gateway
13. Mobile Field Crew interfaces • E.g. Between field crews and GIS • Between field crews and substation equipment
14. Metering interface • E.g. Between sub-meter to meter • Between PEV meter to Energy Service Provider
15. Decision support interfaces • E.g. Between WAMS and ISO/RTO

3.2 IMPACT LEVELS

The IAC impact levels are low, moderate and high. The levels are defined in Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. Following are the definitions for confidentiality, integrity and availability, as defined in statute and a table that defines low, moderate, and high impact.

CONFIDENTIALITY

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

A loss of *confidentiality* is the unauthorized disclosure of information.

INTEGRITY

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

A loss of *integrity* is the unauthorized modification or destruction of information.

AVAILABILITY

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of *availability* is the disruption of access to or use of information or an information system.

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
			individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

3.3 LOGICAL INTERFACE CATEGORY DEFINITIONS

Included in this section are the category names and definitions, the constraints and issues aggregated from the individual interface definitions, and the CIA levels. For this draft, the CIA levels are specified for the critical data.

Category	Category Description	Examples
Category 1	**Control systems with high data accuracy and high availability, as well as media and compute constraints**	Between SCADA and field equipment
Constraints	• Media is usually narrowband, limiting the volume of traffic and impacting the types of security measures that are feasible. • Intelligent Electronic Devices (IEDs) can be limited in compute power, but that is becoming less of an issue as newer more capable devices become available. However, the large legacy of devices in the field will need be addressed through mitigating technologies and methods. • IEDs can be on pole tops and other insecure locations • Wireless media is often less expensive than wired media, which mean that wireless vulnerabilities exists, and will require security controls (either physical or cryptographic) appropriate for wireless	

	• None of the communication protocols currently used (primarily Distributed Network Protocol (DNP3) and sometimes International Electrotechnical Commission (IEC) 61850) are typically implemented with security measures, although IEC 62351 (which are the security standards for these protocols) is now available but implementation adoption and feasibility is not yet clear. • These functions have real-time operational requirements, with critical time latencies, which limits the choices for stopping or mitigating on-going attacks • Some of the equipment is legacy (particularly the Remote Terminal Units (RTUs) which limit the types of security controls that could be implemented without replacing or upgrading the equipment • Key management with thousands of devices is an issue that needs to be solved in terms of operational feasibility and cost. • Since confidentiality has not been perceived as important, and where the media and compute constraints apply, payload encryption may not necessarily be required for general messaging • Many of the SCADA Masters may have no way to add security without complete replacement • Many devices have no notion of a user or a role making security management a challenge. • Often no security event information available from these systems • No standard for security events or logging
Issues	There are critical and non-critical control systems. The requirements for availability will vary depending on a system's criticality and its impact on the power system.

Overall impacts		
	L, M, H	**Impact**
Confidentiality	L	Loss of confidentiality may lead to negative operational and/or financial impacts that affect the organization, but not the power system.
Integrity	H	Integrity is high because the corrupted data will result in bad decisions at the control and/or enterprise level that could lead to catastrophic adverse affects on the power system. (e.g. broad power outages or permanent damage to critical power assets)
Availability	H	The control path for critical systems must be available at all times. Large scale and distributed control systems can fail without high availability impacting critical power grid functions (e.g. SCADA, protection, etc.), which could result in widespread power outages if

		exploited by attackers. **Note:** There are critical and non-critical control systems. The requirements for availability will vary depending on a system's criticality and its impact on the power system.

Category	Category Description	Examples
Category 2	**Control systems with no bandwidth constraints (WAN), but are in different organizations**	Between an RTO/ISO EMS and a utility energy management system: • Transmission system real-time operational data from the transmission SCADA/EMS • Operational information, commands, requests from the ISO/RTO SCADA/EMS • Real-time transmission system, distribution system, and customer information data • Power flow results, including reliability and efficiency information • Real-time data, settings, and application results from analyses that are relevant to both systems
Constraints	• Different organizations can have different security policies, different enforcement levels, and different security technologies, thus possibly leading to interoperability issues, security gaps, and decreased availability of data. • The most commonly used protocol, IEC 60870-6 (ICCP), has authentication and encryption security through IEC 62351, but this security is not widely implemented. • These interactions may be one-way deliberately to minimize security vulnerabilities of cross-organizational data exchanges. For instance, the ISO/RTO may collect data using their own RTUs in the substation, and may just issue emails or other notifications to computers not directly connected to the SCADA/EMS. • Real-time data is being exchanged, with time latency requirements to within a few seconds. • Clear path with message priority must be provided for control commands and requests. • No major constraints on types of security measures such as encryption,	

	key management, etc. except for time-based control actions, as long as communications performance and timing requirements are met.
Issues	

Overall impacts		
	L, M, H	**Impact**
Confidentiality	M	Breach of confidentiality could lead to: • Loss of business confidence between partners • Diminished functional capabilities of the systems through loss of data exchange • Market manipulation • Possible litigation issues
Integrity	H	Loss of data integrity could result in huge financial consequences, or grid instability issues: • Incorrect or missing real-time data can cause erroneous results in the applications that could lead to reliability problems with the power system, ranging from trivial to serious. • Initial line of defense is the State Estimator bad data detector module, which highlights inconsistent and missing data in the power system data set being analyzed. • State estimator cannot detect aliasing errors which come from data sampling rates occurring at varying time intervals, leading to an inconsistent data set. • Inefficient operations, including incorrect response to market conditions for transmission paths and/or generation. • Lost or incorrect commands or requests could lead to similar types of impacts.
Availability	M	• By itself over a short period of time the loss of data availability is of medium to low impact depending on the data lost. The State Estimator application helps to fill-in missing data but can no longer determine which data is actually bad; results in loss of "observability" of some power system data. • The loss of data availability for extended periods of time could lead to inefficient operations of the power system.

Category	**Category Description**	**Examples**
Category 3	**Control Systems with no bandwidth constraints within the same organization**	Multiple DMS systems belonging the same utility

Constraints	• Because some data is real-time, security controls that introduce latency are undesirable.	
Issues	Not many security issues at this interface, unless the systems are organized into different security domains	
Overall impacts		
	L, M, H	**Impact**
Confidentiality	L	• Data constantly updating; confidentiality a low priority • No direct connection to customer data
Integrity	H	• LMS can impact pricing signals • Power system reliability, power system efficiency, utility and public safety, customer outages and power quality are impacted
Availability	H	• System reliability and efficiency

Category	**Category Description**	**Examples**
Category 4	**Back office systems under common management authority**	Between a customer information system and a meter data management system
Constraints	• Privacy can be a major issue related to sensitive customer information • Given the direct financial impacts to customers on their bills, accuracy (integrity) is crucial including inadvertent errors or incorrectly handled data • On both WAN and LAN configurations, no major constraints on types of security measures such as encryption, key management, authentication, etc • Privacy of the customer information may become an issue if sensitive data is provided to the GIS • Privacy of customer information within the CIS as well as collected through the AMI headend will be critical • Security for some commands such as remote connect/disconnect is of very high priority since the potential impact of disconnecting	
Issues		
Overall impacts		
	L, M, H	**Impact**
Confidentiality	H	• If customer privacy is breached, legal impacts, regulatory impacts, and loss of revenue could occur for the utility

		• If customer privacy is breached, the customer could suffer serious impacts with unknown ramifications
Integrity	H	• Loss of integrity of data can cause power outages, including massive outages if meters are disconnected without authorization • Loss of integrity of data could cause safety hazards for utility personnel, customer, and property
Availability	M	• Low availability could have legal and regulatory impacts if customers contractually should have access to energy usage data, PEV registration data, etc, in a timely manner.

Category	**Category Description**	**Examples**
Category 5	**Back office systems not under common management authority**	Between a third party billing system and a utility meter data management system
Constraints	• Cross-organizational interactions, which limit trust and compatibility of security policies and measures.	
Issues		
Overall impacts		
	L, M, H	**Impact**
Confidentiality	H	Unauthorized access to Customer usage data
Integrity	H	Unauthorized access to Customer usage data
Availability	L	Delays in billing and usage monitoring

Category	**Category Description**	**Examples**
Category 6	**Business to Business (B2B) connections**	Between a Retail aggregator and an Energy Clearinghouse
Constraints	• Load management signals, whether direct load control, indirect pricing, or energy request signals, can have profound effects on customer reactions. If these signals are compromised, serious power system consequences could result, as well as serious customer reactions to the Smart Grid. • These systems are usually organized into different security domains, so a firewall is necessary • Both the AMI network and the public Internet pose privacy and other security issues. The AMI network may have limited bandwidth for some types of exchanges. • The information exchange requirements between the DMS and the AMI	

	head-end, except for outage information, are not known. Local pricing or energy requests may come directly from the utility-owned DMS or may be routed through aggregators and other third parties. Most likely there will be variations across utilities and regulatory environments as to how these interactions become configured. • Cross-organizational interactions • Real-time operational requirements
Issues	

Overall impacts		
	L, M, H	**Impact**
Confidentiality	H	• Sensitive customer information is transmitted through some of these interfaces • Pricing signals can impact market decisions
Integrity	H	• Loss of data integrity can lead to power outages, including potentially wide-spread outages if data sources are reporting erroneous information • Loss of integrity of data could cause safety hazards for utility personnel, customers, and property
Availability	H	• Low availability can impact the quality of DMS/EMS actions, leading to inefficient system operation • Loss of electric network "observability " • May impact customer's access to data

Category	**Category Description**	**Examples**
Category 7	**Interfaces between control systems and non-control systems**	Between a GIS and a LMS/DRMS, or EMS and process information (PI) historian system
Constraints	• Load management signals whether direct load control or indirect pricing or energy request signals, can have profound effects on customer reactions. If these signals are compromised, serious power system consequences could result, as well as serious customer reactions to the Smart Grid. • These systems are usually organized into different security domains, so pertinent system separation measures must be taken (such as separate IP networks, a well configured firewall, etc.) • Both the AMI network and the public Internet pose privacy and other security issues. The AMI network may have limited bandwidth for some	

	types of information exchanges. • The information exchange requirements between the DMS and the AMI head-end, except for outage information, are not known. • Local pricing or energy requests may come directly from the utility-owned DMS or may be routed through aggregators and other 3rd parties. Most likely there will be variations across utilities and regulatory environments as to how these interactions become configured
Issues	

Overall impacts		
	L, M, H	**Impact**
Confidentiality	H	• Sensitive customer information is transmitted through some of these interfaces • Pricing signals can impact market decisions
Integrity	H	• Loss of data integrity can lead to power outages, including potentially wide-spread outages if data sources are reporting erroneous information • Loss of integrity of data could cause safety hazards for utility personnel, customers, and property
Availability	H	• Low availability can impact the quality of DMS/EMS actions, leading to inefficient system operation • Loss of electric network "observability " • May impact customer's access to data

Category	**Category Description**	**Examples**
Category 8	**Sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements**	Between temperature sensor on a transformer and its receiver
Constraints	• IED's and embedded sensors have limited computing power to authenticate each other • If any cryptography can exist in the nodes, usually consist on a shared key between all devices due to key management constraints • Rogue nodes can be added by attackers. This rogue nodes might have much more computing power than the real nodes • Media is usually narrowband, limiting the volume of traffic and impacting the types of security measures and protections that are feasible.	

	• IEDs can be on pole tops and other insecure locations • Wireless media is often less expensive than wired media, which means that wireless vulnerabilities exists, and will require security controls (either physical or cryptographic) appropriate for the wireless network. • None of the communication protocols currently used (primarily DNP3 and sometimes IEC 61850) are typically implemented with security measures, although IEC 62351 (which are the security standards for these protocols) is now available but implementation adoption and feasibility is not yet clear. • These functions have real-time operational requirements, with critical time latencies, which limits the choices for stopping or mitigating on-going attacks • Some of the equipment is legacy (particularly the RTUs) which limit the types of security controls that could be implemented without replacing or upgrading the equipment • Key management with thousands of devices is an issue that needs to be solved in terms of operational feasibility and cost. • Since confidentiality has not been perceived as important, and where the media and compute constraints apply, payload encryption may not necessarily be required for general messaging
Issues	This interface is highly important when the sensor network is remotely accessible. It is highly recommended that the sensor network be isolated architecturally and self-contained within a physically protected boundary, with point-to-point connections preferred.

Overall impacts		
	L, M, H	**Impact**
Confidentiality	L	Loss of confidentiality may lead to negative operational and/or financial impacts that affect the organization, but not the power system.
Integrity	H	If sensor access is over a remote link then impact is high. If the connection is point-to-point within a physically controlled area then the impact is low.
Availability	M	Losing one site will not necessarily cause a severe adverse affect to the broader power system.

Category	**Category Description**	**Examples**
Category 9	**Interfaces between sensor networks and control systems**	Between a sensor receiver and the substation master

Constraints	• Communications media is usually narrowband, limiting the volume of traffic and impacting the types of security measures that are feasible for cyber protection and monitoring. • IEDs can be limited in compute power, but that is becoming less of an issue as newer more capable devices become available. However, the large legacy of devices in the field will need be addressed through mitigating technologies and methods. • IEDs may be located on pole tops and other locations with limited physical security • Wireless media is often less expensive than wired media, which mean that wireless vulnerabilities exists, and will require security controls (physical or cryptographic) appropriate for wireless • None of the communication protocols currently used (primarily DNP3 and sometimes IEC 61850) are typically implemented with security measures, although IEC 62351 (which are the security standards for these protocols) is now available but implementation adoption and feasibility is not yet clear. • These functions have real-time operational requirements, with critical time latencies, which limits the choices for stopping or mitigating on-going attacks • Some of the equipment is legacy (particularly the RTUs) which limit the types of security controls that could be implemented without replacing or upgrading the equipment • Key management with thousands of devices is an issue that needs to be solved in terms of operational feasibility and cost. • Since confidentiality has not been perceived as important, and where the media and compute constraints apply, payload encryption may not necessarily be required for general messaging • Data is typically time stamped at the source of measurement so that data from various devices can be correlated when analyzing system events. Modifying the internal clock or altering the time stamp in data exchanges may impact the utility's ability to determine the root cause of a system event.	
Issues		
Overall impacts		
	L, M, H	**Impact**
Confidentiality	L	Loss of confidentiality may lead to negative operational and/or financial impacts that affect the organization, but not the power system.
Integrity	H	False sensor data can cause one to operate in an erroneous manner

		which can have catastrophic effect.
Availability	M	Losing one site may not cause a severe adverse affect to the broader power system.

Category	**Category Description**	**Examples**
Category 10	**Interfaces that use the AMI network**	• Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment
Constraints		
Issues		
Overall impacts		
	L, M, H	**Impact**
Confidentiality	L-M	Deduce usage patterns, costs, etc. marginal privacy issues
Integrity	M-H	Impact from erroneous data
Availability	L-M	Continue current operation state if no new info

Category	**Category Description**	**Examples**
Category 11	**Interfaces that use customer (residential, commercial, and industrial) site networks such as HANs and BANs**	• Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV
Constraints	• Microprocessor constraints on memory and compute capabilities • Real-time operational requirements • Legacy end-devices and systems • Legacy communication protocols	
Issues		
Overall impacts		
	L, M, H	**Impact**

Confidentiality	L-M	• Eavesdropping on electrical system management info
Integrity	L-H	• Individual consumer: High for overall system • Unauthorized manipulation of electrical management system
Availability	L-M	• Individual consumer: High for overall system • Failure to communicate HAN device to EMS

Category	**Category Description**	**Examples**
Category 12	**Interface to the Customer Site**	• Between Customer and CIS Web site • Between Third Party and HAN Gateway
Constraints	• Microprocessor constraints on memory and compute capabilities • Real-time operational requirements • Legacy end-devices and systems • Legacy communication protocols • Legal constraints	
Issues	• Many Platform and Network Vulnerabilities • The security of the Human Machine Interface (HMI) will depend on the overall network protection of the premises where they reside and communication (Local Area Network (LAN) vs. Wireless LAN (WLAN) • There is no standards for HMI, but documents exists on clearly presenting the information • The level of automation will increase the importance of availability (human vs. machine errors) • Authentication and re-authentication problematic for monitoring stations	
Overall impacts		
	L, M, H	**Impact**
Confidentiality	L-M	• Eavesdropping issues • Legal litigation concerns for data that is not open to public
Integrity	L-H	• Individual consumer: High for overall system • Manipulation of pricing information could adversely impact users financially (too low) or induce inappropriate demand response behavior (too high), both decreasing user confidence • Erroneous data may trigger erroneous modification of field

		equipment
Availability	L-H	• Individual consumer: High for overall system • Service should continue in the absence of pricing information, some negative impact from failure to notice increased prices possible • No feedback to field equipment. Impact depends of the criticality of the feedback to field equipments

Category	**Category Description**	**Examples**
Category 13	**Mobile Field Crew interfaces**	• Between field crews and GIS • Between field crews and substation equipment
Constraints	If narrowband wireless systems (e.g., trunked mobile radio systems) are used, they can limit the types of security that can be implemented, and can pose additional types of security vulnerabilities.	
Issues	• Use of public wireless systems (e.g., General Packet Radio Service (GPRS) can pose confidentiality and some availability concerns, including if the coverage is not complete. • Use of local wireless combined with WAN backhauls (e.g., WiFi in substations connected to the substation LAN and WAN) could also pose confidentiality concerns and availability (interference) concerns.	
Overall impacts		
	L, M, H	**Impact**
Confidentiality	M	Confidentiality is important to protect maps and "as built" information for a potential attacker
Integrity	H	Integrity is critical for safety and other reasons
Availability	M	Low availability could have financial impacts on the utility

Category	**Category Description**	**Examples**
Category 14	**Metering interface**	• Between sub-meter to meter • Between PEV meter to Energy Service Provider
Constraints	• The constraints are the meter's processor capacity, memory resources, network channel capacities, power restriction, thermal/environmental issues. These devices will dwell in harsh unprotected environments for long periods of time.	

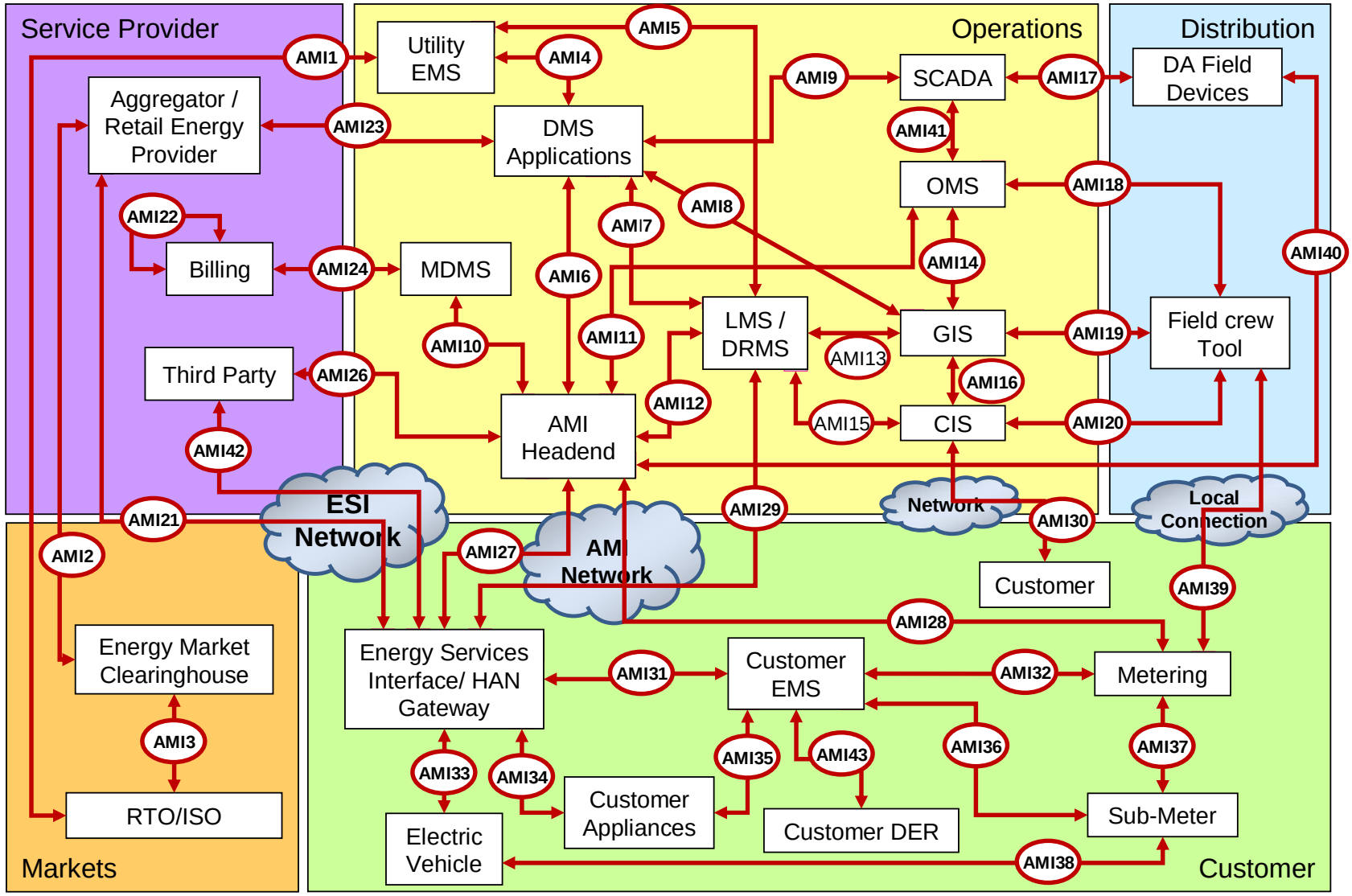
	• Regulatory concerns from the Federal Communications Commission and Public Utilities Commission.	
Issues	• Meters are used for utility revenue, and therefore, revenue protection is a very important issue for utilities. • Remote connect/disconnect control could be vulnerable to malicious use. • If sub-metering is used, the authenticity of the sub-meter must be proven to the customer meter so that the data can be trusted. Meters will be installed at customer sites in very physically unprotected areas.	
Overall impacts		
	L, M, H	**Impact**
Confidentiality	H	Customers can be very concerned that their energy usage patterns can reveal private issues
Integrity	H	Revenue metering requires high integrity. Also access to disconnect/reconnect controls must be protected
Availability	L	Delays in billing and energy usage monitoring are not critical, since the metering information can be retrieved at later times.

Category	**Category Description**	**Examples**
Category 15	**Decision support interfaces**	• Between WAMS and ISO/RTO
Constraints	• Cross-organizational interactions exchanging sensitive power system operational information with very many entities involved, such as all utilities in the Eastern interconnect • Real-time data flows result in very high data volume – making some crypto technologies problematic or costly, performance-wise. Aggregation points for wide-area data are particularly security-sensitive.	
Issues	• Although ISO/RTOs currently get sensitive power system operational information from member utilities, now the utilities would have access to sensitive information from other utilities, possibly from all utilities in an entire Interconnect • Many-to-many – entities have responsibility to secure – will require contractual arrangements	
Overall impacts		
	L, M, H	**Impact**
Confidentiality	M	Market manipulation
Integrity	H	• Operational reliability and potential equipment damage • EMS data is critical input for WAMS assessments (though

		conservative manual operation is still possible without WAMS, and some redundant data collection directly through SCADA systems is possible); Operational reliability and potential equipment damage
Availability	M	Could move to manual or more conservative operation modes – less optimal operations; impact might be low if operators are trained for manual operations and system has reserve capacity. In the future, manual operation may become more difficult as there is a loss of expertise in manual operation, meaning impact could be high.

Included below are the six functional priority area diagrams and interface allocation to these logical interface categories.

3.4 ADVANCED METERING INFRASTRUCTURE CATEGORIZATION OF INTERFACES



AMI Systems Use Cases: Actors, Logical Interfaces, and Networks

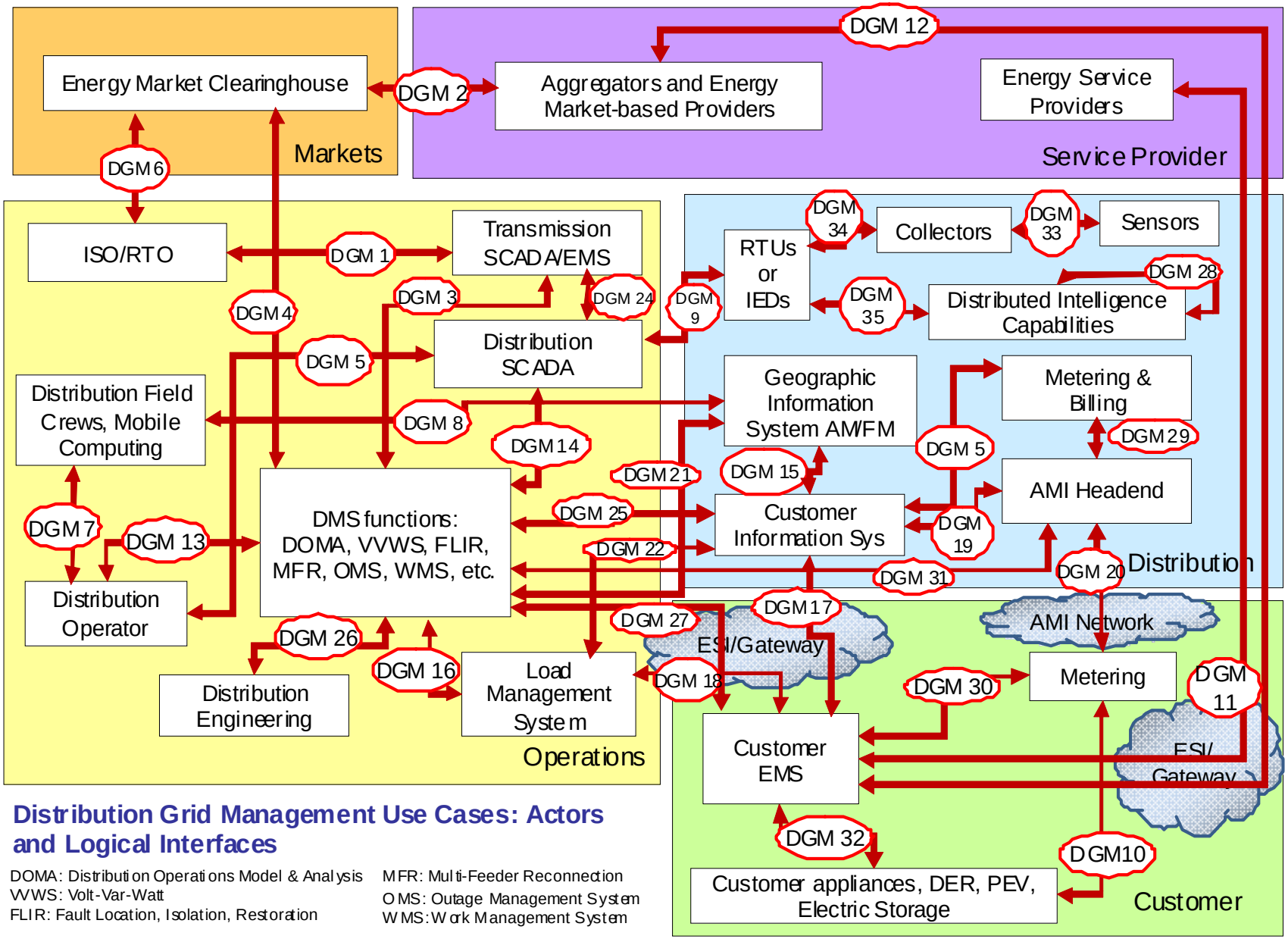
AMI: Advanced Metering Infrastructure
CIS: Customer Information System
DMS: Distribution Management System
DRMS: Demand Response Management System
EMS: Energy Management System
GIS: Geographic Information System
HAN: Home Area Network
ISO: Independent System Operator
LMS: Load Management System
OMS: Outage Management System
RTO: Regional Transmission Operator

The Logical Interfaces in the diagram were categorized according to their type, based on similarity of networks, constraints, and types of information.

Category	Logical Interfaces
1. Control systems with high data accuracy and high availability, as well as media and compute constraints • E.g. Between SCADA and field equipment	AMI17; AMI 40
2. Control systems with no bandwidth constraints (WAN) but are in different organizations • E.g. Between an RTO/ISO EMS and a utility energy management system	AMI1; AMI4; AMI5; AMI6
3. Control systems within the same organization with no bandwidth constraints • E.g. multiple DMS systems belonging to the same utility	AMI9; AMI41
4. Back office systems under common management authority • E.g. Between a CIS and a MDMS	AMI10; AMI11; AMI12; AMI16; AMI22
5. Back office systems not under common management authority • E.g. Between a third party billing system and a utility meter data management system	AMI23; AMI24
6. B2B connections • E.g. Between a Retail aggregator and an Energy Clearinghouse	AMI2; AMI3
7. Interfaces between control systems and non-control systems • E.g. between a GIS and a LMS/DRMS	AMI8; AMI13; AMI14; AMI15
8. Sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements • E.g. between temperature sensor on a transformer and its receiver	None
9. Interfaces between sensor networks and control systems • E.g. between a sensor receiver and the substation master	None
10. Interfaces that use the AMI network • E.g. Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	AMI26; AMI27; AMI29
11. Interfaces that use customer (residential, commercial, and industrial) site networks such as HANs and BANs • E.g. Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	AMI31; AMI32; AMI33; AMI34; AMI35; AMI36; AMI43

Category	Logical Interfaces
12. Interface to the Customer Site • E.g. Between Customer and CIS Web site • Between Third Party and HAN Gateway	AMI21; AMI30; AMI42
13. Mobile Field Crew interfaces • E.g. Between field crews and GIS • Between field crews and substation equipment	AMI18; AMI19; AMI20; AMI39
14. Metering interface • E.g. Between sub-meter to meter • Between PEV meter to Energy Service Provider	AMI28; AMI37; AMI38
15. Decision support interfaces • E.g. Between WAMS and ISO/RTO	None

3.5 DISTRIBUTED GRID MANAGEMENT CATEGORIZATION OF INTERFACES



Distribution Grid Management Use Cases: Actors and Logical Interfaces

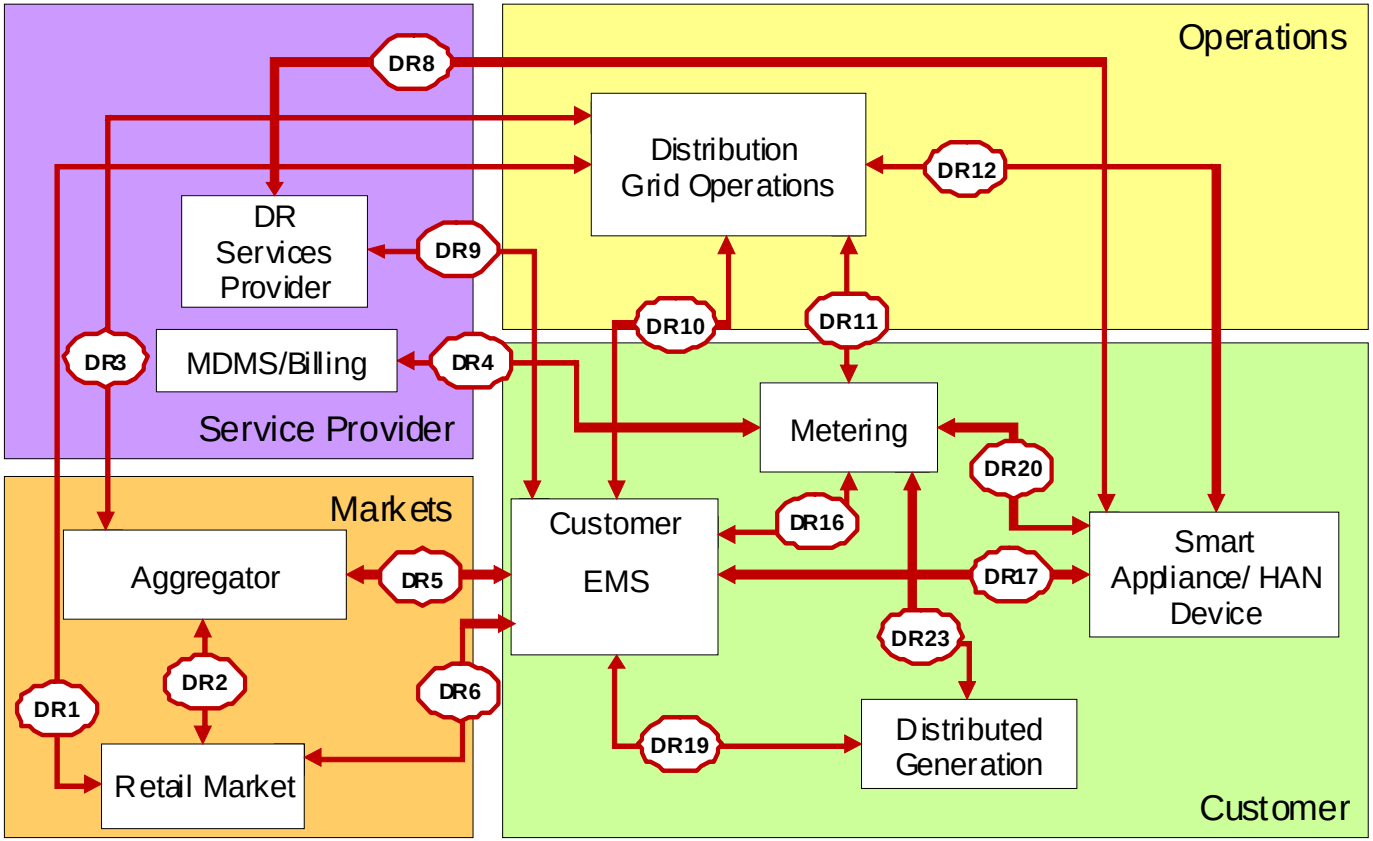
DOMA: Distribution Operations Model & Analysis
VVWS: Volt-Var-Watt
FLIR: Fault Location, Isolation, Restoration
MFR: Multi-Feeder Reconnection
OMS: Outage Management System
WMS: Work Management System

The Logical Interfaces in the diagram were categorized according to their type, based on similarity of networks, constraints, and types of information.

Category	Logical Interfaces
1. Control systems with high data accuracy and high availability, as well as media and compute constraints • E.g. Between SCADA and field equipment	DGM9
2. Control systems with no bandwidth constraints (WAN) but are in different organizations • E.g. Between an RTO/ISO EMS and a utility energy management system	DGM1; DGM3; DGM24
3. Control systems within the same organization with no bandwidth constraints • E.g. multiple DMS systems belonging to the same utility	DGM14; DGM16
4. Back office systems under common management authority • E.g. Between a CIS and a MDMS	DGM5; DGM15; DGM19; DGM29
5. Back office systems not under common management authority • E.g. Between a third party billing system and a utility meter data management system	None
6. B2B connections • E.g. Between a Retail aggregator and an Energy Clearinghouse	DGM2; DGM4; DGM6
7. Interfaces between control systems and non-control systems • E.g. between a GIS and a Load Management/Demand Response System	DGM18; DGM21; DGM22; DGM26; DGM25; DGM27
8. Sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements • E.g. between temperature sensor on a transformer and its receiver	DGM28 (for sensor networks); DGM33
9. Interfaces between sensor networks and control systems • E.g. between a sensor receiver and the substation master	DGM28 (peer-to-peer IED interactions); DGM34; DGM35
10. Interfaces that use the AMI network • E.g. Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	DGM11; DGM12; DGM17; DGM31

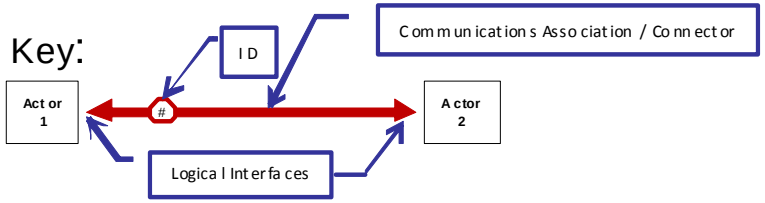
Category	Logical Interfaces
11. Interfaces that use customer (residential, commercial, and industrial) site networks such as HANs and BANs • E.g. Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	DGM10; DGM30; DGM32
12. Interface to the Customer Site • E.g. Between Customer and CIS Web site • Between Third Party and HAN Gateway	DGM13; DGM23
13. Mobile Field Crew interfaces • E.g. Between field crews and GIS • Between field crews and substation equipment	DGM7; DGM8
14. Metering interface • E.g. Between sub-meter to meter • Between PEV meter to Energy Service Provider	DGM20
15. Decision support interfaces • E.g. Between WAMS and ISO/RTO	None

3.6 DEMAND RESPONSE CATEGORIZATION OF INTERFACES



Demand Response Use Cases: Actors and Logical Interfaces

HAN: Home Area Network
EMS: Energy Management System
DR: Demand Response

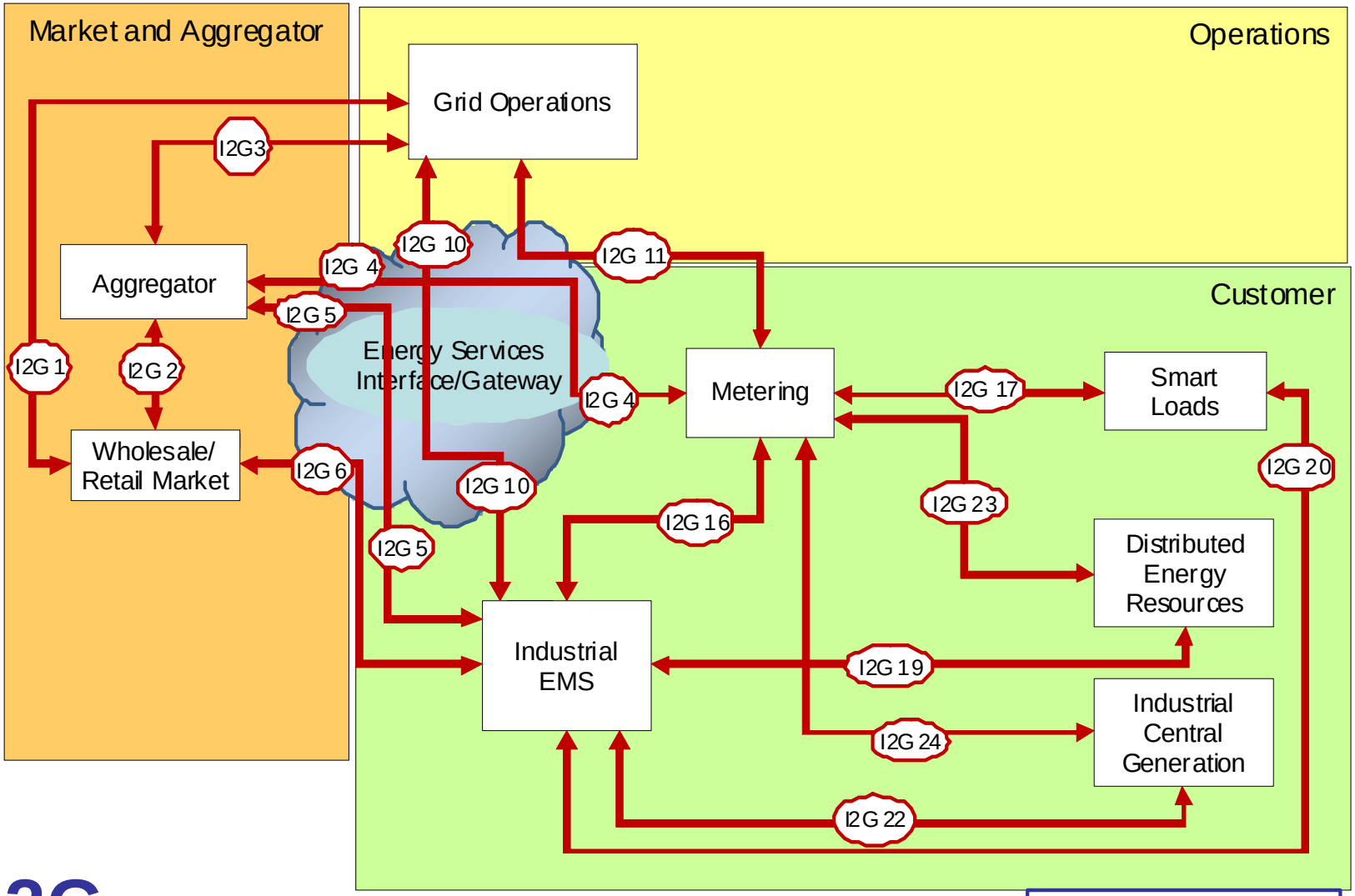


The Logical Interfaces in the diagram were categorized according to their type, based on similarity of networks, constraints, and types of information.

Category	Logical Interfaces
1. Control systems with high data accuracy and high availability, as well as media and compute constraints • E.g. Between SCADA and field equipment	DR12
2. Control systems with no bandwidth constraints (WAN) but are in different organizations • E.g. Between an RTO/ISO EMS and a utility energy management system	None
3. Control systems within the same organization with no bandwidth constraints • E.g. multiple DMS systems belonging to the same utility	None
4. Back office systems under common management authority • E.g. Between a Customer Information System and a Meter Data Management System	None
5. Back office systems not under common management authority • E.g. Between a third party billing system and a utility meter data management system	None
6. B2B connections • E.g. Between a Retail aggregator and an Energy Clearinghouse	DR1; DR2; DR3
7. Interfaces between control systems and non-control systems • E.g. between a GIS and a Load Management/Demand Response System	None
8. Sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements • E.g. between temperature sensor on a transformer and its receiver	None
9. Interfaces between sensor networks and control systems • E.g. between a sensor receiver and the substation master	None
10. Interfaces that use the AMI network • E.g. Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	None

Category	Logical Interfaces
11. Interfaces that use customer (residential, commercial, and industrial) site networks such as HANs and BANs • E.g. Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	DR17; DR19
12. Interface to the Customer Site • E.g. Between Customer and CIS Web site • Between Third Party and HAN Gateway	DR5; DR6; DR8; DR9; DR10
13. Mobile Field Crew interfaces • E.g. Between field crews and GIS • Between field crews and substation equipment	None
14. Metering interface • E.g. Between sub-meter to meter • Between PEV meter to Energy Service Provider	DR4; DR11; DR16; DR20; DR22
15. Decision support interfaces • E.g. Between WAMS and ISO/RTO	None

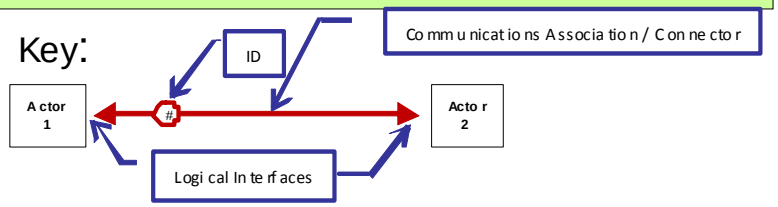
3.7 I2G DEMAND RESPONSE CATEGORIZATION OF INTERFACES



I2G Demand Response Use Cases: Actors and Logical Interfaces

ESI: Energy Services Interface
EMS: Energy Management System
DR: Demand Response

Key:



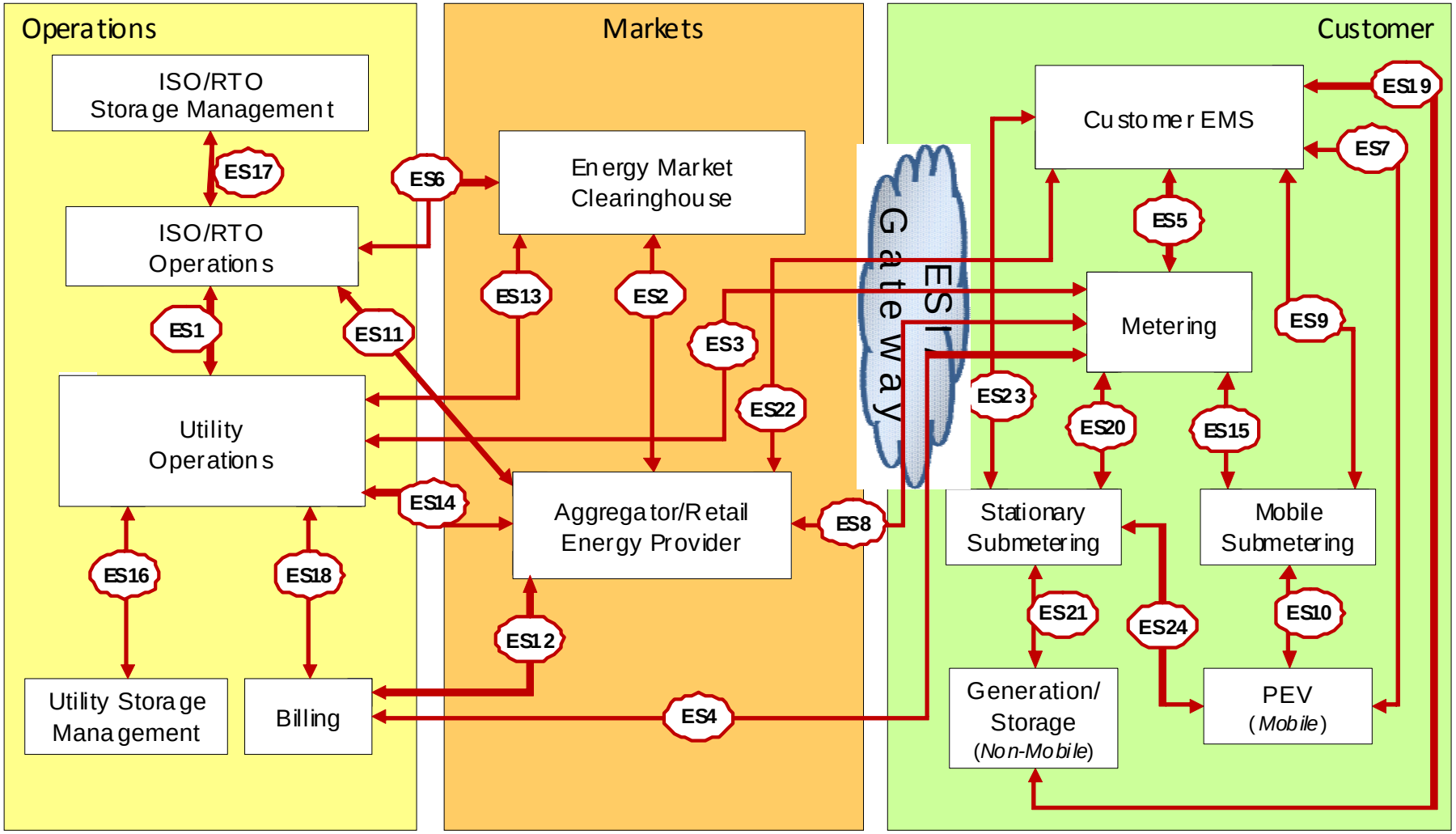
The Logical Interfaces in the diagram were categorized according to their type, based on similarity of networks, constraints, and types of information.

Category	Logical Interfaces
1. Control systems with high data accuracy and high availability, as well as media and compute constraints • E.g. Between SCADA and field equipment	None
2. Control systems with no bandwidth constraints (WAN) but are in different organizations • E.g. Between an RTO/ISO EMS and a utility energy management system	None
3. Control systems within the same organization with no bandwidth constraints • E.g. multiple DMS systems belonging to the same utility	None
4. Back office systems under common management authority • E.g. Between a Customer Information System and a Meter Data Management System	None
5. Back office systems not under common management authority • E.g. Between a third party billing system and a utility meter data management system	None
6. B2B connections • E.g. Between a Retail aggregator and an Energy Clearinghouse	I2G1; I2G2; I2G3
7. Interfaces between control systems and non-control systems • E.g. between a Geographic Information System and a Load Management/Demand Response System	None
8. Sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements • E.g. between temperature sensor on a transformer and its receiver	None
9. Interfaces between sensor networks and control systems • E.g. between a sensor receiver and the substation master	None
10. Interfaces that use the AMI network • E.g. Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	None

Category	Logical Interfaces
11. Interfaces that use customer (residential, commercial, and industrial) site networks such as HANs and BANs • E.g. Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	I2G19; I2G20; I2G22
12. Interface to the Customer Site • E.g. Between Customer and CIS Web site • Between Third Party and HAN Gateway	I2G5; I2G6; I2G10
13. Mobile Field Crew interfaces • E.g. Between field crews and GIS • Between field crews and substation equipment	None
14. Metering interface • E.g. Between sub-meter to meter • Between PEV meter to Energy Service Provider	I2G4; I2G11; I2G16; I2G17; I2G23; I2G24
15. Decision support interfaces • E.g. Between WAMS and ISO/RTO	None

3.8 ELECTRIC STORAGE CATEGORIZATION OF INTERFACES

Electric Storage Use Cases: Actors and Logical Interfaces



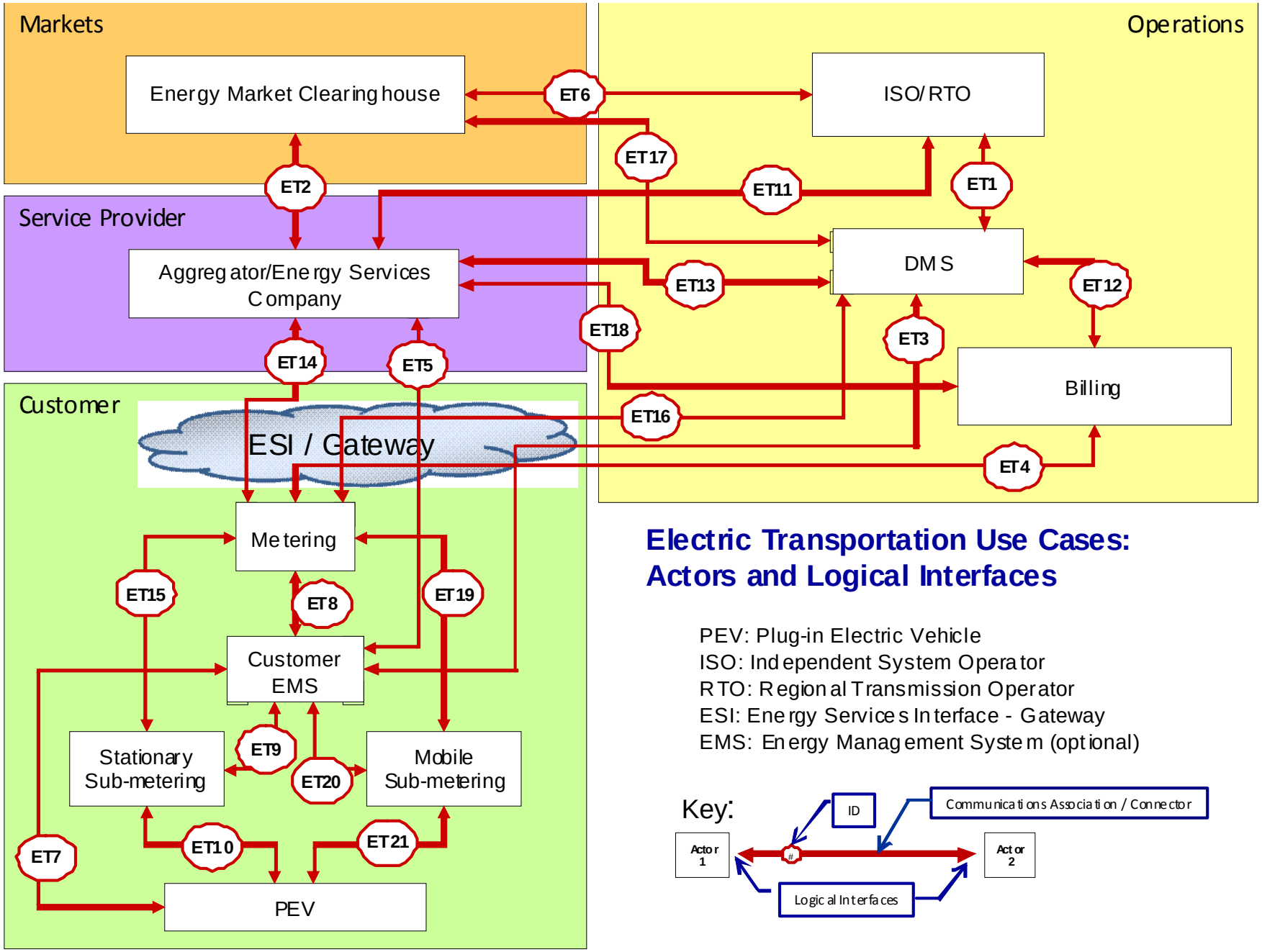
EMS: Energy Management System
ESI: Energy Services Interface
ISO: Independent System Operator
PEV: Plug-in Electric Vehicle
RTO: Regional Transmission Operator

The Logical Interfaces in the diagram were categorized according to their type, based on similarity of networks, constraints, and types of information.

Category	Logical Interfaces
1. Control systems with high data accuracy and high availability, as well as media and compute constraints • E.g. Between SCADA and field equipment	None
2. Control systems with no bandwidth constraints (WAN) but are in different organizations • E.g. Between an RTO/ISO EMS and a utility energy management system	ES1
3. Control systems within the same organization with no bandwidth constraints • E.g. multiple DMS systems belonging to the same utility	ES16; ES17
4. Back office systems under common management authority • E.g. Between a CIS and a MDMS	ES18
5. Back office systems not under common management authority • E.g. Between a third party billing system and a utility meter data management system	ES11; ES14
6. B2B connections • E.g. Between a Retail aggregator and an Energy Clearinghouse	ES2; ES6; ES12; ES13
7. Interfaces between control systems and non-control systems • E.g. between a Geographic Information System and a Load Management/Demand Response System	None
8. Sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements • E.g. between temperature sensor on a transformer and its receiver	None
9. Interfaces between sensor networks and control systems • E.g. between a sensor receiver and the substation master	None
10. Interfaces that use the AMI network • E.g. Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	None
11. Interfaces that use customer (residential, commercial, and industrial) site networks such as HANs and BANs • E.g. Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	ES7; ES19

Category	Logical Interfaces
12. Interface to the Customer Site • E.g. Between Customer and CIS Web site • Between Third Party and HAN Gateway	ES22
13. Mobile Field Crew interfaces • E.g. Between field crews and GIS • Between field crews and substation equipment	None
14. Metering interface • E.g. Between sub-meter to meter • Between PEV meter to Energy Service Provider	ES3; ES4; ES5; ES8; ES9; ES10; ES15; ES20; ES21; ES23; ES24
15. Decision support interfaces • E.g. Between WAMS and ISO/RTO	None

3.9 ELECTRIC TRANSPORTATION CATEGORIZATION OF INTERFACES



Electric Transportation Use Cases: Actors and Logical Interfaces

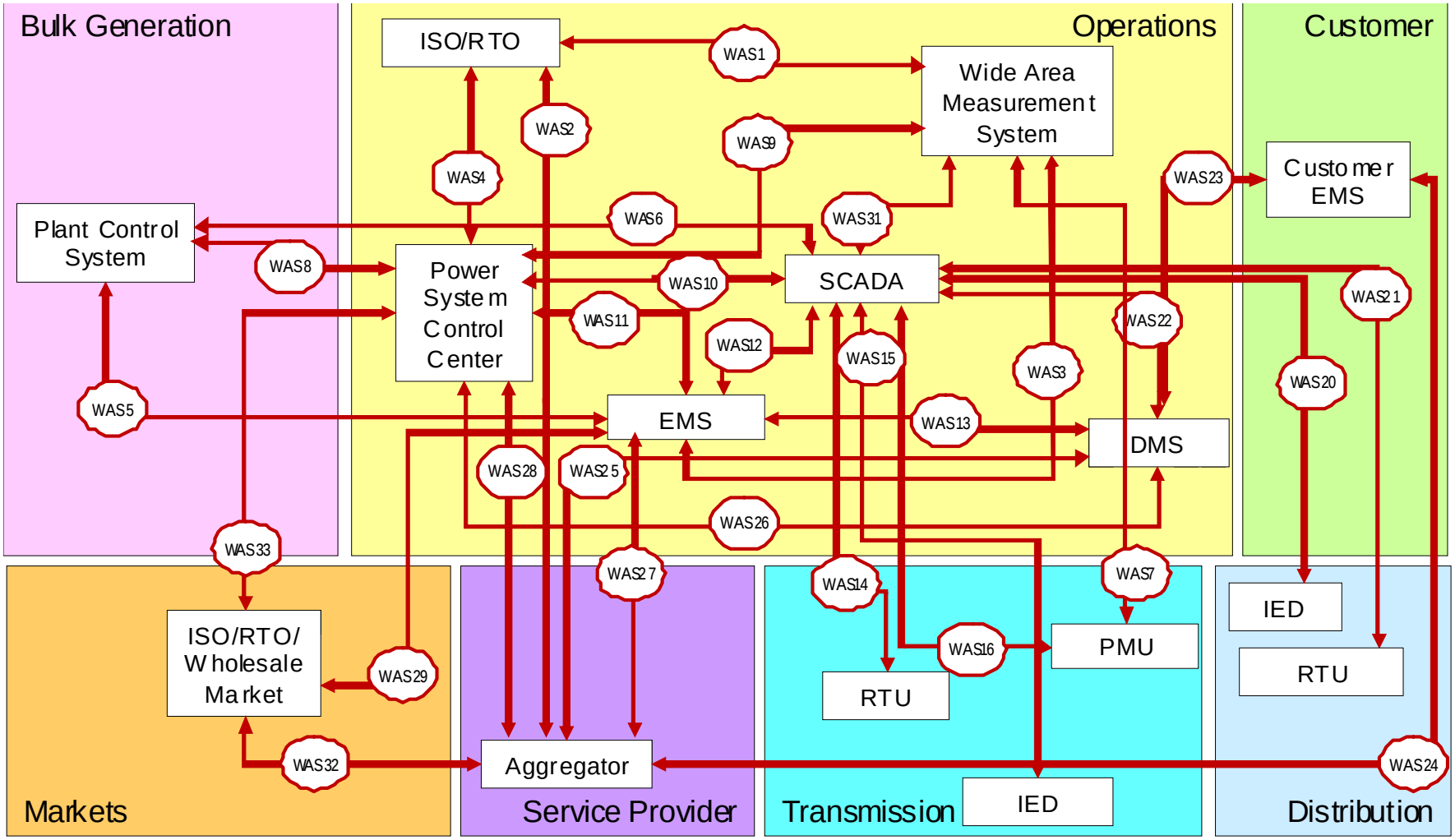
PEV: Plug-in Electric Vehicle
ISO: Independent System Operator
RTO: Regional Transmission Operator
ESI: Energy Services Interface - Gateway
EMS: Energy Management System (optional)

The Logical Interfaces in the diagram were categorized according to their type, based on similarity of networks, constraints, and types of information.

Category	Logical Interfaces
1. Control systems with high data accuracy and high availability, as well as media and compute constraints • E.g. Between SCADA and field equipment	None
2. Control systems with no bandwidth constraints (WAN) but are in different organizations • E.g. Between an RTO/ISO EMS and a utility energy management system	ET1
3. Control systems within the same organization with no bandwidth constraints • E.g. multiple DMS systems belonging to the same utility	None
4. Back office systems under common management authority • E.g. Between a Customer Information System and a Meter Data Management System	None
5. Back office systems not under common management authority • E.g. Between a third party billing system and a utility meter data management system	ET12
6. B2B connections • E.g. Between a Retail aggregator and an Energy Clearinghouse	ET2; ET6; ET11; ET13; ET17; ET18
7. Interfaces between control systems and non-control systems • E.g. between a Geographic Information System and a Load Management/Demand Response System	None
8. Sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements • E.g. between temperature sensor on a transformer and its receiver	None
9. Interfaces between sensor networks and control systems • E.g. between a sensor receiver and the substation master	None
10. Interfaces that use the AMI network • E.g. Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	None

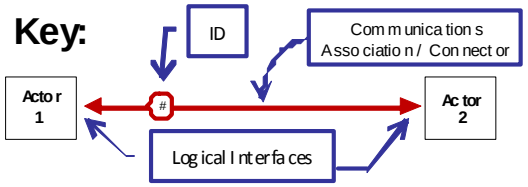
Category	Logical Interfaces
11. Interfaces that use customer (residential, commercial, and industrial) site networks such as HANs and BANs • E.g. Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	ET7
12. Interface to the Customer Site • E.g. Between Customer and CIS Web site • Between Third Party and HAN Gateway	ET3; ET5
13. Mobile Field Crew interfaces • E.g. Between field crews and GIS • Between field crews and substation equipment	None
14. Metering interface • E.g. Between sub-meter to meter • Between PEV meter to Energy Service Provider	ET4; ET8; ET9; ET10; ET14; ET15; ET16; ET19; ET20; ET21
15. Decision support interfaces • E.g. Between WAMS and ISO/RTO	None

3.10 WIDE-AREA SITUATIONAL AWARENESS CATEGORIZATION OF INTERFACES



Wide-Area Situational Awareness (WASA) Use Cases: Actors and Logical Interfaces

IED: Intelligent Electronic Device
DMS: Distribution Management System
EMS: Energy Management System
SCADA: Supervisory Control and Data Acquisition
AMI: Advanced Metering Infrastructure



The Logical Interfaces in the diagram were categorized according to their type, based on similarity of networks, constraints, and types of information.

Category	Logical Interfaces
1. Control systems with high data accuracy and high availability, as well as media and compute constraints • E.g. Between SCADA and field equipment	WAS14; WAS15; WAS20; WAS21
2. Control systems with no bandwidth constraints (WAN) but are in different organizations • E.g. Between an RTO/ISO EMS and a utility energy management system	WAS4; WAS5; WAS6; WAS8; WAS10; WAS11; WAS12; WAS13; WAS22; WAS26
3. Control systems within the same organization with no bandwidth constraints • E.g. multiple DMS systems belonging to the same utility	None
4. Back office systems under common management authority • E.g. Between a Customer Information System and a Meter Data Management System	None
5. Back office systems not under common management authority • E.g. Between a third party billing system and a utility meter data management system	None
6. B2B connections • E.g. Between a Retail aggregator and an Energy Clearinghouse	WAS29; WAS32; WAS33
7. Interfaces between control systems and non-control systems • E.g. between a Geographic Information System and a Load Management/Demand Response System	WAS2; WAS25; WAS27; WAS28; WAS31
8. Sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements • E.g. between temperature sensor on a transformer and its receiver	None
9. Interfaces between sensor networks and control systems • E.g. between a sensor receiver and the substation master	None
10. Interfaces that use the AMI network • E.g. Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	None
11. Interfaces that use customer (residential, commercial, and industrial) site networks such as HANs and BANs • E.g. Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	None

Category	Logical Interfaces
12. Interface to the Customer Site • E.g. Between Customer and CIS Web site • Between Third Party and HAN Gateway	WAS23; WAS24
13. Mobile Field Crew interfaces • E.g. Between field crews and GIS • Between field crews and substation equipment	None
14. Metering interface • E.g. Between sub-meter to meter • Between PEV meter to Energy Service Provider	None
15. Decision support interfaces • E.g. Between WAMS and ISO/RTO	WAS1; WAS3; WAS9

3.11 ALL INTERFACES BY CATEGORY

Following is a roll-up of the allocation of logical interfaces to the categories.

Category	Logical Interfaces
1. Control systems with high data accuracy and high availability, as well as media and compute constraints • E.g. Between SCADA and field equipment	AMI17; AMI 40; DR12; DGM9; WAS14; WAS15; WAS20; WAS21
2. Control systems with no bandwidth constraints (WAN) but are in different organizations E.g. Between an RTO/ISO EMS and a utility energy management system	AMI1; AMI4; AMI5; AMI6; DGM1; DGM3; DGM24; ES1; ET1; WAS4; WAS5; WAS6; WAS8; WAS10; WAS11; WAS12; WAS13; WAS22; WAS26
3. Control systems within the same organization with no bandwidth constraints • E.g. multiple DMS systems belonging to the same utility	AMI9; AMI41; DGM14; DGM16; ES16; ES17
4. Back office systems under common management authority • E.g. Between a Customer Information System and a Meter Data Management System	AMI10; AMI11; AMI12; AMI16; AMI22; DGM5; DGM15; DGM19; DGM29; ES18
5. Back office systems not under common management authority • E.g. Between a third party billing system and a utility meter data management system	AMI23; AMI24; ES11; ES14; ET12

Category	Logical Interfaces
6. B2B connections • E.g. Between a Retail aggregator and an Energy Clearinghouse	AMI2; AMI3; DGM2; DGM4; DGM6; DR1; DR2; DR3; I2G1; I2G2; I2G3; ES2; ES6; ES12; ES13; ET2; ET6; ET11; ET13; ET17; ET18; WAS29; WAS32; WAS33
7. Interfaces between control systems and non-control systems • E.g. between a Geographic Information System and a Load Management/Demand Response System	AMI8; AMI13; AMI14; AMI15; DGM18; DGM21; DGM22; DGM26; DGM25; DGM27; WAS2; WAS25; WAS27; WAS28; WAS31
8. Sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements • E.g. between temperature sensor on a transformer and its receiver	DGM28 (for sensor networks); DGM33
9. Interfaces between sensor networks and control systems • E.g. between a sensor receiver and the substation master	DGM28 (peer-to-peer IED interactions); DGM34; DGM35
10. Interfaces that use the AMI network • E.g. Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	AMI26; AMI27; AMI29; DGM11; DGM12; DGM17; DGM31
11. Interfaces that use customer (residential, commercial, and industrial) site networks such as HANs and BANs • E.g. Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	AMI31; AMI32; AMI33; AMI34; AMI35; AMI36; AMI43; DGM10; DGM30; DGM32; DR17;DR19; I2G19; I2G20; I2G22; ES7; ES19; ET7
12. Interface to the Customer Site • E.g. Between Customer and CIS Web site • Between Third Party and HAN Gateway	AMI21; AMI30; AMI42; DGM13; DGM23; DR5; DR6; DR8; DR9; DR10; I2G5; I2G6; I2G10; ES22; ET3; ET5; WAS23; WAS24
13. Mobile Field Crew interfaces • E.g. Between field crews and GIS • Between field crews and substation equipment	AMI18; AMI19; AMI20; AMI39; DGM7; DGM8

Category	Logical Interfaces
14. Metering interface • E.g. Between sub-meter to meter • Between PEV meter to Energy Service Provider	AMI28; AMI37; AMI38; DGM20; DR4; DR11; DR16; DR20; DR22; I2G4; I2G11; I2G16; I2G17; I2G23; I2G24; ES3; ES4; ES5; ES8 ES9; ES10; ES15; ES20; ES21; ES23; ES24; ET4; ET8; ET9; ET10; ET14; ET15; ET16; ET19; ET20; ET21
15. Decision support interfaces • E.g. Between WAMS and ISO/RTO	WAS1; WAS3; WAS9

CHAPTER 4

AMI SECURITY REQUIREMENTS

The following security requirements were developed by ASAP-SG. They are included in the document *Security Profile for Advanced Metering Infrastructure*, Version 0.44, *September 17, 2009*. This document was published by the ASAP-SG for the The UtiliSec Working Group (UCAIug) and the NIST Cyber Security Coordination Task Group. The AMI requirements have been included here with permission of the ASAP-SG.

The requirements cited are the initial set covering only a subset of interfaces identified in Chapter 3, Logical Interface Analysis. The CSCTG will continue its work in developing security requirements for the remainder of the interfaces in subsequent versions of this NISTIR. DHS numbering to identify requirements is used for traceability purposes.

4.1 AMI RECOMMENDED REQUIREMENTS

The following requirements are adapted from the DHS Catalog of Control Systems Security[8] and have been modified or extended as appropriate for AMI security. The DHS requirement section numbers are only provided for traceability, and not intended to indicate that the requirements in this document are the DHS requirements themselves. When the ASAP-SG team created requirements for which there was no DHS counterpart, the "ASAP-" prefix is used instead of "DHS-". For each requirement, the NIST SP 800-53 reference is included.

DHS-2.8 System and Communication Protection

System and communication protection consists of steps taken to protect the AMI components and the communication links between system components from cyber intrusions. Although AMI system and communication protection might logically include both physical and cyber protection, this section addresses only cyber protection. Physical protection is addressed in Section 2.4 of the DHS controls.

DHS-2.8.1/NIST SP 800-53 SC-1 System and Communication Protection Policy and Procedures

DHS-2.8.1.1 Requirement:

The organization shall develop, disseminate, and periodically review and update:

1. A formal, documented system and communication protection policy that addresses:
    1. The purpose of the AMI system and communication protection policy as it relates to protecting the organization's personnel and assets;
    2. The scope of the AMI system and communication protection policy as it applies to all the organizational staff and third-party contractors;

[8] Department of Homeland Security, National Cyber Security Division. 2008, January. Catalog of Control Systems Security: Recommendations for Standards Developers. Retrieved from http://www.us-cert.gov/control_systems/

3. The roles, responsibilities and management accountability structure of the security program to ensure compliance with the organization's system and communications protection policy and other regulatory commitments;

2. Formal, documented procedures to facilitate the implementation of the AMI system and communication protection policy and associated systems and communication protection controls.

DHS-2.8.1.2 Supplemental Guidance:

The organization shall ensure the AMI system and communication protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The AMI system and communication protection policy needs to be included as part of the general information security policy for the organization. System and communication protection procedures can be developed for the security program in general, and an AMI system in particular, when required.
These documents also need to include a documented plan that covers the policies and procedures that cover a breach in security.

DHS-2.8.1.3 Requirement Enhancements:

None.

DHS-2.8.2 Management Port Partitioning

DHS-2.8.2.1 Requirement:

AMI components must separate telemetry/data acquisition services from management port functionality.

DHS-2.8.2.2 Supplemental Guidance:

The AMI system management port needs to be physically or logically separated from telemetry/data acquisition services and information storage and management services (e.g., database management) of the system. Separation may be accomplished by using different computers, different central processing units, different instances of the operating systems, different network addresses or protocol ports (e.g., TCP ports), combinations of these methods, or other methods as appropriate. Such precautions reduce the risk of allowing access to a data acquisition server and can help limit the damage of a compromised system.
Configuration and testing ports for AMI components should be disabled when not in use. Depending on the criticality of the system it may be advised that a device be physically disconnected.

DHS-2.8.2.3 Requirement Enhancements:

None.

DHS-2.8.3/ NIST SP 800-53 SC-7 Security Function Isolation

DHS-2.8.3.1 Requirement:

AMI components must isolate security functions from non-security functions.

DHS-2.8.3.2 Supplemental Guidance:

AMI components must isolate security functions from non-security functions by means of partitions, domains, etc., including control of access to and integrity of the hardware, software, and firmware that perform those functions. The AMI system maintains a separate execution domain (e.g., address space) for each executing process. Some AMI components may not implement this capability. In situations where it is not implemented, the organization details its risk acceptance and mitigation in the AMI system security plan
The AMI system must employ the following underlying hardware separation mechanisms to facilitate security function isolation:

1. Each AMI component isolates critical security functions (i.e., functions enforcing access and information flow control) from both non-security functions and from other security functions;
2. Each AMI component minimizes the number of non – security functions included within the isolatio boundary containing security functions;
3. AMI security functions are implemented as largely independent modules that avoid unnecessary interactions between modules;
4. In each AMI component, security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.
5. Passwords and/or security keys should be of limited value, avoiding significant reuse of keys or passwords between different components and users. For example, compromising one key must not allow compromise of an entire network.

DHS-2.8.3.3 Requirement Enhancements:

None.

DHS-2.8.4/ NIST SP 800-53 SC-4 Information Remnants

DHS-2.8.4.1 Requirement:

AMI components shall prevent unauthorized or unintended information transfer via shared system resources.

DHS-2.8.4.2 Supplemental Guidance:

Control of information system remnants, sometimes referred to as object reuse, or data remnants, must prevent information, including cryptographically protected representations of information previously produced by the AMI system, from being available to any current user/role/process that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Such information must be cleared before freeing the resource for other use.

DHS-2.8.4.3 Requirement Enhancements:

None.

DHS-2.8.5/ NIST SP 800-53 SC-5 Denial-of-Service Protection

DHS-2.8.5.1 Requirement:

AMI components shall protect against or limit the effects of denial-of-service attacks.

DHS-2.8.5.2 Supplemental Guidance:

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial-of-service attacks. For example, network perimeter devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial-of-service attacks.

1. The AMI system must restrict the ability of users to launch denial-of-service attacks against other AMI components or networks.
2. The AMI system must manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.
3. Wireless assets and networks are also vulnerable to radio-frequency jamming and steps must be taken and personnel trained to address tracking and resolution of such issues. This may include radio-frequency direction finding and other such technologies.

DHS-2.8.5.3 Requirement Enhancements:

None.

DHS-2.8.6/ NIST SP 800-53 SC-6 Resource Priority

DHS-2.8.6.1 Requirement:

AMI components must limit the use of resources by priority.

DHS-2.8.6.2 Supplemental Guidance:

Priority protection helps prevent a lower-priority process from delaying or interfering with the AMI system servicing any higher-priority process.

DHS-2.8.6.3 Requirement Enhancements:

None.

DHS-2.8.7/ NIST SP 800-53 SC-2, SC-7, SC-32 Boundary Protection

DHS-2.8.7.1 Requirement:

The organization shall define the external boundary(ies) of the AMI system. Procedural and policy security functions must define the operational system boundary, the strength required of the boundary, and the respective barriers to unauthorized access and control of system assets and components. The AMI system monitors and manages communications at the operational system boundary and at key internal boundaries within the system. In AMI, the very concept of boundaries is problematic. Internal systems within the organization may be more easily protected than components which reside outside significant physical boundaries and controls.

Meters and poll-top and other systems without significant controls and external monitoring cannot be amply secured and should always be considered relatively untrusted.

DHS-2.8.7.2 Supplemental Guidance:

Any connection to the Internet or other external network or computer system needs to occur through managed interfaces (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels). AMI system boundary protections at any designated alternate processing/control sites must provide the same levels of protection as that of the primary site.
At this time components and systems connected to the Internet constitute a substantial increase in risk for the core functionality of the AMI system. Connections to the Internet and other public networks is discouraged for AMI systems.
The HAN is not controlled or owned by the utility, and should be treated as a hostile network by the AMI meter. Because of this, we recommend that AMI components should not request or accept information from HAN components. We recommend that AMI components should only push traffic to the home area network.
The following guidance also applies:

1. The organization physically must locate publicly accessible AMI system components to separate sub networks with separate, physical network interfaces. Publicly accessible AMI system components include, for example, public web servers. Generally, no AMI system information should be publicly accessible;
2. The organization must prevent public access into the organization's internal AMI system networks except as appropriately mediated and monitored;
3. The organization shall limit the number of access points to the AMI system to allow for better monitoring of inbound and outbound network traffic;
4. The organization shall implement a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing security measures appropriate to the required protection of the integrity and confidentiality of the information being transmitted;
5. The AMI system shall deny network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).
6. The organization shall prevent the unauthorized release of information outside of the AMI system boundary or any unauthorized communication through the AMI system boundary when there is an operational failure of the boundary protection mechanisms.
7. Field service tools should not interface to the meter through the HAN.

DHS-2.8.7.3 Requirement Enhancements:

None.

DHS-2.8.8/ NIST SP 800-53 SC-8 Communication Integrity

DHS-2.8.8.1 Requirement:

The AMI system design and implementation must protect the integrity of electronically communicated information.

DHS-2.8.8.2 Supplemental Guidance:

If the organization is relying on a commercial service provider for communication services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security measures for transmission integrity. When it is infeasible or impractical to obtain the necessary assurances of effective security through appropriate contracting vehicles, the organization must either implement appropriate compensating security measures or explicitly accepts the additional risk. Contracts and other legal documents with vendors should allow for security and integrity testing of products and services used in the AMI systems.

DHS-2.8.8.3 Requirement Enhancements:

1. The organization shall employ cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures. The level of protection that is required is determined by the sensitivity of the data being transmitted. (e.g., protective distribution systems).
2. The use of cryptography within an AMI system will introduce latency to AMI system communication. The latency introduced from the use of cryptographic mechanisms must not degrade the operational performance of the AMI system or impact personnel safety.
3. Failure of a cryptographic mechanism must not create a denial of service or fail to an unprotected open state. Alternative systems should be in place in case of such failure. AMI systems generally support the objectives of availability, integrity, and confidentiality.

DHS-2.8.9/ NIST SP 800-53 SC-9 Communication Confidentiality

DHS-2.8.9.1 Requirement:

The AMI system design and implementation must protect the confidentiality of communicated information where necessary.

DHS-2.8.9.2 Supplemental Guidance:

The use of a third-party communication service provider instead of organization owned infrastructure may warrant the use of encryption. The use of cryptographic mechanisms within an AMI system could introduce communications latency due to the additional time and computing resources required to encrypt, decrypt, and authenticate each message. Any latency induced from the use of cryptographic mechanisms must not degrade the operational performance of the AMI system.

DHS-2.8.9.3 Requirement Enhancements:

None.

DHS-2.8.10/ NIST SP 800-53 SC-11 Trusted Path

DHS-2.8.10.1 Requirement:

The AMI system must establish trusted communications paths between the user (or agent) and the components making up the AMI system.

DHS-2.8.10.2 Supplemental Guidance:

A trusted path is employed for high-confidence connections between the security functions of the AMI system and the meter. It is recommended that login to the field service tool interface be protected by a trusted path or a compensating control. A trusted path is a mechanism by which a meter can communicate directly with the Trusted Computing Base (TCB) that provides the security functions of the system. This mechanism can only be activated by the authorized user or the TCB. The TCB is the totality of protection mechanisms within an AMI system – including hardware, firmware, and software – the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel and parameters (e.g., a user's clearance) related to the security policy.

DHS-2.8.10.3 Requirement Enhancements:

None.

DHS-2.8.11/ NIST SP 800-53 SC-12 Cryptographic Key Establishment and Management

DHS-2.8.11.1 Requirement:

When cryptography is required and employed within the AMI system, the organization shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

DHS-2.8.11.2 Supplemental Guidance:

Organizations need to select cryptographic protection that matches the value of the information being protected and the AMI system operating constraints. A formal written policy needs to be developed to document the practices and procedures relating to cryptographic key establishment and management. These policies and procedures need to address, under key establishment, such items as the key generation process is in accordance with a specified algorithm and key sizes are based on an assigned standard. Key generation needs to be performed using an effective random number generator. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution in accordance with defined standards.

DHS-2.8.11.3 Requirement Enhancements:

None.

DHS-2.8.12/ NIST SP 800-53 SC-13 Use of Validated Cryptography

DHS-2.8.12.1 Requirement:

The organization shall develop and implement a policy governing the use of cryptographic mechanisms for the protection of AMI system information. The organization ensures all cryptographic mechanisms comply with applicable laws, regulatory requirements, directives, policies, standards, and guidance.

DHS-2.8.12.2 Supplemental Guidance:

Any cryptographic modules deployed within an AMI system, at a minimum, must be able to meet the Federal Information Processing Standard (FIPS) 140-2. Assessment of the modules must include validation of the cryptographic modules operating in approved modes of operation. The most effective safeguard is to use a cryptographic module validated by the Cryptographic Module Validation Program. Additional information on the use of validated cryptography can be found at http://csrc.nist.gov/cryptval.

DHS-2.8.12.3 Requirement Enhancements:

1. The organization protects cryptographic hardware from physical tampering and uncontrolled electronic connections.
2. The organization selects cryptographic hardware with remote key management capabilities.

DHS-2.8.13/ NIST SP 800-53 SC-15 Collaborative Computing N/A

DHS-2.8.13.1 Requirement:

The use of collaborative computing mechanisms on AMI components is strongly discouraged and provides an explicit indication of use to the local users.
Alternative statement: Given the current state of this technology and/or the ability to secure it would substantially increase the security risk at this time.

DHS-2.8.13.2 Supplemental Guidance:

Collaborative computing mechanisms include, for example, video and audio conferencing capabilities or instant messaging technologies. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.

DHS-2.8.13.3 Requirement Enhancements:

If collaborative computing mechanisms are utilized on the AMI system, they are disconnected and powered down when not in use.

DHS-2.8.14/ NIST SP 800-53 SC-16 Transmission of Security Parameters

DHS-2.8.14.1 Requirement:

The AMI components must reliably associate security parameters (e.g., security labels and markings) with information exchanged between the enterprise information systems and the AMI system.

DHS-2.8.14.2 Supplemental Guidance:

Security parameters may be explicitly or implicitly associated with the information contained within the AMI system.

DHS-2.8.14.3 Requirement Enhancements:

None.

DHS-2.8.15/ NIST SP 800-53 SC-17 Public Key Infrastructure Certificates

DHS-2.8.15.1 Requirement:

The organization shall issue public key certificates under an appropriate certificate policy or obtain public key certificates under an appropriate certificate policy from an approved service provider.

DHS-2.8.15.2 Supplemental Guidance:

Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

DHS-2.8.15.3 Requirement Enhancements:

Any latency induced from the use of public key certificates must not degrade the operational performance of the AMI system.

DHS-2.8.16/ NIST SP 800-53 SC-18 Mobile Code

DHS-2.8.16.1 Requirement:

The organization shall:

1. Establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the AMI system if used maliciously;
2. Document, monitor, and manage the use of mobile code within the AMI system.

Appropriate organizational officials should authorize the use of mobile code.
Given the current state of this technology and the limited ability to secure it, use of mobile code substantially increases the security risk at this time.

DHS-2.8.16.2 Supplemental Guidance:

Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance need to apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. procedures need to prevent the development, acquisition, or introduction of unacceptable mobile code within the AMI system. Additional information on risk-based approaches for the implementation of mobile code technologies can be found at https://iase.disa.mil/mcp/index.html.
Mobile code should not be used in the configuration for management interfaces for components on the AMI system. Example: HTTP Web interface for AMI network aggregator.

DHS-2.8.16.3 Requirement Enhancements:

None.

DHS-2.8.17/ NIST SP 800-53 SC-19 Voice-Over Internet Protocol

DHS-2.8.17.1 Requirement:

The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and limits the use of VOIP within the AMI system. Given the current state of this technology and/or the ability to secure it would substantially increase the security risk at this time.

DHS-2.8.17.2 Supplemental Guidance:

Generally, VOIP technologies should not be employed on AMI systems. If VOIP is used in support of field services it should not be considered secure. Customer information, passwords or other security information should not be transmitted.

DHS-2.8.17.3 Requirement Enhancements:

None.

DHS-2.8.18/ NIST SP 800-53 CA-3 System Connections

DHS-2.8.18.1 Requirement:

All external AMI components and communication connections must be identified and adequately protected from tampering or damage.

DHS-2.8.18.2 Supplemental Guidance:

External access point c//onnections to the AMI system must be secured to protect the system. Access points include any externally connected communication end point (for example, dial-up modems) terminating at any component within the electronic security perimeter. The first step in securing these connections is to identify the connections along with the purpose and necessity of the connection. This information must be documented, tracked, and audited periodically. After identifying these connection points, the extent of their protection needs to be determined. Policies and procedures must be developed and implemented to protect the connection to the business or enterprise information system. This might include disabling the connection except when specific access is requested for a specific need, automatic timeout for the connection, etc.

DHS-2.8.18.3 Requirement Enhancements:

None.

DHS-2.8.19/ NIST SP 800-53 SA-9 Security Roles

DHS-2.8.19.1 Requirement:

The AMI system design and implementation must specify the security roles and responsibilities for the users of the system.

DHS-2.8.19.2 Supplemental Guidance:

Security roles and responsibilities for AMI system users must be specified, defined, and implemented based on the sensitivity of the information handled by the AMI system. These roles may be defined for specific task and data handled.

DHS-2.8.19.3 Requirement Enhancements:

None.

DHS-2.8.20/ NIST SP 800-53 SC-8 Message Authenticity

DHS-2.8.20.1 Requirement:

The AMI system must provide mechanisms to protect the authenticity of device-to-device communications.

DHS-2.8.20.2 Supplemental Guidance:

Message authentication provides protection from malformed traffic from mis-configured components and malicious entities.

DHS-2.8.20.3 Requirement Enhancements:

Message authentication mechanisms should be implemented at the protocol level for both serial and routable protocols.

DHS-2.8.21/ NIST SP 800-53 SC-22 Architecture and Provisioning for Name/Address Resolution Service

DHS-2.8.21.1 Requirement:

AMI components that collectively provide name/address resolution services for an organization must be fault tolerant and implement address space separation.

DHS-2.8.21.2 Supplemental Guidance:

In general, do not use domain name system (DNS) services on an AMI system. Host-based name resolution solutions are the recommended practice. However, if DNS services are implemented, it is recommended to deploy at least two authoritative DNS servers. The DNS configuration on the host will reference one DNS server as the primary source and the other as the secondary source. Additionally, locate the two DNS servers on different network subnets and separate geographically. If AMI system resources are accessible from external networks, establish authoritative DNS servers with separate address space views (internal and external) to the AMI system resources. The DNS server with the internal view provides name/address resolution services within the AMI system boundary. The DNS server with the external view only provides name/address resolution information pertaining to AMI system resources accessible from external resources. The list of clients who can access the authoritative DNS server with a particular view must also specified.

DHS-2.8.21.3 Requirement Enhancements:

The use of secure name/address resolution services must not adversely impact the operational performance of the AMI system.

DHS-2.8.22/ NIST SP 800-53 SC20 Secure Name / Address Resolution Service (Authoritative Source)

DHS-2.8.22.1 Requirement:

The AMI system resource (i.e., authoritative DNS server) that provides name/address resolution service must provide additional artifacts (e.g., digital signatures and cryptographic keys) along with the authoritative DNS resource records it returns in response to resolution queries.

DHS-2.8.22.2 Supplemental Guidance:

In general, do not use DNS services on an AMI system. Host-based name resolution solutions are best practice. This requirement enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A DNS server is an example of AMI system resource that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

DHS-2.8.22.3 Requirement Enhancements:

None.

DHS-2.8.23/ NIST SP 800-53 SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

DHS-2.8.23.1 Requirement:

The AMI system resource (i.e., resolving or caching name server) that provides name/address resolution service for local clients shall perform data origin authentication and data integrity verification on the resolution responses it receives from authoritative DNS servers when requested by client systems.

DHS-2.8.23.2 Supplemental Guidance:

In general, do not use DNS services on an AMI system. Host-based name resolution solutions are best practice. A resolving or caching DNS server is an example of an AMI system resource that provides name/address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

DHS-2.8.23.3 Requirement Enhancements:

The AMI system resource that implements DNS services performs data origin authentication and data integrity verification on all resolution responses whether or not local DNS clients (i.e., stub resolvers) explicitly request this function.

ASAP-2.8.24 Secure Name/Address Resolution Service (Address Resolution Tampering)

ASAP-2.8.24.1 Requirement:

The organization shall monitor address resolution traffic to identify potentially malicious patterns of behavior.

ASAP-2.8.24.2 Supplemental Guidance:

Appropriate components or programming must be included within the AMI networks to identify potentially malicious address-resolution behavior (eg. ARP spoofing/cache poisoning). Such behavior should be identified, tracked, and the appropriate incident handling team-members alerted.

ASAP-2.8.24.3 Requirement Enhancements:

ARP spoofing and similar attacks may allow an attacker to subvert natural automated network behavior in order to all the attacker to get "in the middle" of valid communication. Such attacks, when successful, may allow traffic to be captured, analyzed, and possibly even modified in-transit.

DHS-2.9 Information and Document Management

Information and document management is generally a part of the company records retention and document management system. Digital and hardcopy information associated with the development and execution of AMI components is important, sensitive, and needs to be managed. AMI components design, operations data and procedures, risk analyses, business impact studies, risk tolerance profiles, etc. contain sensitive company information and needs to be protected. Security measures, philosophy, and implementation strategies are other examples. Additionally, business conditions change and require updated analyses and studies. Care is given to protect this information and verify that the appropriate versions are retained. Inherent in this is an information classification system that allows information assets to receive the appropriate level of protection.
The following are the controls for Information and Document Management that need to be supported and implemented by the organization to protect the AMI components.

DHS-2.9.1 Information and Document Management Policy and Procedures

DHS-2.9.1.1 Requirement:

The organization shall develop, disseminate, and periodically review/update:

1. A formal, documented, AMI system information and document management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the AMI system information and document management policy and associated system maintenance controls.

DHS-2.9.1.2 Supplemental Guidance:

The organization must ensure that the AMI system information and document management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The AMI system information and document management policy can be included as part of the general information security policy for the organization. System information and document management procedures can be developed for the security program in general, and for a particular AMI component, when required.

DHS-2.9.1.3 Requirement Enhancements:

None.

DHS-2.9.2 Information and Document Retention

DHS-2.9.2.1 Requirement:

The organization shall manage AMI components related data, including establishing retention policies and procedures for both electronic and paper data, and must manage access to the data based on formally assigned roles and responsibilities.

DHS-2.9.2.2 Supplemental Guidance:

The organization shall develop policies and procedures detailing the retention of company information. These procedures address retention/destruction issues for all applicable information media. Any legal or regulatory requirements are considered when developing these policies and procedures. Information associated with the development and execution of an AMI system is important, sensitive, and needs to be appropriately managed.

DHS-2.9.2.3 Requirement Enhancements:

The organization shall perform legal reviews of the retention policies to ensure compliance with all applicable laws and regulations.

DHS-2.9.3/ NIST SP 800-53 MP-1 Information Handling

DHS-2.9.3.1 Requirement:

Organization implemented policies and procedures detailing the handling of information should be developed and periodically reviewed and updated.

DHS-2.9.3.2 Supplemental Guidance:

Written policies and procedures detail access, sharing, copying, transmittal, distribution, and disposal or destruction of AMI system information. These policies or procedures include the periodic review of all information to ensure it is being properly handled. The organization shall protect information against unauthorized access, misuse, or corruption during transportation or transmission. The organization shall distribute or shares information on a need-to-know basis and considers legal and regulatory requirements when developing these policies and procedures.

DHS-2.9.3.3 Requirement Enhancements:

None.

DHS-2.9.4/ NIST SP 800-53 RA-2 Information Classification

DHS-2.9.4.1 Requirement:

All information related to AMI components is classified to indicate the protection required commensurate with its sensitivity and consequence.

DHS-2.9.4.2 Supplemental Guidance:

It is recommended that a minimum of three levels of classification be defined for information related to AMI components to indicate the protection required commensurate with its sensitivity and consequence. These levels may be company proprietary, restricted, or public, indicating the need, priority, and level of protection required for that information. These information classification levels provide guidance for access and control to include sharing, copying, transmittal, and distribution appropriate for the level of protection required.

DHS-2.9.4.3 Requirement Enhancements:

None.

DHS-2.9.5 Information Exchange

DHS-2.9.5.1 Requirement:

Formal contractual and confidentiality agreements are established for the exchange of information and software between the organization and external parties.

DHS-2.9.5.2 Supplemental Guidance:

When it is necessary for the AMI components to communicate information to another organization or external party system, the operators need to mutually develop a formal contractual and confidentiality agreement and use a secure method of communication. These formal exchange policies, procedures, and security controls need to be in place to protect the exchange of information through the use of all types of communication facilities.

DHS-2.9.5.3 Requirement Enhancements:

If a specific component needs to communicate with another component outside the AMI system network, communications must be limited to only the components that need to communicate. All other ports and routes must to be locked down or disabled.

DHS-2.9.6 Information and Document Classification

DHS-2.9.6.1 Requirement:

The organization shall develop policies and procedures to classify data, including establishing:

1. Retention policies and procedures for both electronic and paper media;
2. Classification policies and methods, (e.g., restricted, classified, general, etc.).;
3. Access and control policies, to include sharing, copying, transmittal, and distribution appropriate for the level of protection required;

4. Access to the data based on formally assigned roles and responsibilities for various components of AMI system

DHS-2.9.6.2 Supplemental Guidance:

Companies use both comprehensive information and document management policies for their cyber security management system. Inherent in this is an information classification system that allows information assets to receive the appropriate level of protection. The organization defines information classification levels (e.g., restricted, classified, general, etc.) for access and control to include sharing, copying, transmittal, and distribution appropriate for the level of protection required. The organization also classifies all information (i.e., AMI system design information, network diagrams, process programs, vulnerability assessments, etc.) to indicate the need, priority, and level of protection required commensurate with its sensitivity and consequence.

DHS-2.9.6.3 Requirement Enhancements:

The organization periodically reviews information that requires special control or handling to determine whether such special handling is still required.

DHS-2.9.7 Information and Document Retrieval

DHS-2.9.7.1 Requirement:

The organization shall develop policies and procedures that provide details of the retrieval of written and electronic records, equipment, and other media for components of the AMI system in the overall information and document management policy.

DHS-2.9.7.2 Supplemental Guidance:

The organization shall employ appropriate measures to ensure long-term records information can be retrieved (i.e., converting the data to a newer format, retaining older equipment that can read the data, etc.). Any legal or regulatory requirements are considered when developing these policies and procedures. The organization must take special care to confirm the security, availability, and usability of the AMI components configuration, which includes the logic used in developing the configuration or programming for the life of AMI system.

DHS-2.9.7.3 Requirement Enhancements:

None.

DHS-2.9.8 Information and Document Destruction

DHS-2.9.8.1 Requirement:

The organization shall develop policies and procedures detailing the destruction of written and electronic records, equipment, and other media for the AMI components, without compromising the confidentiality of the data.

DHS-2.9.8.2 Supplemental Guidance:

The organization shall develop policies and procedures detailing the destruction and disposal of written and electronic records, equipment, and other media in the overall information and

document management policy. This also includes the method of disposal, such as shredding of paper records, erasing of disks or other electronic media, or physical destruction. All legal or regulatory requirements need to be considered when developing these policies and procedures.

DHS-2.9.8.3 Requirement Enhancements:

None.

DHS-2.9.9 Information and Document Management Review

DHS-2.9.9.1 Requirement:

The organization shall perform periodic reviews of compliance with the AMI system information and document security management policy to ensure compliance with any laws and regulatory requirements.

DHS-2.9.9.2 Supplemental Guidance:

The organization shall regularly review compliance in the information and document management security policy. The compliance review procedure needs to consider all legal and regulatory documentation requirements applicable to the AMI system.

DHS-2.9.9.3 Requirement Enhancements:

None.

DHS-2.9.10/ NIST SP 800-53 AC-15 Automated Marking

DHS-2.9.10.1 Requirement:

The components of AMI system shall automatically mark any external data output (physical/paper output) using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

DHS-2.9.10.2 Supplemental Guidance:

Automated marking refers to markings employed on external media (e.g., hardcopy documents output from the AMI components).

DHS-2.9.10.3 Requirement Enhancements:

None.

DHS-2.10 System Development and Maintenance

DHS-2.10.1/ NIST SP 800-53 MA-1 System Maintenance Policy and Procedures

DHS-2.10.1.1 Requirement:

The organization shall develop, disseminate, and regularly review and update:

1. A documented policy for maintenance of all components of the AMI system. These documents address purpose, scope, roles, responsibilities, coordination among organizational entities, and compliance testing.
2. Documented procedures for implementing the maintenance policy.

DHS-2.10.1.2 Supplemental Guidance:

The organization must ensure that the maintenance policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The maintenance policy can be included as part of the general information security policy for the organization. Maintenance policies and procedures can be developed for the security program in general and for particular components of the AMI system when required.

DHS-2.10.1.3 Requirement Enhancements:

None.

DHS-2.10.2 Legacy System Upgrades

DHS-2.10.2.1 Requirement:

The organization shall develop policies and procedures to upgrade all legacy components of the AMI system to include security mitigating measures needed to bring all elements of the AMI system into compliance with current security requirements commensurate with the organization's risk tolerance for those components.

DHS-2.10.2.2 Supplemental Guidance:

Legacy systems are those components currently in place as part of a working AMI system. In some cases, these systems were installed before there was a concern about system security, and hence, security mitigation measures were not included. The organization determines the current security configuration of legacy components and updates or replaces hardware and software as required.

DHS-2.10.2.3 Requirement Enhancements:

None.

DHS-2.10.3/ NIST SP 800-53 CA-2 System Monitoring and Evaluation

DHS-2.10.3.1 Requirement:

The organization shall regularly evaluate all components of the AMI system for security vulnerabilities and for compliance with its maintenance and security policies. All components of the AMI system are updated or replaced to address identified vulnerabilities or non-compliance issues in accordance with the maintenance policy and procedures.

DHS-2.10.3.2 Supplemental Guidance:

The frequency of evaluations is based on the organization's risk mitigation policy. Changing security requirements and discovery of vulnerabilities necessitate a review. These reviews must

be carefully planned and documented in accordance with the organization's maintenance policies and procedures.

DHS-2.10.3.3 Requirement Enhancements:

None.

DHS-2.10.4/ NIST SP 800-53 CP-6 Backup and Recovery

DHS-2.10.4.1 Requirement:

The organization shall secure backups of critical software, applications, and data for all components of the AMI system. The organization shall backup all data and applications needed to replace failed components within a reasonable period of time, and as required to satisfy regulatory requirements. Backups shall be physically separated from the operational components.

DHS-2.10.4.2 Supplemental Guidance:

AMI components may be compromised due to an incident or disaster. A copy of essential software and data must to be made, updated regularly, and stored in a secure environment for later use to restore the system to normal operations.

DHS-2.10.4.3 Requirement Enhancements:

None.

DHS-2.10.5/ NIST SP 800-53 PL-6 Unplanned System Maintenance

DHS-2.10.5.1 Requirement:

The organization shall review and follow security requirements before undertaking any unplanned maintenance on any component of the AMI system. Unplanned maintenance must be documented and include the following:

1. The date and time of maintenance;
2. The name of the individual(s) performing the maintenance;
3. A description of the maintenance performed; If physical access or modification is required, also document the following:
    - The name of the escort, if necessary;
    - A list of equipment removed or replaced (including identification numbers, if applicable).

DHS-2.10.5.2 Supplemental Guidance:

Unplanned maintenance is required to support system operation in the event of system/component malfunction or failure. Security requirements necessitate that all unplanned maintenance activities use approved contingency plans and document all actions taken to restore operability to the system.

DHS-2.10.5.3 Requirement Enhancements:

The organization documents the decision and justification should unplanned maintenance not be performed after the identification of a security vulnerability.

DHS-2.10.6/ NIST SP 800-53 MA-2 Periodic System Maintenance

DHS-2.10.6.1 Requirement:

The organization schedules, performs, and documents routine preventive and regular maintenance for all components of the AMI system in accordance with manufacturer or vendor specifications and/or organizational policies and procedures.

DHS-2.10.6.2 Supplemental Guidance:

Hardware maintenance includes planned replacement of functional equipment (e.g., deployment of new routers). Software maintenance (e.g., patches), like hardware maintenance, requires taking components off-line for some period of time. All maintenance must be approved by the appropriate organization official(s) and planned to avoid significant impact on operations. After maintenance is performed, the organization checks the security features to ensure that they are still functioning properly.

DHS-2.10.6.3 Requirement Enhancements:

The organization keeps a maintenance record for the system that includes the date and time of maintenance, the name of the individual(s) performing the maintenance, the name of the escort (if necessary), a description of the maintenance performed, and a list of equipment removed or replaced (including identification numbers, if applicable).
The organization employs automated mechanisms to schedule and conduct maintenance as required and to create up-to-date, accurate, complete, and available records of all maintenance actions, both needed and completed.
Before disposal of equipment, all critical/sensitive information (e.g., keys) must be removed using approved procedures.

ASAP-2.10.7/ NIST SP 800-53 MA-3 Field Tools

ASAP-2.10.7.1 Requirement:

The organization shall approve, manage, protect, and monitor the use of field tools and maintains the integrity of these tools on an ongoing basis.

ASAP-2.10.7.2 Supplemental Guidance:

The intent of this requirement is to address hardware and software connected to component of the AMI system for diagnostics and repairs (e.g., a hardware or software packet sniffer introduced for a particular maintenance activity). Field tools include, for example, diagnostic and test equipment used to conduct maintenance on the network's software or hardware. Hardware and/or software components that may support maintenance yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this requirement.

ASAP-2.10.7.3 Requirement Enhancements:

1. The organization shall check all media containing diagnostic and test programs for malicious code before the media are used in the AMI system.
2. The organization shall check all field tools that can retain information so that no sensitive information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed unless an appropriate organization official explicitly authorizes an exception.

DHS-2.10.8/ NIST SP 800-53 MA-5 Maintenance Personnel

DHS-2.10.8.1 Requirement:

The organization shall document authorization and approval policies and procedures and maintains a list of personnel authorized to perform maintenance. Only authorized and qualified organization or vendor personnel perform maintenance.

DHS-2.10.8.2 Supplemental Guidance:

Maintenance personnel must have appropriate access authorization when maintenance activities allow access to organizational information that could result in a future compromise of availability, integrity, or confidentiality. When maintenance personnel do not have required access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities.

DHS-2.10.8.3 Requirement Enhancements:

None.

DHS-2.10.9/ NIST SP 800-53 MA-4 Remote Maintenance

DHS-2.10.9.1 Requirement:

The organization shall authorize, manage, and monitor remotely executed maintenance and diagnostic activities on all components of the AMI system. When remote maintenance is completed, the organization or AMI component must terminate all sessions and remote connections invoked in the performance of that activity.

DHS-2.10.9.2 Supplemental Guidance:

Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools must be consistent with organizational policy and documented in the security plan. The organization shall maintain records for all remote maintenance and diagnostic activities.

DHS-2.10.9.3 Requirement Enhancements:

The organization audits all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions.

The organization shall address the installation and use of remote maintenance and diagnostic links in the security plan.

DHS-2.12 Incident Response

DHS-2.12.1/ NIST SP 800-53 IR-1 Incident Response Policy and Procedures

DHS-2.12.1.1 Requirement: The organization shall develop, disseminate, and periodically review and update:

A documented incident response policy that addresses purpose, scope, roles, responsibilities, coordination among organizational entities, and compliance; and
Documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

DHS-2.12.1.2 Supplemental Guidance:

The organization must ensure the incident response policy and procedures are consistent with applicable laws, directives, policies, regulations, standards, and guidance.

DHS-2.12.1.3 Requirement Enhancements:

None.

DHS-2.12.2/ NIST SP 800-53 CP-1 Continuity of Operations Plan

DHS-2.12.2.1 Requirement:

The organization shall develop and implement a continuity of operations plan dealing with the overall issue of maintaining or re-establishing operation of the AMI system in case of an undesirable interruption. The plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring system operations after a disruption or failure. Designated officials within the organization review and approve the continuity of operations plan.

DHS-2.12.2.2 Supplemental Guidance:

A continuity of operations plan addresses both business continuity planning and recovery of all vital components of the AMI system.

DHS-2.12.2.3 Requirement Enhancements:

Following a disruption, the organization initiates a root cause analysis for the event and submits any findings from the analysis to the organizations corrective action program.

DHS-2.12.3/ NIST SP 800-53 CP-2 Continuity of Operations Roles and Responsibilities

DHS-2.12.3.1 Requirement:

The organization's continuity of operations plan shall define and communicate the specific roles and responsibilities for each part of the plan in relation to various types of disruptions to the operation of the AMI system.

DHS-2.12.3.2 Supplemental Guidance:

The continuity of operations plan defines the roles and responsibilities of the various employees and contractors in the event of a significant incident. The plans identify responsible personnel to lead the recovery and response effort if an incident occurs.

DHS-2.12.3.3 Requirement Enhancements:

None.

DHS-2.12.4/ NIST SP 800-53 IR-2 Incident Response Training

DHS-2.12.4.1 Requirement:

The organization shall train personnel in their continuity of operations plan roles and responsibilities with respect to the AMI system. The organization provides refresher training annually. The training covers employees, contractors, and stakeholders in the implementation of the continuity of operations plan.

DHS-2.12.4.2 Supplemental Guidance:

None.

DHS-2.12.4.3 Requirement Enhancements:

Incident response retraining must include the annual dissemination of information concerning the organizations incident response plan to utility customers.

DHS-2.12.5/ NIST SP 800-53 CP-4, IR-3 Continuity of Operations Plan Testing

DHS-2.12.5.1 Requirement:

The organization shall test the continuity of operations plan to determine its effectiveness and documents the results. Appropriate officials within the organization must review the documented test results and initiate corrective actions if necessary. The organization shall test the continuity of operations plan for the AMI system at least annually, using organization prescribed tests and exercises to determine the plan's effectiveness and the organization's readiness to execute the plan.

DHS-2.12.5.2 Supplemental Guidance:

The organization must maintain a list of incident response activities and mitigations for the utility and its customers in accordance with the provisions of the organization incident response policy and procedures. Customers and utility operators need to be notified when testing is

scheduled and informed as to how it will be conducted. There are several methods for testing and/or exercising continuity of operations plans to identify potential weaknesses (e.g., full-scale business continuity plan testing, functional/tabletop exercises, etc.). Following the preparation of the various plans, a schedule needs to be developed to review and test each plan and ensure that each still meets the objectives.

DHS-2.12.5.3 Requirement Enhancements:

Utility customers are notified of tests that could affect electrical service.

DHS-2.12.6/ NIST SP 800-53 CP-5 Continuity of Operations Plan Update

DHS-2.12.6.1 Requirement:

The organization shall review the continuity of operations plan for the AMI system at least annually and updates the plan to address system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing.

DHS-2.12.6.2 Supplemental Guidance:

Organizational changes include changes in mission, functions, or business processes supported by the AMI system. The organization must communicate the changes to appropriate organizational elements responsible for related plans.

DHS-2.12.6.3 Requirement Enhancements:

Electrical customers will be notified immediately of changes to the plan that may affect them in the event of a contingency or otherwise.

DHS-2.12.7/ NIST SP 800-53 IR-4 Incident Handling

DHS-2.12.7.1 Requirement:

All components of the AMI system shall support operations in a safe/limited mode which allows for examination of logs and configuration information, resetting of the component, and enabling and disabling of the component.

DHS-2.12.7.2 Supplemental Guidance:

Incident related information must be available, as appropriate, from all components of the AMI system. This information will include activity logs, network logs, and integrity checks.

DHS-2.12.7.3 Requirement Enhancements:

None.

DHS-2.12.8/ NIST SP 800-53 IR-5 Incident Monitoring

DHS-2.12.8.1 Requirement:

The organization must track and document AMI system security incidents on an ongoing basis.

DHS-2.12.8.2 Supplemental Guidance:

None.

DHS-2.12.8.3 Requirement Enhancements:

The communication aggregator shall be able to operate in a safe mode in which communications are relayed from the meter to head end but commands from the head end are not relayed to the individual meters until normal operations are resumed. The component shall also detect and alarm/respond on abnormal command patterns from the head end and abnormal communications patterns from the meters.

DHS-2.12.9/ NIST SP 800-53 IR-6 Incident Reporting

DHS-2.12.9.1 Requirement:

The organization promptly reports security incident information to the appropriate authorities.

DHS-2.12.9.2 Supplemental Guidance:

The organization shall develop guidance to determine what is a reportable incident and the granularity of the information reported (e.g., aggregation of common malicious activity) and who to report to (e.g., management, IT security, process safety, control systems engineering, law enforcement agencies, customers). Reporting documents include the details of the incident, the lessons learned, and the course of action to prevent it from occurring again. The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. In addition to incident information, weaknesses and vulnerabilities in all components of the AMI system need to be reported to appropriate organizational officials in a timely manner to prevent security incidents. Each organization establishes reporting criteria, to include sharing information through appropriate channels. The United States Computer Emergency Readiness Team maintains the Industrial Control System Security Center at http://www.uscert.gov/control_systems.

DHS-2.12.9.3 Requirement Enhancements:

The organization shall employ automated mechanisms to assist in the reporting of security incidents.

DHS-2.12.10/ NIST SP 800-53 IR-7 Incident Response Assistance

DHS-2.12.10.1 Requirement:

The AMI component vendor must support customers or customer facing organizations with advice and assistance in the handling and reporting of security incidents as appropriate..

DHS-2.12.10.2 Supplemental Guidance:

Possible implementation of incident response support could include a help desk and/or an assistance group and access to forensic service when required.

DHS-2.12.10.3 Requirement Enhancements:

None.

DHS-2.12.11/ NIST SP 800-53 PE-6 Incident Response Investigation and Analysis

DHS-2.12.11.1 Requirement:

The organization shall document its policies and procedures to show that investigation and analysis of incidents are included in the planning process. The procedures ensure that all components of the AMI system are capable of providing event data to the proper personnel for analysis and for developing mitigation steps. The organization must ensure that a dedicated group of personnel is assigned to periodically review the data at a minimum monthly, if not daily or more frequently.

DHS-2.12.11.2 Supplemental Guidance:

The organization shall develop an incident response investigation and analysis program, either internally or externally, to investigate incidents. These investigations consider incidents based on the potential outcome as well as the actual outcome, recognizing that the cyber incident may include intentional and unintentional incidents.

DHS-2.12.11.3 Requirement Enhancements:

1. The organization shall develop, test, deploy, and fully document an incident response investigation and analysis process;
2. The organization shall specify roles and responsibilities with respect to local law enforcement and/or other critical stakeholders in an internal and shared incident response investigation and analysis program.

DHS-2.12.12/ NIST SP 800-53 CP-4 Corrective Action

DHS-2.12.12.1 Requirement:

The organization shall include processes and mechanisms in the planning to ensure that corrective actions identified as the result of a cyber security incident are fully implemented.

DHS-2.12.12.2 Supplemental Guidance:

The organization must review investigation results and determine corrective actions needed to ensure that similar events do not happen again. The organization shall encourage and promote cross-industry incident information exchange and cooperation to learn from the experiences of others.

DHS-2.12.12.3 Requirement Enhancements:

None.

DHS-2.12.13/ NIST SP 800-53 CP-6 Alternate Data Storage Sites

DHS-2.12.13.1 Requirement:

The organization shall identify an alternate storage site and initiate necessary agreements to permit the storage of software, data, and configuration information for all components of the AMI system.

DHS-2.12.13.2 Supplemental Guidance:

The frequency of backups of component software and data, and the transfer rate of backup information to the alternate storage site (if so designated) should be consistent with the organization's recovery time objectives and recovery point objectives.

DHS-2.12.13.3 Requirement Enhancements:

1. The organization must identify potential accessibility problems at the alternative storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions;
2. The organization shall identify an alternate storage site that is geographically separated from the primary storage site so it is not susceptible to the same hazards;
3. The organization shall configure the alternate storage site to facilitate timely and effective recovery operations;
4. The organization shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

DHS-2.12.14/ NIST SP 800-53 CP-4 Alternate Command/Control Methods

DHS-2.12.14.1 Requirement:

The meter shall have a manual connect/disconnect switch and communication ports by which a field tool can be used to extract electric use data in the event that the communication network becomes inoperable or unavailable.

DHS-2.12.14.2 Supplemental Guidance:

The intention is that electrical service can be activated and deactivated and usage records from the meter can be obtained by field personal in the event of the communication network becoming unavailable for prolonged periods of time.

DHS-2.12.14.3 Requirement Enhancements:

For the communication aggregator device, there shall be an alternate command path available. The appropriate alternative command/control method should be chosen based on the criticality of the device. This criteria should be capture in organizational policy and reflect system design requirements.

DHS-2.12.15/ NIST SP 800-53 CP-6, CP-7,CP-8 Alternate Control Center

DHS-2.12.15.1 Requirement:

The organization shall identify an alternate control center, necessary telecommunications, and initiate necessary agreements to permit the resumption of the operation of the AMI system within an organization-prescribed time period when the primary control center is unavailable.

DHS-2.12.15.2 Supplemental Guidance:

Equipment, telecommunications, and supplies required to resume operations within the organization-prescribed time period need to be available at the alternative control center or by a contract in place to support delivery to the site.

DHS-2.12.15.3 Requirement Enhancements:

1. The organization shall identify an alternate control center that is geographically separated from the primary control center so it is not susceptible to the same hazards;
2. The organization shall identify potential accessibility problems to the alternate control center in the event of an area-wide disruption or disaster and outline explicit mitigation actions;
3. The organization shall develop alternate control center agreements that contain priority-of-service provisions in accordance with the organization's availability requirements;
4. The organization must fully configure the alternate control center and telecommunications so that they are ready to be used as the operational site supporting a minimum required operational capability.

ASAP-2.12.16/ NIST SP 800-53 CP-9 Business Data Backup

ASAP-2.12.16.1 Requirement:

The organization shall conduct backups of critical business information stored in all the components of the AMI system: this includes electric use data and other billing information, and any other data essential to the utilities other business functions. These backups must occur on a regular schedule as defined by the organization, and the information is stored at an appropriately secured location.

ASAP-2.12.16.2 Supplemental Guidance:

The frequency of backups and the transfer rate of backup information to alternate storage sites (if so designated) needs to be consistent with the organization's recovery time objectives and recovery point objectives.

ASAP-2.12.16.3 Requirement Enhancements:

1. The organization shall test backup information periodically to verify media reliability and information integrity;
2. The organization shall selectively use backup information in the restoration of AMI system functions as part of contingency plan testing;
3. The organization shall protect system backup information from unauthorized modification;
4. The organization shall employ appropriate mechanisms (e.g., digital signatures, cryptographic hash) to protect the integrity of backups.

DHS-2.12.17/ NIST SP 800-53CP-10 Control System Recovery and Reconstitution

DHS-2.12.17.1 Requirement:

All components of the AMI system shall employ mechanisms to enable recovery and/or reconstitution of the AMI system by authorized personnel after a disruption or failure.

DHS-2.12.17.2 Supplemental Guidance:

The essence of this requirement is that backups made of critical operating software, data, configurations, etc. can be used to restore all components of the AMI system to an operational state.

DHS-2.12.17.3 Requirement Enhancements:

None.

DHS-2.12.18/ NIST SP 800-53 CP-8 Fail-Safe Response

DHS-2.12.18.1 Requirement:

All components of the AMI system must fail safe upon the loss of communications with any and all other components of the AMI system.

DHS-2.12.18.2 Supplemental Guidance:

Failures of any and all components of the AMI system shall not jeopardize the Field services devices should have limited capability to make unstable or unsafe settings for the AMI components to which they control.

DHS-2.12.18.3 Requirement Enhancements:

The communication aggregator shall detect and prevent unsafe actions requested by components in the enterprise domain of components in the premise edge and utility edge domains.

DHS-2.14 System and Information Integrity

Maintaining an AMI system, including information integrity, increases assurance that sensitive data have neither been modified nor deleted in an unauthorized or undetected manner. The security controls described under the system and information integrity family provide policy and procedure for identifying, reporting, and correcting AMI system flaws. Controls exist for malicious code detection, spam protection, and intrusion detection tools and techniques. Also provided are controls for receiving security alerts and advisories and the verification of security functions on the AMI system. In addition, there are controls within this family to detect and protect against unauthorized changes to software and data, restrict data input and output, check the accuracy, completeness, and validity of data, and handle error conditions.

DHS-2.14.1/ NIST SP 800-53 SI-1 System and Information Integrity Policy and Procedures

DHS-2.14.1.1 Requirement:

The organization must develop, disseminate, and periodically review/updates:

1. Formal, documented, system and control integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
2. Formal, documented procedures to facilitate the implementation, ongoing maintenance, and support of the AMI system and information integrity policy and associated system and information integrity controls.

DHS-2.14.1.2 Supplemental Guidance:

The organization shall ensure the system and information integrity policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general control security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular AMI component, when required.

DHS-2.14.1.3 Requirement Enhancements:

None.

DHS-2.14.2/ NIST SP 800-53 SI-2 Flaw Remediation

DHS-2.14.2.1 Requirement:

The organization shall identify, report, and remediate AMI system flaws (per organizational, legal, and/or regulatory policies).

DHS-2.14.2.2 Supplemental Guidance:

The organization shall identify AMI systems and system components containing software affected by recently announced flaws (and potential vulnerabilities resulting from those flaws). Proprietary software can be found in either commercial/government off-the-shelf component products or in custom-developed applications. The organization (or the software developer/vendor for software developed and maintained by a vendor/contractor) must promptly evaluate newly released security-relevant patches, service packs, and hot fixes and tests them for effectiveness and potential impacts on the organization's AMI system before installation. Flaws discovered during security assessments, continual monitoring, or under incident response activities also need to be addressed expeditiously. It is generally not recommended to shut down and restart AMI system components when an anomaly is identified.

DHS-2.14.2.3 Requirement Enhancements:

1. The organization shall centrally manage the flaw remediation process and installs updates automatically. Organizations must consider the risk of employing automated flaw remediation processes on an AMI system;
2. The use of automated flaw remediation processes must not degrade the operational performance of the AMI system;
3. The organization must employ automated mechanisms to periodically and upon demand determine the state of AMI system components with regard to flaw remediation.

DHS-2.14.3/ NIST SP 800-53 SI-3 Malicious Code Protection

DHS-2.14.3.1 Requirement:

The AMI system must employ malicious code protection.

DHS-2.14.3.2 Supplemental Guidance:

Malicious code protection mechanisms are central to the AMI system design to control the flow of information within the interconnected elements of the system and to detect and eradicate malicious code.

From a system perspective, malicious code protection mechanisms must be deployed in such a manner as to limit the impact of the attack to a small geographical area prior to detection and eradication. These include critical entry and exit points between Wide Area Networks (WAN), Neighborhood Area Networks (NAN), and in-premise networks.

From a host device perspective, one challenge of an AMI system design is that the field deployed host devices are typically not suitable for traditional third party host based malicious code protection mechanisms. This combined with very little or no physical security warrants that emphasis be placed on the risk associated with these widely dispersed assets. For the AMI meters in particular, the Home Area Network (HAN) interface represents and entry point not only into the device but into the utility's Neighborhood Area Network (NAN) as well. The AMI meter must ensure that no malicious code can pass from the consumer's HAN to the utility's NAN. The AMI meter must also protect the consumer's HAN equipment from any attack which attempts to propagate malicious code utilizing the utility's NAN.

Field tools represent a potentially higher risk due to their portability and likelihood of being connected to numerous networks. If not properly secured and controlled, they can be a mechanism to bypass security controls and allow malicious code to be transported from one security zone to another.

In all cases, care should be taken if automated response mechanisms are deployed so that receipt of false positives from the malicious code protection mechanisms does not adversely affect the availability of the AMI system.

DHS-2.14.3.3 Requirement Enhancements:

1. The use of mechanisms to centrally manage malicious code protection shall not interfere with the reliable operation of the AMI system.
2. All signature files and definitions for malicious code detection mechanisms used within the AMI system shall be updated automatically from a centralized managed trusted source.
3. Centralized configuration management and change control shall be employed for all AMI system assets.
4. Periodic and automatic auditing/verification of configuration (programming parameters, firmware and revision level, etc.) shall be performed for all AMI system assets.
5. All detection of and actions taken within the AMI system to respond to malicious code shall be logged to a centralized repository.
6. Intrusion Detection System (IDS) capability shall be installed within each Neighborhood Area Network (NAN) network segment to monitor incoming and outgoing network traffic, including anti-virus, anti-spyware and signature and anomaly-based traffic monitors.
7. Access Control Lists (ACL) shall be employed at all points which bridge Neighborhood Area Network (NAN) segments to Wide Area Networks (WAN) to limit incoming and outgoing connections to only those necessary to support the AMI system.
8. Dynamic packet filtering shall be employed at all points which bridge Neighborhood Area Network (NAN) segments and Wide Area Networks (WAN).
9. The transfer of executable files through the perimeters of the Neighborhood Area Network (NAN) and the Wide Area Network (WAN) shall be restricted.
10. All components of the AMI system or any device connected to the AMI network shall employ host hardening, including patch application and security-minded configurations of the operating system (OS), browsers, and other network-aware software. All components of the AMI system or any device connected to the AMI network shall employ integrity checking mechanisms for firmware/software.
11. All firmware/software shall be scanned prior to loading on any component of the AMI system or device connected to the AMI network.
12. The authenticity of all firmware/software shall be verified prior to loading on any component of the AMI system or device connected to the AMI network.
13. All AMI components shall be verified to have the proper software revisions and patches prior to being allowed full operation within the AMI network.
14. All centrally located components of the AMI system shall employ anti-virus software.
15. The AMI meter or gateway device shall not allow uploading of any executable code from the consumer's HAN.
16. Field tools shall have additional control applied as follows:

1. Security updates from the manufacturer of the appropriate operating system, and/or application software, shall be kept current (e.g., patched and updated) on all field tools.
2. Field tools shall employ firewall software or hardware to aid in the prevention of malicious code attacks/infections.
3. Field tools shall employ host hardening, including patch application and security-minded configurations of the operating system (OS), browsers, and other network-aware software.
4. Field tools shall utilize anti-virus, anti-spam, and anti-spyware software.
5. Field tools shall scan removable media devices for malicious code before accessing any data on the media.
6. Field tools shall scan email attachments and shared files of unknown integrity for malicious code before they are opened or accessed.
7. The field tool shall utilize a restricted operating system which only allows execution of known and signed code/applications.

DHS-2.14.4/ NIST SP 800-53 SI-4 System Monitoring Tools and Techniques

DHS-2.14.4.1 Requirement:

All components of the AMI system shall log and report all security events and system activities to the AMI management system.

DHS-2.14.4.2 Supplemental Guidance:

Effective monitoring, logging, and alerting of security events requires that all components of the AMI system must be able to generate appropriate logs corresponding to predefined security events.

Including accurate and relevant information in log files is essential. In general, all logs from AMI system components must answer the five basic questions of; Who, What, Where, When, and How. When determining the actions of reading, writing, deleting, and modification of data, it should be possible to determine the process, who owns it, when it was initiated, where the action occurred, and why the process ran. Additionally, all administrative, authentication, authorization, and communication events associated with any AMI system component should be logged and reported.

One challenge when considering an attack on a field-deployed AMI component is that the logging and reporting capability of the component may have be compromised and/or disabled by the attacker. If the monitoring system is only equipped to alert based on logs/reports which are received by the end devices, an attack may go undetected for some period of time if logs representing the security event are not delivered to the central monitoring system.

DHS-2.14.4.3 Requirement Enhancements:

1. The monitoring and logging function must not adversely impact the operational performance of the AMI system or component.
2. Logs generated by AMI system components shall conform to all applicable recommendations outlined in NIST SP800-92, Guide to Computer Security Log Management.
3. The AMI system component shall support standard syslog format (RFC 3164).
4. The AMI system component shall provide an authentication mechanism for the logs.
5. The AMI system component shall provide a mechanism by which missing logs are detected.
6. The AMI system component must be capable of storing a sufficient number of security events in the components buffer to support the system-wide monitoring function.

DHS-2.14.5/ NIST SP 800-53 SI-5 Security Alerts and Advisories

DHS-2.14.5.1 Requirement:

The organization:

1. Receives AMI system security alerts/advisories regularly and in response to system-based occurrences;
2. Issues alerts/advisories to appropriate personnel;
3. Takes appropriate actions in response.

DHS-2.14.5.2 Supplemental Guidance:

The organization documents the types of actions to be taken in response to security alerts and advisories. The organization also shall maintain contact with special interest groups (e.g., information security forums) that:

1. Facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies);
2. Provide access to advice from security professionals;
3. Improve knowledge of security best practices.

DHS-2.14.5.3 Requirement Enhancements:

The organization shall employ automated mechanisms to make security alert and advisory information available throughout the organization as needed.

DHS-2.14.6/ NIST SP 800-53 SI-6 Security Functionality Verification

DHS-2.14.6.1 Requirement:

All components of the AMI system shall employ controls which independently and in concert with the AMI management system verify that that all security functions within the component

are in an online/active state. This shall be done upon component and system startup and restart; upon command by a user with appropriate privilege; periodically; and/or at defined time periods.

DHS-2.14.6.2 Supplemental Guidance:

The AMI management system is ultimately tasked with verification of the proper operation of the security functionality however effectively doing so relies heavily on the capabilities embedded within the various components of the AMI system to support this function.
In addition to processing requests initiated by the AMI management system, the AMI system components shall also be able to perform basic automated self-tests independent of the AMI management system. Because of wide geographic deployment and limited physical security of the field deployed AMI components, verification of the proper operation of the security functionality is essential for these components.

DHS-2.14.6.3 Requirement Enhancements:

1. All AMI system components shall be capable of periodically performing automated self-test of the security functions at predefined intervals.
    1. Any failure of the component self-test shall result in a security event being logged and reported to the appropriate logging system (for further details, see requirement "2.14.4 System Monitoring Tools and Techniques").
    2. Any failure of the component self test shall result in the component transitioning to a safe state including:
        1. Inhibiting all control capabilities of the component.
        2. Inhibiting all communications initiated within the HAN to the NAN.
        3. Inhibiting all relaying/repeating functionality of the component.

DHS-2.14.7/ NIST SP 800-53 SI-7 Software and Information Integrity

DHS-2.14.7.1 Requirement:

The AMI system must monitor and detect unauthorized changes to software and information.

DHS-2.14.7.2 Supplemental Guidance:

The organization shall employ integrity verification techniques on the AMI system to look for evidence of information tampering, errors, and/or omissions. The organization shall employ good software engineering practices with regard to commercial-off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the IT systems, AMI components, and the applications they host.

DHS-2.14.7.3 Requirement Enhancements:

Although automated tools can be risky for use in AMI system, the following can be considered as appropriate for the AMI system:

1. The organization shall reassess the integrity of software and information by performing integrity scans of the AMI system;

2. The organization shall employ automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification;
3. The organization shall employ centrally managed integrity verification tools;
4. The use of integrity verification applications must not adversely impact the operational performance of the AMI system.

DHS-2.14.8/ NIST SP 800-53 SI-8 Spam Protection

DHS-2.14.8.1 Requirement:

The AMI system must implement spam protection.

DHS-2.14.8.2 Supplemental Guidance:

The organization shall employ spam protection mechanisms at critical AMI system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, and/or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet access, or other common means. The organization considers using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another for workstations).
For an AMI system, the organization should minimize any use of and remove if possible any electronic messaging functions and services (e.g., electronic mail, Internet access). Due to differing operational characteristics between AMI systems and general IT systems, AMI systems do not generally employ spam protection mechanisms. Unusual traffic flow, such as during crisis situations, may be misinterpreted and caught as spam, which can cause issues with the system and possible failure of the system.

DHS-2.14.8.3 Requirement Enhancements:

The organization shall centrally manage spam protection mechanisms. The AMI system must automatically update spam protection mechanisms. Organizations consider the risk of employing mechanisms to centrally manage spam protection on an AMI system. The use of mechanisms to centrally managed spam protection must not degrade the operational performance of the AMI system.

DHS-2.14.9/ NIST SP 800-53 SI-9 Information Input Restrictions

DHS-2.14.9.1 Requirement:

The organization shall implement security measures to restrict information input to the AMI system to authorized personnel only.

DHS-2.14.9.2 Supplemental Guidance:

Restrictions on personnel authorized to input information to the AMI system may extend beyond the typical access requirements employed by the system and include limitations based on specific operational or project responsibilities.

DHS-2.14.9.3 Requirement Enhancements:

None.

DHS-2.14.10/ NIST SP 800-53 SI-10 Information Input Accuracy, Completeness, Validity, and Authenticity

DHS-2.14.10.1 Requirement:

All AMI system components must employ controls to check information for accuracy, completeness, validity, and authenticity.

DHS-2.14.10.2 Supplemental Guidance:

The design of the AMI system component must consider all valid inputs during its operation. The AMI system component should filter all inputs and allow only those matching a predefined valid set to be processed by the internal hosted application(s). All other inputs not matching this predefined set should be rejected and logged.

DHS-2.14.10.3 Requirement Enhancements:

None.

DHS-2.14.11/ NIST SP 800-53 SI-11 Error Handling

DHS-2.14.11.1 Requirement:

All AMI system components shall employ controls to identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries.

ASAP/DHS-2.14.11.2 Supplemental Guidance:

The structure and content of error messages displayed by and transmitted from the AMI system components should to be carefully considered by the organization. These error messages must provide timely and useful information without providing potentially harmful information that could be exploited by adversaries. Detailed AMI system component error messages should be revealed only to authorized personnel (e.g., systems administrators, maintenance personnel). The nature of the AMI system architecture makes it susceptible to observing messages displayed on components and monitoring messages transmitted between components. As such, this opens the risk of an attacker determining specific details about the system or its components by observing error messages on device displays or monitoring error messages transmitted from the field deployed AMI components. Such details can provide hackers important clues on potential flaws in the AMI componets.
Risks associated with improper error handling are not limited to those which are transparent to the system operation. AMI system components should not be susceptible to security problems caused by improper error handling, such as:

1. Fail-open security check – The component should assume no access until proven otherwise. All security mechanisms should deny access until specifically granted, not grant access until denied, which is a common reason why fail open errors occur.

2. Impacts to component resources - Errors that can cause the component to crash or consume significant resources, effectively denying or reducing service to legitimate users.

ASAP-2.14.11.3 Requirement Enhancements:

1. Error messages displayed by any field deployed AMI component should not reveal internal details of the component. The component shall provide the user with diagnostic information (e.g., data validation errors), but should NOT provide developer level diagnostic/debug information. Detailed error messages should only be transmitted to the utilities designated logging server.
2. The AMI component must not fail in an open condition (grant access unless specifically denied).

DHS-2.14.12/ NIST SP 800-53 SI-12 Information Output Handling and Retention

DHS-2.14.12.1 Requirement:

The organization shall handle and retain output from the AMI system in accordance with applicable laws, regulations, standards, and organizational policy, as well as operational requirements of the AMI system.

DHS-2.14.12.2 Supplemental Guidance:

None.

DHS-2.14.12.3 Requirement Enhancements:

None.

DHS-2.15 Access Control

The focus of access control is ensuring that resources are only accessed by the appropriate personnel and that personnel are correctly identified. The first step in access control is creating access control lists with access privileges for personnel. The next step is to implement security mechanisms to enforce the access control lists. Mechanisms also need to be put into place to monitor access activities for inappropriate access attempts. The access control lists need to be managed through adding, altering, and removing access rights as necessary.
Identification and authentication is the process of verifying the identity of a user, process, or component, as a prerequisite for granting access to resources in an AMI system. Identification could use a password, a cryptographic token, or a biometric (eg. fingerprint). Authentication is the challenge process to prove (validate) the identification provided. An example is using a fingerprint (identification) to access a computer via a biometric device (authentication). The biometric device authenticates the identity of the fingerprint.

DHS-2.15.1/ NIST SP 800-53 AC-1Access Control Policy and Procedures

DHS-2.15.1.1 Requirement:

The organization shall develop, disseminate, and periodically review/update:

1. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
2. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Access control policies and procedures for highly-critical management tasks must specify strict security controls commensurate with the criticality of the task - including requirements for physical presence at a management console situated in a physically secure location, multiple levels of approval/authorization (by those with appropriate organizational roles), and strong multi-factor authentication.

DHS-2.15.1.2 Supplemental Guidance:

The organization shall ensure that access control policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular AMI component, when required.

It is recommended that the access control policy include the requirement that the **HAN interface shall pass no control signals to the utility.** Only informational signals may be passed on to the utility which shall base no control decisions on HAN-sourced communications without confirmation that the HAN-sourced information is strongly authenticated and consistent with information provided from utility-owned devices within utility-controlled security domains (physical and logical). The utility shall have the ability to set the HAN interface to ignore (i.e., filter) non-authenticated HAN communications or communications from specific HAN-devices when it deems such communications to be a threat to security or safety.

DHS-2.15.1.3 Requirement Enhancements:

None.

DHS-2.15.2/ NIST SP 800-53 IA-2 Identification and Authentication Policy and Procedures

DHS-2.15.2.1 Requirement:

The organization shall develop, disseminate, and periodically review/update:

1. A formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

2. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

All communications between AMI components must be strongly authenticated. Any communications upon which critical management and control decisions are based must be confirmed by multiple independent means (which may include "out-of-band" communications). Any communication to be passed onto the utility by the HAN-interface must be strongly authenticated and non-control in nature.

DHS-2.15.2.2 Supplemental Guidance:

The organization shall ensure the identification and authentication policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular AMI system, when required.

DHS-2.15.2.3 Requirement Enhancements:

None.

DHS-2.15.3/ NIST SP 800-53 AC-2 Account Management

DHS-2.15.3.1 Requirement:

The organization shall manage AMI system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews AMI system accounts, policies, and procedures at least annually, with the frequency depending on criticality.

DHS-2.15.3.2 Supplemental Guidance:

Account management includes the identification of account types (i.e., individual, group, role-based, device-based, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization shall identify authorized users of the AMI system and specifies access rights and privileges; i.e., access control list. The organization shall grant access to the AMI system based on:

1. A valid need-to-know/need-to-share basis that is determined by assigned official duties and that satisfies all personnel security criteria;

2. Intended system use. The organization must require proper identification for requests to establish AMI system accounts and must approve all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. The organization ensures that account managers for the AMI system are notified when users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' AMI system usage or need-to-know/need-to-share changes. In cases where accounts are role-based, i.e., the workstation, hardware, and/or field devices define a user role, access to the AMI system includes physical security policies and procedures based on organization risk assessment. In cases where physical access to the workstation, hardware, and/or field devices predefine privileges, the organization must implement physical security policies, and procedures based on

organization risk assessment. Account management may include additional account types (e.g., role-based, device-based, attribute-based). The organization removes, disables, or otherwise secures default accounts (e.g., maintenance).

3. Default passwords are changed.

DHS-2.15.3.3 Requirement Enhancements:

1. The organization shall employ automated mechanisms to support the management of AMI system accounts. For some AMI components (e.g., field devices), account management may have to be performed manually, where automated mechanisms are not available.
2. The AMI system must automatically terminate temporary and emergency accounts.
3. The AMI system must automatically disable inactive accounts.
4. The organization must employ automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.
5. The organization must ensure default passwords are changed.

DHS-2.15.4/ NIST SP 800-53 IA-4 Identifier Management

DHS-2.15.4.1 Requirement:

The organization shall manage user identifiers by:

1. Uniquely identifying each user;
2. Verifying the identity of each user;
3. Receiving authorization to issue a user identifier from an appropriate organization official;
4. Ensuring that the user identifier is issued to the intended party;
5. Disabling user identifier after a pre-determined time period of inactivity;
6. Archiving user identifiers.

DHS-2.15.4.2 Supplemental Guidance:

All actions within an AMI system should be traceable to an individual user. Guest, Anonymous, and Group accounts should not be used. "root" or similar administrative accounts should not be used for normal operation. For administrative tasks, individual accounts should be used in conjunction with "runas" or "sudo" or similar logging access-control mechanism.
For some AMI components, the capability for immediate operator interaction is critical. Local emergency actions for the AMI system must not be significantly hampered by identification requirements. Access to these systems may be restricted by appropriate physical security mechanisms, and should cause immediate alerting of security personnel.
Failure of identification system should not fail to an open unprotected state. It should fail to a protected, recoverable backup state.

DHS-2.15.4.3 Requirement Enhancements:

None.

DHS-2.15.5/ NIST SP 800-53 IA-5 Authenticator Management

DHS-2.15.5.1 Requirement:

The organization shall manage AMI system authenticators by:

1. Defining initial authenticator content criteria;
2. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;
3. Changing default authenticators upon AMI system installation;
4. Changing/refreshing authenticators periodically.
5. All components must be able to support these organizational activities.
6. All permissions associated with authenticators should be maintained at as low a level as possible so that, in case of compromise, an attacker's access would be limited (see DHS-2.15.9 Least Privilege)

DHS-2.15.5.2 Supplemental Guidance:

System authenticators include, for example, cryptographic tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately.
Passwords must not be embedded into tools, source code, scripts, aliases or shortcuts. Many AMI components and software are shipped with factory default authentication credentials to allow for initial installation and configuration. However, factory default authentication credentials are often well known, easily discoverable, present a great security risk and therefore should be changed.

DHS-2.15.5.3 Requirement Enhancements:

For symmetric/password-based authentication, the AMI system:

1. Protects passwords from unauthorized disclosure and modification when stored or transmitted;
2. Prohibits passwords from being displayed when entered;
3. Enforces password minimum and maximum lifetime restrictions;
4. Prohibits password reuse for a specified number of generations.

For asymmetric/PKI-based authentication, the AMI system:

1. Validates certificates by constructing a certification path to an accepted trust anchor;
2. Establishes control of the corresponding private key;
3. Maps the authenticated identity to the user account.

4. Restricts field tools password and keys life-span in case they are stolen.

DHS-2.15.6 / NIST SP 800-53 PE-2 Supervision and Review

DHS-2.15.6.1 Requirement:

The organization must supervise and review the activities of users with respect to the enforcement and usage of AMI system access control. AMI components must provide auditing capability specified in section DHS-2.16.

DHS-2.15.6.2 Supplemental Guidance:

The organization shall review audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization must investigate any unusual AMI system-related activities and periodically review changes to access authorizations. The organization shall review the activities of users with significant roles and responsibilities for the AMI system more frequently. The extent of the audit record reviews is based on the impact level of the AMI system. For example, for low-impact systems it is not intended that security logs be reviewed frequently for every workstation but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records.
The organization shall have in place policies and procedures that deal specifically with breaches in security, that detail specifically what actions are to occur to secure the breach and investigate any damage. This plan should also include who is responsible for patches and updates and how they are to occur.

DHS-2.15.6.3 Requirement Enhancements:

The organization should employ automated mechanisms to facilitate the review of user activities on the AMI system.

DHS-2.15.7/ NIST SP 800-53 AC-3 Access Enforcement

DHS-2.15.7.1 Requirement:

AMI components must enforce assigned authorizations for controlling access to the system in accordance with applicable policy.
Access to AMI components that perform managed services (e.g Field Tool) must be tightly controlled. Interfaces of particular interest are AMI components that use a PC (or laptop) or mobile devices for interfacing with control functions.

DHS-2.15.7.2 Supplemental Guidance:

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, and cryptography) are employed by organizations to control access to the AMI system. The organization shall consider the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events.
The functionality of field tools and other systems which perform managed services must be limited to the bare minimum to perform the needed task. E-mail and web functions should be removed or limited to access only an approved list. Other applications not required to perform the functions must be removed.

DHS-2.15.7.3 Requirement Enhancements:

1. The AMI system shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. Explicitly authorized personnel include, for example, AMI system operators, security administrators, system and network administrators, and other privileged users who have access to system control, monitoring, or administration functions. Access to privileged functions by privileged users may also be restricted based on components (e.g., remote terminal units and field devices).
2. The AMI system must requires dual authorization, based on approved organization procedures, to privileged functions that have impacts on facility, human, and environmental safety. The utility should develop and implement a procedure that can be executed in times of emergency for access to otherwise restricted passwords and keys
3. Access enforcement mechanisms must not adversely impact the operational performance of the AMI system.
4. The meter IR port must be protected from unauthorized access. Permit only the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks (see section DHS-2.15.9 "Least Privilege").
5. The meter HAN interface must be protected from unauthorized access. Permit only the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks (see section DHS-2.15.9 "Least Privilege").
6. AMI field tool must require access control to utilize the tool. Field service tool should not save or store customer information, passwords, encryption key, or any other information that may compromise the AMI system or network.
7. The HAN interface shall never allow HAN-devices access to utility control functions.

DHS-2.15.8/ NIST SP 800-53 AC-5 Separation of Duties

DHS-2.15.8.1 Requirement:

The organization shall enforce separation of duties through assigned access authorizations.

DHS-2.15.8.2 Supplemental Guidance:

The organization must establish appropriate divisions of responsibility and separate duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. Access control software needs to be on the AMI system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include 1) mission functions and distinct AMI system support functions are divided among different individuals/roles; 2) different individuals perform AMI system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and 3) security personnel who administer access control functions must not administer audit functions.

DHS-2.15.8.3 Requirement Enhancements:

None.

DHS-2.15.9/ NIST SP 800-53 AC-6 Least Privilege

DHS-2.15.9.1 Requirement:

The organization shall enforce the most restrictive set of rights/privileges or accesses to users or workstations (or processes acting on behalf of users) for the performance of specified tasks. The AMI components shall support this organizational requirement.

DHS-2.15.9.2 Supplemental Guidance:

The organization shall employ the concept of least privilege for specific duties and AMI components (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

DHS-2.15.9.3 Requirement Enhancements:

None.

DHS-2.15.10/ NIST SP 800-53 AC-2 User Identification and Authentication

DHS-2.15.10.1 Requirement:

The AMI system shall uniquely identify and authenticate users (or processes acting on behalf of users).

DHS-2.15.10.2 Supplemental Guidance:

Users must be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with security control. Authentication of user identities shall be accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination of these. In addition to identifying and authenticating users at the AMI system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.
Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For some components of AMI system, the capability for immediate operator interaction is critical. The utility must develop and implement a procedure that can be executed in times of emergency for access to otherwise restricted passwords and keys.Access to these systems may be restricted by appropriate physical security mechanisms.

DHS-2.15.10.3 Requirement Enhancements:

Remote user access to AMI system components is only enabled when necessary, approved, and authenticated.

DHS-2.15.11/ NIST SP 800-53 AC-14 Permitted Actions without Identification or Authentication

DHS-2.15.11.1 Requirement:

The organization shall identify, document, and provide security justification for specific user actions that can be performed on the AMI system without identification or authentication.

DHS-2.15.11.2 Supplemental Guidance:

The use of anonymous accounts, public accounts, and guest accounts is prohibited.
The HAN interface should not permit any actions (including communications) without identification or authentication. AMI components that perform management services (e.g. Field Tool) shall not be permitted to perform any actions without identification or authentication.

DHS-2.15.11.3 Requirement Enhancements:

None.

DHS-2.15.12/ NIST SP 800-53 IA-3 Device Identification and Authentication

DHS-2.15.12.1 Requirement:

The AMI system must employ a mechanism to identify and authenticate specific components before establishing a connection. In particular, the HAN interface requires strong authentication, as do components that perform management services (e.g. Field Tool).

DHS-2.15.12.2 Supplemental Guidance:

The strength of the device authentication mechanism is based on the security categorization of the AMI system. Automatic equipment identification may be considered as a means to authenticate connections. Field devices must have the capability to support authentication mechanisms

DHS-2.15.12.3 Requirement Enhancements:

None.

DHS-2.15.13/NIST SP 800-53 IA-6 Authenticator Feedback

DHS-2.15.13.1 Requirement:

The authentication mechanisms in the AMI component/system must obfuscate feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. This applies to authentication by one component to another as well as by individuals.

DHS-2.15.13.2 Supplemental Guidance:

The AMI component/system shall obscure feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password). The feedback from the AMI component/system does not provide information that would allow an unauthorized user to compromise the authentication mechanism.

AMI components involved in authentication must not at any time pass key or token information in an unencrypted format.
Authentication mechanisms should not provide differences which indicate whether the failure is due to invalid userid or password/key.

DHS-2.15.13.3 Requirement Enhancements:

None.

DHS-2.15.14/ NIST SP 800-53 IA-7 Cryptographic Module Authentication

DHS-2.15.14.1 Requirement:

The AMI component/system shall employ authentication methods that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.
Must comply with FIPS 140-2 and NERC security authentication method requirements.

DHS-2.15.14.2 Supplemental Guidance:

None.

DHS-2.15.14.3 Requirement Enhancements:

Failure of cryptographic module authentication must not create a denial of service or adversely impact the operational performance of the AMI system. The system must also not fail to an open unprotected state. Systems critical to overall performance, reliability, safety, and security must provide safe secure failover protection in case of primary authentication failure.

DHS-2.15.15/ NIST SP 800-53 AC-4 Information Flow Enforcement

DHS-2.15.15.1 Requirement:

The AMI component/system shall enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. As stated earlier, the HAN interface shall not pass control signals from the HAN to the utility.

DHS-2.15.15.2 Supplemental Guidance:

Information flow control regulates where information is allowed to travel within an AMI system and between AMI components (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few general examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within AMI system and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards,

encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict AMI system services or provide a packet-filtering capability.

DHS-2.15.15.3 Requirement Enhancements:

1. The information system shall implement information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions. Information flow control enforcement using explicit labels is used, for example, to control the release of certain types of information.
2. The information system shall implement information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.
3. The information system shall implement information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.

DHS-2.15.16 Passwords

DHS-2.15.16.1 Requirement:

The AMI components that support passwords should enforce a level of complexity based on the criticality level of the device/system. Default passwords of applications, operating systems, etc must be changed immediately. Passwords need to be changed regularly and systems should enforce an expiration policy based on the criticality level of the AMI component/system. Passwords must not to be embedded into tools, source code, scripts, aliases or shortcuts.

DHS-2.15.16.2 Supplemental Guidance:

1. Default passwords of applications, operating systems, database management systems, or other programs must be changed immediately after installation.
2. The organization must replace default usernames whenever possible. Passwords need to be allocated, protected, and used based on the criticality level of the systems to be accessed.
3. The organization shall develop policies that stipulate the complexity (min/max length, combination of lower/upper case, numerals, special characters, etc.) level of the password for each criticality level. Short or easily guessed passwords are prohibited. Passwords can be a means of system protection when properly generated and used. Although passwords are not advisable in all AMI system applications, there are some cases where they are of benefit such as for remote access. These passwords are developed to meet defined metrics.
4. Good security practices must be followed in the generation of passwords. Passwords should not easily be associated with the user or the organization and follow appropriate complexity rules. Initial or default passwords must be changed immediately on first log-in. Following generation, passwords shall not be sent across any network unless protected by encryption or salted cryptographic hash specifically designed to prevent replay attacks.

5. Passwords must be transferred to the user via secure media and the recipient must be verified. The logon ID and password must be never combined in the same communication.
6. The authority to keep and change high-level passwords shall be given to a trusted employee who is available during emergencies.
7. A log for master passwords needs to be maintained separately from the AMI system, possibly in a notebook in a vault or safe.
8. Passwords must be changed regularly and expire when the user leaves the organization or after an extended period of inactivity.
9. Users are responsible for their passwords and are instructed not to share them or write them down, and need to be aware of their surroundings when entering passwords. If the operating system supports encryption, stored passwords are encrypted. Passwords must not to be embedded into tools, source code, scripts, aliases or shortcuts.

DHS-2.15.16.3 Requirement Enhancements:

None.

DHS-2.15.17/ NIST SP 800-53 AC-8 System Use Notification

DHS-2.15.17.1 Requirement:

When appropriate, the AMI component or system shall display an approved, system use notification message before granting access.

DHS-2.15.17.2 Supplemental Guidance:

The organization or the AMI system displays an approved, system-use notification message at the time of AMI system logon informing the user:

1. Of the organization's privacy policy before granting system access to potential users and/or workstations;
2. That system usage may be monitored, recorded, and subject to audit;
3. That unauthorized use of the system is prohibited and subject to criminal and civil penalties;
4. That use of the system indicates consent to monitoring and recording.

The system use notification message provides appropriate privacy and security notices (based on organization's associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to AMI system. Privacy and security policies are consistent with applicable federal and state laws, organization directives, policies, regulations, standards, and guidance.

DHS-2.15.17.3 Requirement Enhancements:

None.

DHS-2.15.18/ NIST SP 800-53 AC-10 Concurrent Session Control

DHS-2.15.18.1 Requirement:

The AMI components limit the number of concurrent sessions for any user on the AMI system based on the criticality level of the component.
The organization limits the number of concurrent sessions for any user on the AMI system.

DHS-2.15.18.2 Supplemental Guidance:

None.

DHS-2.15.18.3 Requirement Enhancements:

None.

DHS-2.15.19/ NIST SP 800-53 AC-9 Previous Logon Notification

DHS-2.15.19.1 Requirement:

The AMI components shall notify the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon based on the criticality level of the component.
The AMI system notifies the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

DHS-2.15.19.2 Supplemental Guidance:

None.

DHS-2.12.19.3 Requirement Enhancements:

None.

DHS-2.15.20/ NIST SP 800-53 AC-7 Unsuccessful Login Attempts

DHS-2.15.20.1 Requirement:

The AMI components shall limit the number of consecutive invalid access attempts by a user during a given time period based on the criticality level of the component. The component disables user accounts when the maximum number of unsuccessful attempts is exceeded and logs all unsuccessful login attempts.
The AMI system shall limit the number of consecutive invalid access attempts by a user during a given time period. The AMI system must temporarily disable the user account when the maximum number of unsuccessful attempts is exceeded and logs all unsuccessful login attempts.

DHS-2.15.20.2 Supplemental Guidance:

Because of the potential for denial of service, automatic lockouts initiated by the AMI system are usually temporary and automatically released after a predetermined time period established by the organization. Permanent automatic lockouts initiated by the AMI system must be carefully considered before being used due to safety considerations and the potential for denial of service.

DHS-2.12.20.3 Requirement Enhancements:

The AMI system must automatically lock the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

DHS-2.15.21/ NIST SP 800-53 AC-11 Session Lock

DHS-2.15.21.1 Requirement:

After a predetermined period of inactivity, the AMI system shall prevent further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

DHS-2.15.21.2 Supplemental Guidance:

Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the AMI system.

DHS-2.15.21.3 Requirement Enhancements:

None.

DHS-2.15.22 Remote Session Termination

DHS-2.15.22.1 Requirement:

The AMI system must automatically terminate a remote session after a defined period of inactivity for workstations that are used for AMI system monitoring and maintenance activities based on the risk assessment of the AMI system and the organization's security policy.
On critical high-risk systems it may also be advised that the ports and/or software applications for remote access must be disabled and in some cases physically disconnected

DHS-2.15.22.2 Supplemental Guidance:

A remote session is initiated whenever an organizational AMI system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Some AMI components may not or cannot allow sessions to be terminated.

DHS-2.15.22.3 Requirement Enhancements:

Automatic session termination applies to local and remote sessions. The AMI system terminates a network connection at the end of a session or after a period of inactivity per organization policy and procedures.

DHS-2.15.23/ NIST SP 800-53 AC-17 Remote Access Policy and Procedures

DHS-2.15.23.1 Requirement:

The organization shall develop a formal written policy and appropriate security procedures to address and protect against the risks of remote access to the AMI system, field devices, and communication facilities.

DHS-2.15.23.2 Supplemental Guidance:

In many cases, AMI components are not located within the boundaries of the control room or where there may be a need for access to equipment remote from the user, including

telecommuting or mobile computing. A formal, written procedure is required to address access to systems remote from the user. This policy might include system locking of an interactive session after a specified period of user inactivity, using encrypted password setting on boot up and login for computers not in the control room, encrypted file system, callback and authentication on modems, or the inactivation or disconnection from the network when connections are not required. Appropriate organization officials need to authorize each remote access method for the AMI system and authorize only the necessary users, based on their roles and responsibilities, for access methods identified in the risk assessment.

DHS-2.15.23.3 Requirement Enhancements:

None.

DHS-2.15.24/ NIST SP 800-53 AC-17 Remote Access

DHS-2.15.24.1 Requirement:

Remote access to the AMI components must be enabled only when appropriate and with a level of authentication appropriate to the criticality of the system.

The organization shall authorize, monitor, and manage all methods of remote access to the AMI system.

DHS-2.15.24.2 Supplemental Guidance:

The organization shall document, monitor, and manage all methods of remote access (e.g., dialup, Internet, physical) to the AMI system. Appropriate authentication methods are required to adequately secure remote access.
Remote access is any access to the AMI system or components by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Remote access includes wireless and access via portable and mobile devices. Examples of remote access methods include dial-up, broadband, and wireless. Remote access security requirements are applicable to AMI components other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology).
Remote access to AMI component locations (e.g., control center, field locations) is only enabled when necessary, approved, and authenticated. The organization considers multifactor authentication for remote user access to the AMI system.

DHS-2.15.24.3 Requirement Enhancements:

1. The organization shall employ automated mechanisms to facilitate the monitoring and control of remote access methods.
2. The organization shall use cryptography to protect the confidentiality and integrity of remote access sessions. Any latency induced from the use of encryption, must not degrade the operational performance of the AMI system.

3. The organization shall provide remote accesses through a limited number of managed access control points.
4. The organization shall permit remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the AMI system.

DHS-2.15.25/ NIST SP 800-53 AC-19 Access Control for Portable and Mobile Devices

DHS-2.15.25.1 Requirement:

The organization must:

1. Establish use restrictions and implementation guidance for all portable media and mobile IT devices
2. Document, monitor, log, and limit access of these portable media and mobile devices to AMI system. Appropriate organizational officials authorize the use of portable and mobile devices per organization's established security policy and procedures.

DHS-2.15.25.2 Supplemental Guidance:

Portable media and mobile devices (e.g., notebook computers, workstations, and personal digital assistants) are allowed access to organizational networks and AMI system by meeting organizational security policies and procedures. Security policies and procedures include such activities as scanning the components for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless).
Organizations must disable unused or unnecessary I/O ports.

DHS-2.15.25.3 Requirement Enhancements:

None.

DHS-2.15.26/ NIST SP 800-53 AC-18 Wireless Access Restrictions

DHS-2.15.26.1 Requirement:

The organization must:

1. Establish use restrictions and implementation guidance for wireless technologies
2. Authorize, monitor, and manage wireless access to the AMI system.

DHS-2.15.26.2 Supplemental Guidance:

The organization shall use authentication and cryptography or enhanced defense mechanisms to protect wireless access to the AMI system. Wireless technologies include, but are not limited to, microwave, satellite, packet radio [UHF/VHF], 802.11, 802.15, 802.16, cellular, Zigbee, ISA100, WiHart, and Bluetooth.

DHS-2.15.26.3 Requirement Enhancements:

1. The organization shall use authentication and encryption to protect wireless access to the AMI system. Any latency induced from the use of encryption, must not degrade the operational performance of the AMI system.
2. The organization shall scan for unauthorized wireless access points at a specified frequency and takes appropriate action if such access points are discovered. Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact AMI components. The scan is not limited to only those areas within the facility containing the high-impact AMI components.

DHS-2.15.27/ NIST SP 800-53 AC-20 Personally Owned Information

DHS-2.15.27.1 Personally Owned Information

DHS-2.15.27.1 Requirement:

The organization must restrict the use of personally owned information copied to the AMI system or AMI system user workstation that is used for official organization business. This includes the processing, storage, or transmission of organization business and critical AMI system information. The terms and conditions need to address, at a minimum;

1. The types of applications that can be accessed from personally owned IT, either remotely or from within the AMI system;
2. The maximum security category of information that can processed, stored, and transmitted;
3. How other users of the personally owned AMI components will be prevented from accessing organization information;
4. The use of virtual private networking (VPN) and firewall technologies;
5. The use of and protection against the vulnerabilities of wireless technologies;
6. The maintenance of adequate physical security mechanisms;
7. The use of virus and spyware protection software; and
8. How often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, malware definitions).

DHS-2.15.27.2 Supplemental Guidance:

The organization must establish strict terms and conditions for the use of personally owned information on AMI components.

DHS-2.15.27.3 Requirement Enhancements:

None.

DHS-2.15.28/ NIST SP 800-53 IA-2, IA-8 External Access Protections

DHS-2.15.28.1 Requirement:

The organization shall employ mechanisms in the design and implementation of an AMI system to restrict public access to the AMI system from the organization's enterprise network.

DHS-2.15.28.2 Supplemental Guidance:

Public access is defined as access from the enterprise system. Care should be taken to ensure data shared with the enterprise system are protected for integrity of the information and applications. Public access to the AMI system to satisfy business requirements needs to be limited to read only access through the corporate enterprise systems via a demilitarized zone (DMZ). The organization shall explicitly allow necessary network protocols in the DMZ; blocks or filters unnecessary protocols, configure firewalls to block inbound connections, limits outbound connections to only those specifically required for operations, and eliminates network connections that bypass perimeter protection mechanisms (e.g. firewall, VPN, DMZ).

DHS-2.15.28.3 Requirement Enhancements:

None.

DHS-2.15.29/ NIST SP 800-53 SC-7 Use of External Information Control Systems

DHS-2.15.29.1 Requirement:

The organization shall establish terms and conditions for authorized individuals to:

1. Access the AMI system from an external system;
2. Process, store, and/or transmit organization-controlled information using an external system.

DHS-2.15.29.2 Supplemental Guidance:

External systems are systems or components of systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no control over the application of required security levels or the assessment of security effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications components resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization.

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems).

DHS-2.15.29.3 Requirement Enhancements:

1. The organization shall establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address, as a minimum the types of applications that can be accessed on the organizational information system from the external information system.
2. The organization prohibits authorized individuals from using an external system to access the AMI system or to process, store, or transmit organization-controlled information except in situations where the organization: 1) can verify the employment of required security mechanisms on the external system as specified in the organization's security policy and system security plan; or 2) has approved system connection or processing agreements with the organizational entity hosting the external system.

ASAP-2.15.30 Unauthorized Access Reporting

ASAP-2.15.30.1 Requirement:

The AMI components must record and report unauthorized and unsuccessful attempts to access the system.

ASAP-2.15.30.2 Supplemental Guidance

This can be accomplished with a number of approaches including:

1. System Use Notification (DHS-2.15.17, DHS-2.15.19, DHS-2.15.20)
2. Previous Logon Notification
3. Unsuccessful Login Attempts

ASAP-2.15.30.3 Requirement Enhancements:

None.

ASAP-2.15.31 Unauthorized Access

ASAP-2.15.31.1 Requirement:

The AMI components limit opportunities for unauthorized access.

ASAP-2.15.31.2 Supplemental Guidance

This can be accomplished with a number of approaches including:

1. Concurrent Session Control
2. Session Lock
3. Remote Session Termination

ASAP-2.15.31.3 Requirement Enhancements:

None.

DHS-2.16 Audit and Accountability

Periodic audits and logging of the AMI components and system need to be implemented to validate that the security mechanisms present during system validation testing are still installed and operating correctly. These security audits review and examine a system's records and activities to determine the adequacy of system security controls and to ensure compliance with established security policy and procedures. Audits are also used to detect breaches in security services through examination of system logs. Logging is necessary for anomaly detection as well as forensic analysis.

DHS-2.16.1/ NIST SP 800-53 AU-1 Audit and Accountability Policy and Procedures

DHS-2.16.1.1 Requirement:

The organization shall develop, disseminate, and periodically review/update:

1. A formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
2. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

DHS-2.16.1.2 Supplemental Guidance:

The organization shall ensure the audit and accountability policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general, and for a particular AMI component, when required.

DHS-2.16.1.3 Requirement Enhancements:

None.

DHS-2.16.2/ NIST SP 800-53 AU-2, AU-13 Auditable Events

DHS-2.16.2.1 Requirement:

All AMI components must generate audit records, at a minimum, for the following events whether or not the attempts were successful:

1. Security Events
2. Control Events
3. System/Device Configuration Changes

All AMI systems and components must transmit all audit records and logs to a dedicated log management system. Audit record generation and processing must not degrade the operational performance of the AMI components or system.

DHS-2.16.2.2 Supplemental Guidance:

The organization shall specify which AMI system components carry out auditing activities and ensure that certain events are included or excluded from the set of auditable events based on specified attributes. Auditing activity can affect AMI system performance; therefore, the organization decides, based on a risk assessment, which events require auditing continually and which events require auditing in response to specific situations. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. The targeted security functionality must be able to generate an audit record of:

1. Startup and shutdown of the audit functions;
2. Successful and failed logins
3. Failed authentications of signed or encrypted requests
4. Change in access control or privilege
5. Changes to security settings
6. Creation, deletion, or modifications of users, password, tokens, and security keys
7. Triggering of tamper sensors

The purpose of this requirement is to identify significant and relevant events to the security of the AMI system that needs to be audited. The organization specifies which AMI components carry out auditing activities. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.
The organization must maintain a centralized log management system for long term storage and log correlation. This system must:

1. Provide the capability to compile audit records from multiple components throughout the system into a system wide (logical or physical), time-correlated audit trail.
2. Provide the capability to manage the selection of events to be audited by individual components of the system.
3. Provide the organization the ability to periodically review and update the list of organization-defined auditable events.

DHS-2.16.3/ NIST SP 800-53 AU-3 Content of Audit Records

DHS-2.16.3.1 Requirement:

All AMI components must capture sufficient and detailed information in audit records to establish what events occurred, the sources of the events, and their outcomes.

DHS-2.16.3.2 Supplemental Guidance:

Two types of audits must be tracked:

1. General quality assurance audits of the configuration and operation of the AMI system that verify compliance with organization’s security plan;

2. Audits of operational events encountered by the AMI system when the system operates outsides its normal operating parameters.

General quality assurance audit records contain information of what was audited and the results of the audit; that is, the system is in compliance or not, and if not, what areas are out of compliance. Operational event audits are initiated by the organization's corrective action process when the AMI system operates outsides its normal operating parameters.
Audit record content typically includes:

1. Date and time of the event;
2. The component of the AMI system (e.g., software or hardware component) where the event occurred;
3. Type of event;
4. User/subject/device identity;
5. The operational consequences in the case of an operational event.

All AMI components must provide the capability to include additional, more detailed information in the records for audit events identified by type, location, or subject. All AMI systems and components must provide the capability to centrally manage the content of audit records generated by individual components throughout the AMI system.

DHS-2.16.4/ NIST SP 800-53 AU-4 Audit Storage Capacity

DHS-2.16.4.1 Requirement:

All AMI components must provide sufficient audit record storage capacity and capabilities to configure auditing verbosity to reduce the likelihood of such capacity being exceeded.
Under normal usage conditions, components and systems must store events locally for the following minumal timeframes:

1. Embedded Devices: 1 week
2. Traditional IT or SCADA Servers: 1 month
3. Central Log Management Systems: 1 year

DHS-2.16.4.2 Supplemental Guidance:

None.

DHS-2.16.4.3 Requirement Enhancements:

None.

DHS-2.16.5/ NIST SP 800-53 AU-5 Response to Audit Processing Failures

DHS-2.16.5.1 Requirement:

The log management system must alert appropriate organization personnel in case of audit failure events, such as:

1. Allocated audit record storage volume reaches organization-defined percentage of maximum audit record storage capacity.
2. Log management systems have not received log messages from a particular AMI component for a configurable period of time.
3. Inability to read from or write to the event storage volume.

DHS-2.16.5.2 Supplemental Guidance:

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

DHS-2.16.5.3 Requirement Enhancements:

1. The AMI system provides a warning when allocated audit record storage volume reachesorganization-defined percentage of maximum audit record storage capacity;
2. The AMI system provides a real-time alert when the following organization defined auditfailure events occur.

DHS-2.16.6/ NIST SP 800-53 AU-6 Audit Monitoring, Analysis, and Reporting

DHS-2.16.6.1 Requirement:

The organization regularly monitors, reviews, and analyzes audit records on all dedicated log management systems. The log management systems must provide automated mechanisms for detecting inappropriate, unusual, or suspicious activity or security violations, and automatically alerts approprate personnel in a timely manner.

DHS-2.16.6.2 Supplemental Guidance:

Organizations increase the level of audit monitoring and analysis activity within the log management systems and audit record sources whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. AMI components and system must support this ability. Audit records need to be monitored regularly for inappropriate activities in accordance with organizational procedures. Audit reports need to be provided to those responsible for cyber security.

DHS-2.16.6.3 Requirement Enhancements:

None.

DHS-2.16.7 / NIST SP 800-53 AU-7 Audit Reduction and Report Generation

DHS-2.16.7.1 Requirement:

The dedicated log management systems must provide an audit reduction and report generation capability.

DHS-2.16.7.2 Supplemental Guidance:

Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.

DHS-2.16.7.3 Requirement Enhancements:

None.

DHS-2.16.8/ NIST SP 800-53 AU-8 Time Stamps

DHS-2.16.8.1 Requirement:

All AMI system and components must provide time stamps for use in audit record generation.

DHS-2.16.8.2 Supplemental Guidance:

Time stamps of audit records are generated using internal system clocks synchronized across all of the AMI components.

DHS-2.16.8.3 Requirement Enhancements:

None.

DHS-2.16.9/ NIST SP 800-53 AU-9 Protection of Audit Information

DHS-2.16.9.1 Requirement:

All AMI components and system must protect audit information and audit tools from unauthorized access, modification, and deletion.

DHS-2.16.9.2 Supplemental Guidance:

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit AMI system activity. The logs are important for error correction, security breach recovery, investigations, and related efforts.

DHS-2.16.9.3 Requirement Enhancements:

None.

DHS-2.16.10/ NIST SP 800-53 AU-11 Audit Record Retention

DHS-2.16.10.1 Requirement:

The organization shall retain audit logs for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

DHS-2.16.10.2 Supplemental Guidance:

Logs containing computer or communication system security relevant events need to be retained for a period as defined in the information retention policy. The organization retains audit records until it is determined that they are no longer needed for administrative, legal, regulatory, or other operational purposes.

DHS-2.16.10.3 Requirement Enhancements:

None.

DHS-2.16.11/ NIST SP 800-53 AU-1 Conduct and Frequency of Audits

DHS-2.16.11.1 Requirement:

The organization shall conduct audits at planned intervals to determine whether the security objectives, measures, processes, and procedures:

1. Conform to the requirements and relevant legislation or regulations;
2. Conform to the identified information security requirements;
3. Are effectively implemented and maintained;
4. Perform as expected;
5. Identify inappropriate activities.

DHS-2.16.11.2 Supplemental Guidance:

Audits can be either in the form of internal self-assessment or independent, third-party audits. Internal audits, sometimes called first-party audits, are conducted by, or on behalf of, the organization itself for internal purposes. An internal audit needs to be conducted to ensure that documentation is current with any changes to the AMI system. Independent audits review and examine records and activities to assess the adequacy of AMI system security measures, ensure compliance with established policies and operational procedures, and recommend necessary changes in security requirements, policies, or procedures. For independent audits, the auditor(s) need to be accompanied by an appropriate knowledgeable AMI system staff person(s) to answer any questions about the particular system under review.

DHS-2.16.11.3 Requirement Enhancements:

None.

DHS-2.16.12/ NIST SP 800-53 CA-2 Auditor Qualification

DHS-2.16.12.1 Requirement:

The organization's audit program shall specify auditor qualifications in accordance with the organization's documented training program.

DHS-2.16.12.2 Supplemental Guidance:

The selection of auditors and conduct of audits must ensure the objectivity and impartiality of the audit process. Security auditors need to:

1. Understand the AMI system to be audited and be personally familiar with the systems and operating practices;
2. Understand the risk involved with the audit and the consequences associated with unintentional stimulus or denial of service to the AMI system;

3. Fully understand the corporate cyber and AMI system security policies and procedures and the specific health, safety, and environmental risks associated with a particular facility and/or process.

DHS-2.16.12.3 Requirement Enhancements:

The organization assigns auditor and system administration functions to separate personnel.

ASAP-2.16.13/ NIST SP 800-53 AU-7 Audit Tools

ASAP-2.16.13.1 Requirement:

The organization under the audit program shall specify strict rules and careful use of audit tools when auditing AMI system functions.

ASAP-2.16.13.2 Supplemental Guidance:

As a general practice, system audits determine compliance of the AMI system to the organization's security plan. For new AMI components, system auditing utilities need to be incorporated into the design. Appropriate security audit practices for legacy systems require appropriate precautions be taken before assessing the AMI system. For AMI system audits to determine inappropriate activity, information custodians ensure that AMI system monitoring tools are installed to log system activity and security events. Auditing and log management tools need to be used cautiously in maintaining and proving the integrity of the AMI system from installation through the system life cycle. Access to AMI system audit tools need to be protected to prevent any possible misuse or compromise.

ASAP-2.16.13.3 Requirement Enhancements:

The AMI system and its components shall continue to operate during and after a cyber security scan.

DHS-2.16.14/ NIST SP 800-53 CA-1 Security Policy Compliance

DHS-2.16.14.1 Requirement:

The organization shall demonstrate compliance to the organization's security policy through audits in accordance with the organization's audit program.

DHS-2.16.14.2 Supplemental Guidance:

Periodic audits of the AMI system must be implemented to demonstrate compliance to the organization's security policy. These audits:

1. Assess whether the defined cyber security policies and procedures, including those to identify security incidents, are being implemented and followed;
2. Document and ensure compliance to organization policies and procedures;
3. Identify security concerns, validate the system is free from security compromises, and provide information on the nature and extent of compromises should they occur;
4. Validate change management procedures and ensure that they produce an audit trail of reviews and approvals of all changes;

5. Verify that security mechanisms and management practices present during system validation are still in place and functioning;

Ensure reliability and availability of the system to support safe operation;
Continuously improve performance.

DHS-2.16.14.3 Requirement Enhancements:

None.

APPENDIX A

KEY POWER SYSTEM USE CASES FOR SECURITY REQUIREMENTS

The focus of this document, "***Key Power System Use Cases and Security Requirements***" is to identify the key Use Cases that are "architecturally significant" for security requirements, and to assess the types of security requirements (Integrity, Availability, and Confidentiality) that are pertinent to those Use Cases. In addition, the focus is more on operational functions as opposed to "back office" or corporate functions, since it is the automation and control aspects of power system management that are relatively unique and certainly are the ones that stretch the security risk assessment, the security controls, and the security management.

There are many interfaces and "environments" with constraints and sensitive aspects that make up the information infrastructure which is monitoring and controlling the power system infrastructure. This document does not directly capture those distinctions, but leaves it up to the implementers of security measures to take those into account. The full set of Use Cases, taken from many sources, include the following:

- **IntelliGrid Use Cases** (IntelliGrid web site: http://intelligrid.ipower.com/IntelliGrid_Architecture/Use_Cases/Fun_Use_Cases.htm). There are over 700 of these Use Cases, but really only the power system operations Use Cases and Demand Response/AMI ones are of particular interest for security. The EPRI IntelliGrid project developed the complete list of Use Cases.

- **AMI Business Functions** which were extracted from Appendix B of the AMI-SEC Security Requirements Specification (T&D DEWG and now also posted on CSCTG TWiki).
- **Benefits and Challenges of Distribution Automation** – Use Case Scenarios (White Paper for Distribution on T&D DEWG, extracted from CEC document which has 82 Use Cases, and now also posted on CSCTG TWiki).

- **EPRI Use Case Repository** (http://www.smartgrid.epri.com/usecaserepository.html) which is a compilation of IntelliGrid and SCE Use Cases, plus others.

- **SCE Use Cases** (http://www.sce.com/usecases) These were developed by Southern California Edison (SCE) with the assistance of EnerNex.

There is a certain amount of overlap in these sources, particularly in the new area of AMI, but no-one would argue that even the combined set (reaching over 1000 Use Cases) really covers all requirements - they just act as indications of the areas of interactions. For instance, for just one item, the connect/disconnect of meters, 6 utilities developed over 20 Use Case variations in order to meet their diverse needs, often due to different State regulatory requirements.

The Use Cases were not generally copied verbatim from their sources, but sometimes edited to focus on the security issues.

IAC (Integrity, Availability, Confidentiality) Security Requirements

The following Use Cases 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 with respect to Integrity, Availability, and Confidentiality (IAC).

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

- Data has not been modified without authorization
- Source of data is authenticated
- Timestamp associated with the data is known and authenticated
- Quality of data is known and authenticated

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

- 4 ms for protective relaying
- Sub-seconds for transmission wide-area situational awareness monitoring
- Seconds for substation and feeder SCADA data
- Minutes for monitoring non-critical 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

Confidentiality is generally the least critical for actual power system operations, although this is changing for some parts of the power system, as customer information is 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.

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 24x7 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 may be achievable, but is undesirable because of the loss of functionality that would be necessary to achieve this near perfect state.
- Balance is also needed between risk and the cost of implementing the security measures.

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 IAC) 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 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 by-passing 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 re-assessment of security risks

Category: AMI		
Scenario: Meter Reading Services		
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 which are interfaced to the AMI systems.		
Scenario Description Meter reading services provide the basic meter reading capabilities for generating customer bills. Different types of metering services are usually provided, depending upon the type of customer (residential, smaller commercial, larger commercial, smaller industrial, larger industrial) and upon the applicable customer tariff. Periodic Meter Reading On-Demand Meter Reading Net Metering for DER and PEV Feed-In Tariff Metering for DER and PEV Bill - Paycheck Matching		
Smart Grid Characteristics Enables active participation by consumers Enables new products, services and markets Optimizes asset utilization and operate efficiently	Cyber Security Objectives/Requirements 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	Potential Stakeholder Issues Customer data privacy and security Retail Electric Supplier access Customer data access
Category: AMI		
Scenario: Pre-Paid Metering		

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 which are interfaced to the AMI systems.

Scenario Description

Customers who either want a lower rate or have a history of slow payment can benefit from prepayment of power. Smart metering makes it easier to deploy new types of prepayment to customers and provide them with better visibility on the remaining hours of power, as well as extending time of use rates to prepayment customers.
AMI systems can also trigger notifications when the pre-payment limits are close to being reached and/or have been exceeded.
Limited Energy Usage
Limited Demand

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	Integrity of meter data is critical, to avoid unwarranted disconnections due to perceived lack of pre-payment. Security compromises could have a large impact on the customer and could cause legal repercussions Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database Availability to turn meter back on after payment is important, but could be handled by a truck roll if necessary	Customer data privacy and security Retail Electric Supplier access Customer data access

Category: AMI

Scenario: Revenue Protection

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 which are interfaced to the AMI systems.

Scenario Description

Non-technical losses (or theft of power by another name) has long been an on-going battle between utilities and certain customers. In a traditional meter, when the meter reader arrives, they can look for visual signs of tampering, such as broken seals and meters plugged in upside down. When AMI systems are used, tampering that is not visually obvious may be detected during the analysis of the data, such as anomalous low usage. AMI will help with more timely and sensitive detection of power theft.
Tamper Detection
Anomalous Readings
Meter Status
Suspicious Meter

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Optimizes asset utilization and operate efficiently Operates resiliently against attack and natural disasters	Integrity of meter data is important, but if tampering is not detected or if unwarranted indications of tampering are detected, there is no power system impact, just revenue impact Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database Availability to turn meter back on after payment is important	Customer data privacy and security Retail Electric Supplier access Customer data access

Category: AMI

Scenario: Remote Connect/Disconnect of 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 which are interfaced to the AMI systems.

Scenario Description

Traditionally, utilities send a metering service person to connect or disconnect the meter. With an AMI system, the connect/disconnect can be performed remotely by switching the remote connect/disconnect (RCD) switch for the following reasons.
Remote Connect for Move-In
Remote Connect for Reinstatement on Payment
Remote Disconnect for Move-Out
Remote Disconnect for Non-Payment
Remote Disconnect for Emergency Load Control
Unsolicited Connect / Disconnect Event

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Optimizes asset utilization and operate efficiently Operates resiliently against attack and natural disasters	Integrity of control commands to the RCD switch is critical to avoid unwarranted disconnections or dangerous/unsafe connections. The impact of invalid switching could be very large if many meters are involved Availability to turn meter back on when needed is important Confidentiality requirements of the RCD command is generally not very important, except related to non-payment	Customer data privacy and security Retail Electric Supplier access Customer data access Customer Safety

Category: AMI

Scenario: Outage Detection and Restoration

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 which are interfaced to the AMI systems.

Scenario Description

The AMI system detects customer outages and reports it in near-real-time to the distribution utility. The utility uses the customer information from the Customer Information System, the Trouble Call System, Geographical Information System, and the Outage Management System to identify the probable location of the fault. The process includes the following steps:
Smart meters report one or more power losses (e.g. “last gasp”)
Outage management system collects meter outage reports and customer trouble calls
Outage management system determines location of outage and generates outage trouble tickets
Work management system schedules work crews to resolve outage
Interactive utility-customer systems inform the customers about the progress of events
Trouble tickets are used for statistical analysis of outages

Smart Grid Characteristics	Cyber Security Objectives/Requirements	Potential Stakeholder Issues
Optimizes asset utilization and operate efficiently Operates resiliently against attack and natural disasters	Integrity is important to ensure outages are reported correctly Availability is important to ensure outages are reported in a timely manner (a few seconds) Confidentiality is not very important	Customer data privacy and security Retail Electric Supplier access Customer data access Customer Safety

Category: AMI

Scenario: Meter Maintenance

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 which are interfaced to the AMI systems.

Scenario Description

Meter maintenance is needed to locate and repair/replace meters that have problems, or to update firmware and parameters if updates are required. For those with batteries, such as gas and water meters, battery management will also be needed.
Connectivity validation
Geo-location of meter
Smart meter battery management

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 of meter maintenance repairs and updates are essential to prevent malicious intrusions Availability is important, but only in terms of hours or maybe days Confidentiality is not important unless some maintenance activity involves personal information	Customer data privacy and security Retail Electric Supplier access Customer data access

Category: AMI

Scenario: Meter Detects Removal

Category Description

The AMI category covers the fundamental functions of an advanced metering system. These functions include: meter reading, use of an integrated service switch, theft detection and improved outage detection and restoration. The high level technical requirements for these functions are well understood by the industry, but the specific benefit varies from utility to utility.

Advanced functions that are often associated with AMI are demand response program support and communications to in-home devices. These functions are not exclusive to AMI and will be discussed in separate category areas.

Scenario Description

This scenario discusses the AMI meter's functionality to detect and report unauthorized removal and similar physical tampering. AMI meters require additional capability over traditional meters to prevent theft and tampering due to the elimination of regular visual inspection provided by meter reading.

Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues

Optimizes asset utilization and operate efficiently Operates resiliently against attack and natural disasters	To reduce energy theft To prevent theft/compromise of passwords and key material To prevent installation of malware	Customer data privacy and security Retail Electric Supplier access Customer data access
Category: AMI		
Scenario: Utility Detects Probable Meter Bypass		
Category Description The AMI category covers the fundamental functions of an advanced metering system. These functions include: meter reading, use of an integrated service switch, theft detection and improved outage detection and restoration. The high level technical requirements for these functions are well understood by the industry, but the specific benefit varies from utility to utility. Advanced functions that are often associated with AMI are demand response program support and communications to in-home devices. These functions are not exclusive to AMI and will be discussed in separate category areas.		
Scenario Description AMI meters eliminate the possibility of some forms of theft (i.e. meter reversal). Other types of theft will be more difficult to detect due to the elimination of regular physical inspection provided by meter reading. This scenario discusses the analysis of meter data to discover potential theft occurrences.		
Smart Grid Characteristics	Objectives/Requirements	Potential Stakeholder Issues
Optimizes asset utilization and operate efficiently Operates resiliently against attack and natural disasters	To reduce theft To protect integrity of reporting To maintain availability for reporting and billing	Customer data privacy and security Retail Electric Supplier access Customer data access Customer Safety

Category: Demand Response
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. 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

Use of Real Time Pricing 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 real time pricing 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 24x7 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 non-repudiation, of pricing information is critical, since there could be large financial and possibly legal implications Availability, including non-repudiation, 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

Category: Demand Response

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 time-of-use pricing may be manually handled once the customer is aware of the time periods and the pricing.

Scenario Description

Time of use pricing 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 Real Time Pricing is more flexible than Time of Use, 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

Category: Demand Response

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 Time of Use (TOU) tariffs are employed.
Today larger 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 plug-in electric vehicles (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

Category: Demand Response

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

Category: Demand Response

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 Time of Use 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

Category: Demand Response

Scenario: Mobile Plug-In Electric Vehicle (PEV) 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

Category: Customer Interfaces

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	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

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	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		
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	**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
Category: Customer Interfaces		
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	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

Category: Customer Interfaces

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	Objectives/Requirements	Potential Stakeholder Issues
Enables active participation by consumers Accommodates all generation and	To validate that the notification is legitimate Customer's information is kept	Customer device standards Customer data privacy and security

storage options Enables new products, services and markets	private	

Category: Customer Interfaces

Scenario: Customer Access to Energy-Related Information

Category Description

Customers with Home Area Networks and/or Building Energy Management 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 Home Area Networks and/or Building Energy Management 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, pre-paying 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

Category: Electricity Market

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 a separate section, is a part of the electricity market.

Scenario Description

The bulk power market varies from region to region, and is conducted primarily through Regional Transmission Operators (RTO) and Independent System Operators (ISO). 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	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

Category: Electricity Market

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 a separate section, 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 section.)

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

Category: Electricity Market

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 a separate section, 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	Integrity for pricing and generation information is critical	Customer data privacy and security

participation by consumers Accommodates all generation and storage options Enables new products, services and markets	Availability for pricing and generation information is important within minutes to hours Confidentiality for pricing and generation information is critical	Retail Electric Supplier access Customer data access

Category: Distribution Automation		
Scenario: Distribution Automation (DA) within Substations		
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 (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 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 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	Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers	Customer safety Device standards Cyber Security

a digital economy Optimizes asset utilization and operating efficiency Anticipates and responds to system disturbances in a self-correcting manner	reliably and efficiently Availability for control is critical, while monitoring individual equipment is less critical Confidentiality is not very important	
Category: Distribution Automation		
Scenario: Distribution Automation (DA) Using Local Automation		
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 (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 Local automation of feeder equipment consists of power equipment that is managed locally by computer-based controllers which 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 Provides power quality Optimizes asset	**Cyber Security Objectives/Requirements** Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers	**Potential Stakeholder Issues** Customer safety Customer device standards Demand response acceptance

utilization Anticipates and responds to system disturbances	reliably and efficiently Availability for control is critical, while monitoring individual equipment is less critical Confidentiality is not very important	by customers
Category: Distribution Automation		
Scenario: Distribution Automation (DA) Monitoring and Controlling Feeder Equipment		
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 (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 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 Automation of Emergency Response Dynamic Rating of Feeders		
Smart Grid Characteristics Provides power quality	**Cyber Security Objectives/Requirements** Integrity of distribution control commands is critical for distribution operations, avoiding	**Potential Stakeholder Issues** Customer safety Customer device standards

Optimizes asset utilization Anticipates and responds to system disturbances	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	Demand response acceptance by customers
Category: Distribution Automation		
Scenario: Fault Detection, Isolation, and Restoration		
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 (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 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 be come increasingly critical. The automated fault location, isolation, and service restoration 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

Category: Distribution Automation

Scenario: Load 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 (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

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 pre-cooling, heat storage management).
Direct load control and load shedding
Demand side management
Load shift scheduling
Curtailment planning
Selective load management through Home Area Networks

Smart Grid Characteristics	**Cyber Security Objectives/Requirements**	**Potential Stakeholder Issues**
Provides power quality	Integrity of load control commands is critical to avoid unwarranted outages	Customer safety Customer device standards

Optimizes asset utilization Anticipates and responds to system disturbances	Availability for load control is important – in aggregate (e.g. > 300 MW), it can be critical Confidentiality is not very important	Demand response acceptance by customers
Category: Distribution Automation		
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 (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

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 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 Distribution System Power Flow (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	Integrity is critical to operate the distribution power system reliably, efficiently, and safely Availability is critical to operate the	Customer safety Customer device standards Demand response acceptance

utilization Anticipates and responds to system disturbances	distribution power system reliably, efficiently, and safely Confidentiality is not important	by customers

Category: Distribution Automation

Scenario: Distributed Energy Resource (DER) 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 (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
Plug-in Hybrid Vehicle (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	Integrity is critical for any management/ control of generation and storage Availability requirements may vary depending on the size (individual or	Customer safety Customer device standards Demand response acceptance by customers

responds to system disturbances	aggregate) of the DER plant Confidentiality may involve some privacy issues with customer-owned DER	
Category: Distribution Automation		
Scenario: Distributed Energy Resource (DER) 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 (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 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-Tem Load Forecasts by Area Optimal Placements of Switches, Capacitors, Regulators, and DER Distribution System Upgrades and Extensions Distribution Financial Planners		
Smart Grid Characteristics Provides power quality Optimizes asset	**Cyber Security Objectives/Requirements** Integrity not critical due to multiple sources of data Availability is not important	**Potential Stakeholder Issues** Cyber security

utilization Anticipates and responds to system disturbances	Confidentiality is not important	

Category: Plug In Hybrid Electric Vehicles (PHEV)		
Scenario: Customer Connects Plug In Hybrid Electric Vehicle 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 (PHEV)		
Scenario: Customer Connects Plug In Hybrid Electric Vehicle 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

Category: Plug In Hybrid Electric Vehicles (PHEV)

Scenario: Plug In Hybrid Electric Vehicle 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

Category: Plug In Hybrid Electric Vehicles (PHEV)

Scenario: Plug In Hybrid Electric Vehicle 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	Improved system stability and	Vehicle standards

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	availability Pricing signals are accurate and trustworthy Customer information is kept private	Customer safety Customer device standards Demand response acceptance by customers

Category: Distributed Resources

Scenario: Customer Provides Distributed Resource

Category Description

Traditionally, distributed resources have served as a primary or emergency back-up 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	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 Net metering is accurate and timely	Safety Customer data privacy and security

Category: Distributed Resources

Scenario: Utility Controls Customer's Distributed Resource

Category Description

Traditionally, distributed resources have served as a primary or emergency back-up 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	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 information is kept private DR messages are received timely	Safety Customer data privacy and security

Category: Transmission Operations

Scenario: Real-time Normal Transmission Operations Using 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 Energy Management System (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 Energy Management System. 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	**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. one second) Confidentiality is not important	Customer safety Customer device standards Demand response acceptance by customers

Category: Transmission Operations

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 Energy Management System (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

Energy Management Systems (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

Category: Transmission Operations

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 Energy Management System (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, 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. one second) Confidentiality is not important	Customer safety Customer device standards Demand response acceptance by customers

Category: Transmission Operations

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 Energy Management System (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 Synchro-Phasor 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 are 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. one second) Confidentiality is not important	Cyber Security Customer data privacy and security

Category: RTO/ISO Operations		
Scenario: RTO/ISO Management of Central and DER Generators and Storage		
Category Description		
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 non-market 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	**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 operator commands (e.g. one second) Confidentiality is not important	Cyber Security Customer data privacy and security

Category: Asset Management

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

Category: Asset Management

Scenario: Utility makes decisions on asset replacement based on a range of inputs including comprehensive off line and on line 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, computer-based maintenance management systems (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 on-line condition monitoring devices for the range of assets monitored, off line test results, mobile work force technologies, the communications equipment used to collect the on-line 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

Category: Asset Management

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, computer-based maintenance management systems (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 information 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

Category: Asset Management

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, computer-based maintenance management systems (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 on-line condition monitoring devices for the range of assets monitored, off line test results, mobile work force technologies, the communications equipment used to collect the on-line 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

APPENDIX B

CROSSWALK OF CYBER SECURITY DOCUMENTS

The following is a mapping between the security requirements contained in several relevant documents that include security requirements that may be applicable to the Smart Grid.

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
2.1.1	Security Policies and Procedures	62351-1 (1.2)	5.7.1	4.3.2.6	CIP 003-2 (R1,R1.1,R1.3, R5, R5.3)	4.2	AC-1	FBS-21
2.2.1	Management Policies and Procedures	62351-1 (5.4,5.7)	5.7.1, 5.7.2	4.3.4.4	CIP 003-2 (R1, R2, R3, R4,R5, R6)	ES-3	PM-1	FBS-22 AOR-106
2.2.2	Management Accountability		5.7.2	4.3.2.6	CIP 003-2 (R2, R3)	4.2.1	PM-1	FBS-23 AOR-107 AAY-9
2.2.3	Baseline Practices		5.7.2, 5.5.3.1	A.3.2.5.4.1				FBS-24 AOR-108 AAY-10 AAY-19
2.2.4	Coordination of Threat Mitigation			A.3.2.3.4.2	CIP 008-2 (R1.3)			FBS-25 AOR-109
2.2.5	Security Policies for Third Parties			A.3.3.3.2	CIP 004-2 (R2.1, R3.3, R4.1)	6.1.3		FBS-26 AOR-110
2.2.6	Termination of Third Party Access			A.3.3.5.4.1	CIP 004-2 (R4)			FBS-27 AOR-111
2.3.1	Personnel Security Policies and Procedures			4.3.3.2	CIP 004-2 (R3)	6.2.1	PS-1	AOR-37 AOR-45 AAY-14
2.3.2	Position Categorization			4.3.3.2.3	CIP 004-2 (R3)		PS-2	AOR-38 AOR-46
2.3.3	Personnel Screening			A.3.3.2.2	CIP 004-2 (R3)	6.2.1	PS-3	AOR-39 AOR-47
2.3.4	Personnel Termination			A.3.3.5.3	CIP 004-2 (R4.2)		PS-4	AOR-40

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
					CIP 007-2 (R5.2.3)			AOR-48
2.3.5	Personnel Transfer			4.3.3.2.2	CIP 004-2 (R4.1, R4.2)		PS-5	AOR-41 AOR-49 AAC-12
2.3.6	Access Agreements			A.3.3.2.2			PS-6	AOR-42 AOR-50
2.3.7	Third Party Security Agreements			A.3.2.3.4.2	CIP 004-2 (R3.3)		PS-7	AOR-43 AOR-51
2.3.8	Personnel Accountability	62351-1 (5.4)		A.3.2.3			PS-8	AOR-44 AOR-52 AAY-15
2.3.9	Personnel Roles	-		4.3.2.6				AOR-53
2.4.1	Physical and Environmental Security Policies and Procedures	62351-1 (5.4)		4.3.2.1	CIP 006-2 (R1, R2)	6.2.2	PE-1	AOR-12 AOR-54 AAY-16
2.4.2	Physical Access Authorizations			4.3.3.6.1	CIP 004-2 (R4)		PE-2	FAZ-5 AOR-13 AOR-55
2.4.3	Physical Access Control			A.3.3.3.3.1	CIP 006-2 (R2)	6.2.2	PE-3 PE-4 PE-5	FAZ-6 FAZ-7 FAZ-8 AOR-14 AOR-15 AOR-56
2.4.4	Monitoring Physical Access	62351-1 (5.7)		A.3.3.3.3.1	CIP 006-2 (R5)	6.2.2	PE-6	AOR-57
2.4.5	Visitor Control				CIP 006-2 (R1.4)		PE-7	AOR-18 AOR-58
2.4.6	Visitor Records				CIP 006-2 (R1.4, R6)		PE-8	AOR-19 AOR-59
2.4.7	Physical Access Log Retention				CIP 006-2 (R7)		PE-8	AOR-60
2.4.8	Emergency Shutoff					6.2.2	PE-10	AOR-61

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
2.4.9	Emergency Power			A.3.2.5.4.1			PE-11	AOR-22 AOR-62
2.4.10	Emergency Lighting			A.3.2.5.4.1			PE-12	AOR-23 AOR-63
2.4.11	Fire Protection			A.3.3.3.2			PE-13	FAS-5 FAS-6 AOR-24 AOR-64
2.4.12	Temperature and Humidity Controls			A.3.3.3.2			PE-14	AOR-25 AOR-65
2.4.13	Water Damage Protection			A.3.3.3.2			PE-15	AOR-26 AOR-66
2.4.14	Delivery and Removal			A.4.2.2			PE-16	AOR-27 AOR-67
2.4.15	Alternate Work Site					6.2.2.1	PE-17	AOR-28 AOR-68
2.4.16	Portable Media							AOR-69
2.4.17	Personnel and Asset Tracking			A.3.3.3.2				AOR-70
2.4.18	Location of Control System Assets			4.3.3.3.4			PE-18	AOR-21 AOR-29 AOR-71
2.4.19	Information Leakage						PE-19	AOR-30 AOR-72
2.4.20	Power Equipment and Power Cabling		3.2.27			6.2.2.3	PE-9	AOR-20 AOR-73
2.4.21	Physical Device Access Control		5.5.5, 5.2.1		CIP 006-2 (R2, R3)		PE-3	AOR-74
2.5.1	System and Services Acquisition Policy and Procedures						SA-1	ADR-7 ADR-18 AAY-12

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
2.5.2	Allocation of Resources						SA-2	ADR-8 ADR-19
2.5.3	Life-Cycle Support						SA-3	ADR-9 ADR-20
2.5.4	Acquisitions						SA-4	ADR-10 ADR-21
2.5.5	Control System Documentation						SA-5	ADR-11 ADR-22
2.5.6	Software License Usage Restrictions						SA-6	ADR-12 ADR-23
2.5.7	User-installed Software						SA-7	ADR-13 ADR-24
2.5.8	Security Engineering Principals	62351-1 (5.7)					SA-8 SA-13	ADR-14 ADR-25
2.5.9	Outsourced Control System Services						PS-7	ADR-15 ADR-26
2.5.10	Vendor Configuration Management						SA-4 SA-10	ADR-16 ADR-27 ADR-52
2.5.11	Vendor Security Testing						SA-11	ADR-17 ADR-28
2.5.12	Vendor Life-cycle Practices							ADR-29
2.6.1	Configuration Management Policy and Procedures		5.6	A.3.2.2.3.1 A.3.2.6.2	CIP 003-2 (R6)		CM-1	ADR-30 AAY-13
2.6.2	Baseline Configuration				CIP-2 007 (R9)		CM-2	ADR-31
2.6.3	Configuration Change Control		6.5.3.6	4.3.4.3	CIP 003-2 R6		CM-3 SA-10	ADR-32
2.6.4	Monitoring Configuration Changes			4.3.4.3.3	CIP 003-2 R6		CM-4 SA-10	FIN-18 ADR-33
2.6.5	Access Restrictions for Configuration Change			A.3.4.3.6	CIP 003-2 R6		CM-5	ADR-34

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
2.6.6	Configuration Settings				CIP 003-2 (R6) CIP 005 (R2.2)		CM-6	ADR-35
2.6.7	Configuration for Least Functionality				CIP 007-2 (R2)		CM-7	ADR-36
2.6.8	Configuration Assets				CIP 002-2 (R3, R4) CIP 003-2 (R6) CIP 005-2 (R2.2, R5.1, R5.2) CIP 007-2 (R3, R9)		CM-8	ADR-37
2.6.9	Addition, Removal, and Disposition of Equipment			4.3.3.3.9	CIP 003-2 (R6)		MP-6	ADR-38
2.6.10	Factory Default Authentication Management			4.3.3.5.7	CIP 005-2 R4.4			ADR-39
2.7.1	Strategic Planning Policy and Procedures			4.3.2.3			PL-1	AOR-31 AOR-75 AAY-8 AAY-17
2.7.2	Control System Security Plan	62351-1 (5.7)		A.3.2.3.4.1		6.1.2	PL-2	AOR-32 AOR-76 AAY-18
2.7.3	Interruption Identification and Classification			4.3.4.5			RA-3	FIN-9 FAS-4 AOR-77
2.7.4	Roles and Responsibilities			4.3.4.5.4	CIP 008-2 (R1.2) CIP 009-2 R1.2		IR-1	AOR-78
2.7.5	Planning Process Training		5.6	A.3.2.4.1	CIP 004-2 (R2)		AT-3	AOR-79
2.7.6	Testing			4.3.4.5.11	CIP 007-2 R1		CA-2	AOR-80
2.7.7	Investigate and Analyze	62351-1 (5.5)		A.4.3.3	CIP 008-2 (R1)			FBS-28 AOR-81
2.7.8	Corrective Action	-		4.4.3.4	CIP 009 (R3)		CP-4	FIN-4 AOR-82
2.7.9	Risk Mitigation	62351-1		4.4.3.4	CIP 002-2 (R1)		PL-2	AOR-83

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
		(5.7)						
2.7.10	System Security Plan Update	62351-1 (5.7)		4.3.2.6.7			PL-2	AOR-84
2.7.11	Rules of Behavior			4.3.3.7.1			PL-4	AOR-34 AOR-85
2.7.12	Security-Related Activity Planning	62351-1 (5.5)			CIP 007-2 (R1.1)		PL-6	AOR-36 AOR-86
2.8.1	System and Communication Protection Policy and Procedures			A.3.2.1	CIP 003-2 (R1, R1.1, R1.3)		SC-1	FRS-1 AAY-11
2.8.2	Management Port Partitioning						SC-3	FRS-2
2.8.3	Security Function Isolation						SC-7	FAZ-1 FRS-3 ADR-51 AAC-6 AAC-7
2.8.4	Information Remnants						SC-4	FCP-1 FCP-11 FRS-4
2.8.5	Denial-of-Service Protection	62351-1 (5.6.2,5.8)		A.2.3.3.3			SC-5	FAV-7 FRS-5
2.8.6	Resource Priority			4.2.3.6			SC-6	FAV-5 FAV-6 FAV-8 FRS-6
2.8.7	Boundary Protection			4.3.3.4.2	CIP 005-2 (R1, R1.1, R1.2, R1.3, R1.4, R1.6, R2, R2.1-R2.4, R5, R5.1)		SC-7	FBS-15 FBS-16 FBS-17 FBS-18 FBS-19 FBS-20 FRS-7

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
2.8.8	Communication Integrity						SC-8	FIN-37 FIN-41
2.8.9	Communication Confidentially			A.3.3.6.1			SC-9	FBS-18
2.8.10	Trusted Path						SC-11	FIN-26 FRS-10
2.8.11	Cryptographic Key Establishment and Management						SC-12	FRS-11 FTS-2
2.8.12	Use of Validated Cryptography						SC-13	FAS-2 FCS-6 FRS-12
2.8.13	Collaborative Computing						SC-15	FRS-13
2.8.14	Transmission of Security Parameters						SC-16	FIN-38 FRS-14
2.8.15	Public Key Infrastructure Certificates						SC-17	FRS-15 FTS-1
2.8.16	Mobile Code						SC-18	FRS-16 ADR-50
2.8.17	Voice-over-Internet Protocol						SC-19	FRS-17
2.8.18	System Connections			A.3.3.3.3.1	CIP 005-2 (R2, R2.2-R2.4)		CA-3	FRS-18 AOR-112
2.8.19	Security Roles			4.3.3.7.3	CIP 003-2 (R5)		SA-9	FID-2
2.8.20	Message Authenticity	62351-1 (6.8.1)	5.10.2.3				SC-8	FNR-9 FRS-19
2.8.21	Architecture and Provisioning for Name/Address Resolution Service						SC-22	FIN-40 FRS-21
2.8.22	Secure Name/Address Resolution Service (Authoritative Source)						SC-20	FIN-39 FRS-22
2.8.23	Secure Name/Address						SC-21	FRS-23

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
	Resolution Service (Recursive or Caching Resolver)							
2.9.1	Information and Document Management Policy and Procedures			4.3.4.4	CIP 003-2 R4			AHR-18
2.9.2	Information and Document Retention			4.3.4.4.1	CIP 006-2 (R7)			AHR-19
2.9.3	Information Handling			4.3.4.4.4	CIP 003-2 R4.1		MP-1	AHR-20
2.9.4	Information Classification			4.3.4.4.2	CIP 003-2 (R4, R4.2)		RA-2	AHR-21
2.9.5	Information Exchange			4.3.4.4.2				AHR-22
2.9.6	Information and Document Classification			4.3.4.4.3	CIP 003 (R4,R4.1,R4.2)			AHR-23
2.9.7	Information and Document Retrieval			4.3.4.4.5				AHR-24
2.9.8	Information and Document Destruction			4.3.4.4.4				AHR-25
2.9.9	Information and Document Management Review			4.3.4.4.7	CIP 003-2 (R4)			AHR-26
2.9.10	Automated Marking						AC-15	FIN-42 AHR-27
2.9.11	Automated labeling						AC-16	FID-8 AHR-28
2.10.1	System Maintenance Policy and Procedures			4.3.4.3			MA-1	ADR-1 ADR-40
2.10.2	Legacy System Upgrades			4.3.4.3.4	CIP 003-2 (R6)			ADR-41
2.10.3	System Monitoring and Evaluation	62351-1 (5.2)	5.6	4.3.4.3.6	CIP 007-2 (R8)		CA-2	FIN-18
2.10.4	Backup and Recovery		5.7.4	4.3.4.3.9	CIP 009-2 (R4)		CP-6	ADR-43
2.10.5	Unplanned System Maintenance			A.3.4.3.8			PL-6	ADR-44
2.10.6	Periodic System Maintenance			A.3.4.3.1			MA-2	ADR-2

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
								ADR-45
2.10.7	Maintenance Tools						MA-3	FIN-31 ADR-3 ADR-46
2.10.8	Maintenance Personnel						MA-5	FAZ-4 ADR-5 ADR-47
2.10.9	Remote Maintenance	62351-1 (6.9.1)	4.4, 5.5.4.1, 5.5.5				MA-4	FCP-15 ADR-4 ADR-48
2.10.10	Timely Maintenance				CIP 009-2 (R4)		MA-6	ADR-6 ADR-49
2.11.1	Security Awareness Training Policy and Procedures			A.3.2.4.1	CIP 004-2 (R1, R2)		AT-1	AOR-1 AOR-87
2.11.2	Security Awareness			A.3.2.4.2	CIP 004-2 (R1)		AT-2	AOR-2 AOR-88
2.11.3	Security Training			A.3.2.4.2	CIP 004-2 (R2)		AT-3	AOR-3 AOR-89
2.11.4	Security Training Records			A.3.2.4.3.2	CIP 004-2 (R2.3)		AT-4	AOR- AOR-90
2.11.5	Contact with Security Groups and Associations						AT-5	AOR-5 AOR-91
2.11.6	Security Responsibility Training	62351-1 (5.7)		A.3.2.4.3.2				AOR-92
2.12.1	Incident Response Policy and Procedures			A.3.4.5.1	CIP 008-2 (R1, R1.2-R1.5)	6.1.1	IR-1	AHR-1 AHR-11 AHR-29
2.12.2	Continuity of Operations Plan			A.3.2.5	CIP 008-2 (R1) CIP 009-2 (R1)		CP-1	FCP-12 FIN-43 AHR-30
2.12.3	Continuity of Operations Roles and Responsibilities			A.3.2.5.4.1	CIP 009-2 (R1.1, R1.2)	6.2.3	CP-2	AHR-2 AHR-31

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
2.12.4	Incident Response Training			A.3.4.5.5.2	CIP 009-2 (R2)		IR-2	AHR-3 AHR-12 AHR-32
2.12.5	Continuity of Operations Plan Testing			A.3.4.5.5.1	CIP 008-2 (R1.6) CIP 009-2 (R2, R5)	6.2.3 6.2.3.2	CP-4, IR-3	AHR-4 AHR-13 AHR-33
2.12.6	Continuity of Operations Plan Update			A.3.4.5.2	CIP 009-2 (R3)		CP-5	AHR-5 AHR-34
2.12.7	Incident Handling			4.3.3.3.8 A.4.2.2	CIP 008-2 (R1.1, R1.2, R1.3)		IR-4	FIN-5 FAC-1 FAC-2 FAS-7 FAS-8 AOR-17 AHR-14 AHR-35
2.12.8	Incident Monitoring				CIP 007-2 (R6, R6.2)		IR-5	AHR-15 AHR-36
2.12.9	Incident Reporting			4.3.4.5.5	CIP 008-2 (R1.3)		IR-6	FAS-3 AHR-16 AHR-37
2.12.10	Incident Response Assistance				CIP 008-2 (R1, R1.2, R1.3)		IR-7	AHR-17 AHR-38
2.12.11	Incident Response Investigation and Analysis			A.3.4.5.5.2	CIP 008-2 (R1)		PE-6	AHR-39
2.12.12	Corrective Action			A.3.4.5.5.2 .j	CIP 008-2 (R1.4) CIP 009-2 (R3)		CP-4	FIN-6 AHR-40
2.12.13	Alternative Storage Sites			A.3.2.5.4.2 .b			CP-6	AHR-6 AHR-41
2.12.14	Alternate Command/Control Methods			A.3.3.4.3			CP-4 **CP-8**	AHR-7 AHR-42
2.12.15	Alternate Control Center			A.3.3.4.3			CP-6,7	AHR-8

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
							CP-8	AHR-43
2.12.16	Control System Backup			4.3.4.3.9	CIP 009-2 (R4, R5)	6.2.3	CP-9	AHR-9 AHR-44
2.12.17	Control System Recovery and Reconstitution			4.3.2.5	CIP 009-2 (R4)	6.2.3.2	CP-10	FCP-12 FIN-1 FIN-12 FIN-14 FAV-1 FAV-9 AHR-10 AHR-45
2.12.18	Fail-Safe Response					5.10	**CP-8**	FIN-1 FIN-11 FIN-12 AHR-46
2.13.1	Media Protection and Procedures					3.3.2	MP-1	AOR-6 AOR-93
2.13.2	Media Access					3.3.2	MP-2	FCP-15 AOR-7 AOR-94
2.13.3	Media Classification				CIP 003-2 (R4)	6.2.1 6.2.2	AC-16	AOR-8 AOR-95
2.13.4	Media Labeling						MP-3	AOR-8 AOR-96
2.13.5	Media Storage						MP-4	AOR-9 AOR-97
2.13.6	Media Transport						MP-5	AOR-10 AOR-98
2.13.7	Media Sanitization and Storage				CIP 007-2 (R7, R7.1, R7.2, R7.3)	6.2.7	MP-6	AOR-11 AOR-99
2.14.1	System and Information Integrity Policy and Procedures	62351-1 (5.4)					SI-1	FIN-29

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
2.14.2	Flaw Remediation				CIP 007-2 (R3, R3.1, R3.2)		SI-2	FIN-30
2.14.3	Malicious Code Protection				CIP 007-2 (R4, R4.1, R4.2)	3.3.2, 6.2, 6.2.6, 6.2.6.1	**SI-3**	FIN-5 FIN-31 FAS-4
2.14.4	System Monitoring Tools and Techniques				CIP 007-2 (R6)		SI-4	FCP-13 FIN-5 FIN-7 FIN-8 FIN-9 FIN-25
2.14.5	Security Alerts and Advisories						SI-5	
2.14.6	Security Functionality Verification				CIP 007-2 R1		SI-6	FIN-3 FIN-20 FIN-21 FIN-22 FIN-24 FIN-32 FNS-3
2.14.7	Software and Information Integrity						SI-7	FIN-2 FIN-5 FIN-33 FIN-43 FAS-1 FNS-1
2.14.8	Spam Protection				CIP 007-2 (R4)	3.2, 6.2.6	SI-8	
2.14.9	Information Input				CIP 003-2 (R5) CIP 007-2 (R5, R5.1, 5.2)		SI-9	FIN-26 FIN-34 FRS-24
2.14.10	Information Input Accuracy, Completeness, Validity and Authenticity						SI-10	FIN-17 FIN-27 FIN-35 FRS-25

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
								FRS-26 FRS-33
2.14.11	Error Handling						SI-11	FCP-14
2.14.12	Information Output and Retention						SI-12	FIN-28 FIN-36
2.15.1	Access Control Policies and Procedures	62351-1 (6.2)		4.3.3.3.1	CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)	3.2.2	AC-1	AOR-117 AAC-1 AAC-8
2.15.2	Identification and Authentication Procedures and Policy			4.3.3.5.1	CIP 003-2 (R1, R1.1, R1.3)		IA-1	AOR-116
2.15.3	Account Management	62351-1 (6.2)		4.3.3.5	CIP 003-2 (R5, R5.1, R5.2, 5.3) CIP 004-2 (R4, R4.1, R4.2) CIP 005-2 (R2.5) CIP 007-2 (R5, R5.1, R5.2)		AC-2	FAT-27 FRS-37 AOR-118 AAY-1 AAY-2
2.15.4	Identifier Management			4.3.3.5.4			IA-4	FCP-1 FID-6
2.15.5	Authenticator Management			4.3.3.6.3	CIP 007-2 (R5, R5.1, R5.2, R5.3)		IA-5	FCP-1 FCP-2 FCP-3 FCP-4 FCP-13 FCP-15 FAT-55
2.15.6	Supervision and Review			A.3.3.5.4.1	CIP 007-2 (R5.1.2)		PE-2	AAC-2 AAC-9 AAC-13
2.15.7	Access Enforcement	62351-1 (6.7.1)		A.3.3.5.3	CIP 004-2 (R4) CIP 005-2 (R2, R2.1-R2.4)		AC-3	FIN-34 FAV-3 FID-4 FAZ-3 FID-7

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
								FAT-27 FAT-28 FAT-29 FAT-30 FAT-31 FAT-32 FAZ-11 FRS-24 FRS-25 FRS-27 FRS-28 AAC-3 AAC-4 AAC-10 AAC-11
2.15.8	Separation of Duties			A.3.3.5.3			AC-5	FAT-36 FAZ-2
2.15.9	Least Privilege			A.3.3.4.1	CIP-007-2 (R5.1)		AC-6	FAT-37 FAZ-10
2.15.10	User Identification and Authentication			4.3.3.6.2	CIP 005-2 (R2,)		AC-2	FID-1 FID-5 FAT-4 FAT-26 FAT-42
2.15.11	Permitted Actions without Identification and Authentication						AC-14	
2.15.12	Device Authentication and Identification	62351-1 (6.3)		A.3.3.6.3.1			IA-3,	FAT-2
2.15.13	Authenticator Feedback						IA-6	FCP-15
2.15.14	Cryptographic Module Authentication						IA-7	FAT-3 FCS-6
2.15.15	Information Flow Enforcement						AC-4	FCP-16

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
								FAT-5 FAT-27 FAZ-3 FRS-27
2.15.16	Passwords			A.3.3.6.3.1, A.3.3.6.2	CIP 007-2 (R5.3)		--	FIN-16 FAT-55
2.15.17	System Use Notification				CIP-005-2 (R2.6)		AC-8	FAC-32 FBS-10 FNS-5 AOR-113
2.15.18	Concurrent Session Control						AC-10	FAZ-14 FBS-2 FBS-4
2.15.19	Previous Logon Notification						AC-9	FAC-31 FBS-11 FBS-12 FNS-4
2.15.20	Unsuccessful Logon Notification			A.3.3.6.2			AC-7	FAT-57 FAZ-12 AAY-4
2.15.21	Session Lock						AC-11	FAT-1 FAT-46 FAT-56 FAZ-12 FBS-5 FBS-7
2.15.22	Remote Session Termination						Withdrawn	FAZ-13 FBS-5 FBS-8 FRS-44
2.15.23	Remote Access Policy and Procedures			4.3.3.6.5	CIP 005-2 (R1, R1.1, R1.2, R2, R2.3, R2.4		AC-17	FBS-1 AOR-114

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
2.15.24	Remote Access	62351-1 (6.9.1)		4.3.3.6.4	CIP 005-2 (R2, R3, R3.1, R3.2		AC-17	FAT-12
2.15.25	Access Control for Portable and Mobile Devices			A.3.3.6.2	CIP 005-2 (R2.4, R5, R5.1)	6.2.2.2	AC-19	FAT-21
2.15.26	Wireless Access Restrictions	62351-1 (5.6.1)				6.3.2.5	AC-18	FAT-21
2.15.27	Personally Owned Information						AC-20	AOR-115
2.15.28	External Access Protections						IA-2 IA-8	FCP-11
2.15.29	Use of External Information Control Systems			A.3.2.3.4.1 .d A.3.3.4.2			SC-7	FIN-3 FAZ-1
2.16.1	Audit and Accountability Process and Procedures			A.3.4.2.5.3	CIP 003-2 (R1,R1.1, R1.3)	4.2 6.3.3	AU-1	AOR-119 AAY-5 AAY-6
2.16.2	Auditable Events	62351-1 (4.3)			CIP 005-2 (R3) CIP 007-2 (R5.1.2, R5.2.3, R6.1, R6.3)	6.3.3	AU-2 AU-13	FAC-2 FAC-3 AAY-7
	Content of Audit Records	62351-1 (4.3)			CIP 007-2 (R5.1.2)	6.3.3	AU-3	FNR-2 FAC-7 FAC-8 FAC-9
2.16.4	Audit Storage						AU-4	FAC-6 FAC-25 FAC-27
2.16.5	Response to Audit Processing Failures					6.3.3	AU-5	FAC-26 FAC-28
2.16.6	Audit Monitoring, Process, and Reporting	62351-1 (4.3)			CIP 007-2 (R6.5)	6.3.3	AU-6	FAC-10 FAC-11 FAC-12 FAC-13 FAC-14

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
								FAC-15 FAC-16 FAC-17 FAC-18 FAC-19 AOR-120
2.16.7	Audit Reduction and Report Generation					6.3.3	AU-7	FAC-20 FAC-21 FAC-22 FAC-29
2.16.8	Time Stamps					6.3.3	AU-8	FAC-30
2.16.9	Protection of Audit Information				CIP 003-2 (R4)	6.3.3	AU-9	FAC-4 FAC-5 FAC-24
2.16.10	Audit Record Retention				CIP 005-2 (R5.3) CIP 007-2 (R5.1.2, R6.4) CIP 008-2 (R.2)	6.3.3	AU-11	AHR-47
2.16.11	Conduct and Frequency of Audits			A.4.2.4.1b		6.3.1	AU-1	AOR-121
2.16.12	Auditor Qualification			4.4.2.6		4.2.6	CA-2	AOR-122
2.16.13	Audit Tools			A.2.3.3.6.3			AU-7	AOR-123
2.16.14	Security Policy Compliance						CA-1	FNS-2 FNS-3 AOR-124
2.17.1	Monitoring and Reviewing Control System Security management Policy and Procedures			A.4.3.3			CA-2	AOR-100
2.17.2	Continuous Improvement		5.6	A.4.3.6.2.n		6.1.2	CA-2-2	AOR-101
2.17.3	Monitoring of Security Policy			4.4.3.6, 4.4.3.8			CM-1	AOR-102
2.17.4	Best Practices			4.4.3.6			SI-5	AOR-103

DHS Catalog of Control System Security	DHS Catalog of Control System Security	IEC 62351	ANSI/ISA 99-1	ANSI/ISA 99-2	NERC CIPs (1-9) May 2009	NIST SP 800-82	NIST SP 800-53 Rev 3	AM System Security V1.01
2.17.5	Security Accreditation						CA-6 **PM-10**	FAZ-9 AOR-104
2.17.6	Security Certification						CA-4	AOR-33 AOR-105
2.18.1	Risk Assessment Policy and Procedures	62351-1 (5.2.1)	5.5.3	4.3.4.2	CIP 002-2 (R1, R1.1, R1.2, R4) CIP 003-2 (R1, R1.3)	6.1.1	RA-1	
2.18.2	Risk Management Plan	62351-1 (5.2.1)		4.2.3.8, A.2.3.3.1, A.2.3.3.5.2	CIP 003-2 (R4, R4.1, R4.2)		**PM-9**	
2.18.3	Certification, Accreditation, and Security Assessment Policies and Procedures			A.3.4.2.5.3			CA-1	
2.18.4	Security Assessments	62351-1 (5.7)		A.3.4.2.5.3	CIP 007-2 (R1)		CA-2	
2.18.5	Control System Connections				CIP 005-2 (R2)		CA-3	FAZ-1
2.18.6	Plan of Action and Milestones			A.4.3.6.2	CIP 005-2 (R4.5) CIP 007-2 (R8.4)		CA-5	
2.18.7	Continuous Monitoring	62351-1 (5.7)		A.4.2.1			CA-7	
2.18.8	Security Categorization			4.3.3.			RA-2	
2.18.9	Risk Assessment	62351-1 (5.2.1,5.5)	5.5.3	4.2.3.8	CIP 002-2 (R1.2)		RA-3	
2.18.10	Risk Assessment Update	62351-1 (5.5)		4.2.3.10	CIP 002-2 R4		RA-4	
2.18.11	Vulnerability Assessment and Awareness			4.2.3.12	CIP 005-2 (R4, R4.2, R4.3, R4.4) CIP 007-2 (R8)		RA-5	ADR-42
2.18.12	Identify, Classify, Analyze, and Prioritize Potential Security Risks			4.2.3.7 4.2.3.8				

APPENDIX C

NIST CSCTG VULNERABILITY CLASSES

C.1 INTRODUCTION

This document is in draft format. 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 the thing which can be leveraged to cause disruption or have otherwise undo influence over the Smart Grid. Actual attacks and impacts will be noted in additional documentation still being produced.

We envision this information to be used in discussions specifically by the Cyber Security Coordination Task Group at large and its various subgroups.

As input to the classification process, we used many sources of vulnerability information, including NIST 800-82 and 800-53, OWASP vulnerabilities, CWE vulnerabilities, attack documentation from INL, input provided by the NIST CSCTG Bottoms-Up group, and the NERC CIP standards. Compiling one document from these many sources with different view-points has sometimes been challenging, and further refinement is planned based on feedback from the CSCTG. This document is still under revision and is open for comment.

C.2 PEOPLE, POLICY & PROCEDURE

C.2.1 Training

This category of vulnerabilities is related to personnel training in all forms that relates to implementing, maintaining, and operating systems.

C.2.1.1. Insufficient Trained Personnel

Description

Throughout the entire organization everyone needs to acquire a level of Security Awareness training, the degree of this training also is varied based on the technical responsibilities and/or the critical asset/s one is responsible for.

Through this training effort everyone gets a clear understanding of the importance of Cyber Security but more important everyone begins to understand the role they play and importance of each role.

Examples

- Freely releasing information of someone's status, i.e. away on vacation, not in today, etc.
- Opening emails and attachments form unknown sources.
- Posting passwords for all to see.

Potential Impact:

As the social engineering element is one of the primary initiatives in acquiring as much information as possible, giving one in some cases all the visibility, knowledge and opportunity to execute a successful attack.

C.2.1.2. Inadequate Security Training and Awareness Program

Description

As part and continuation of Insufficient trained personnel with the one element being that within the Policy framework to highlight the requirement of a continuous/re-train effort over some identified period of time. The Security profile will always be changes so will the need for new procedures, new technologies and re-enforcement of the importance of the cyber security program.

Examples

Potential Impact

C.2.2 Policy & Procedure

C.2.2.1. Insufficient Identity Validation, Background Checks

Description

Identity Validation/background levels goes directly to the individual's area of responsibility and the level of information they are given access to. The more sensitive information available to an individual the deeper and more detailed the validation and checking process is needed.

Use of know references and background checking by established groups should be implemented.

Examples

Potential Impact

The human factor is always going to be considered the weakest element within any Security posture. But validation and background checking are measures that are imperative to be able manage this element. As the amount of and sensitivity of the information one is given the responsibility of a consideration of multiple signoffs before that information is released, another step in not giving any one individual/s the "keys to the kingdom".

C.2.2.2. Inadequate Security Policy

Description

Vulnerabilities are often introduced due to inadequate policies or the lack of policies. Policies need to drive operating requirements and procedures…

Examples

Potential Impact

Security policy must be structured with several key elements, they must be well understood, they must be of a practical approach, they must be well in practice and monitored, they must be enforceable and they must be flexible enough that they can be continuously improved.

C.2.2.3. Inadequate Privacy Policy

Description

A privacy policy that documents the necessity of protection of private personal information is necessary to ensure that data is not exposed or shared unnecessarily.

Examples

Potential Impact

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

C.2.2.4. Inadequate Patch Management Process

Description

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

Examples

Potential Impact

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

C.2.2.5. Inadequate Change and Configuration Management

Description

Change and configuration management processes are essential to ensuring that

Examples

Changing software configuration that enables an insecure profiles
Adding vulnerable hardware
Changing network configuration that reduces the security profile of the system
Introduction of tampered devices into the system

Potential Impact

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

C.2.2.6. Unnecessary System Access

Description

Under policy is needs to be very clear that only access and information is granted on an as need basis, access needs to be well controlled and monitored and again very dependent of the access requirement and level of impact that access could have on an organization.

Examples

Potential Impact

C.2.3 Risk Management

The vulnerabilities in this section are related to the implementation of a risk management program. Deficiencies in a risk management program can lead to vulnerabilities not only at the technical layer, but at the business decision-making layer as well.

C.2.3.1. Inadequate Periodic Security Audits

Description

Independent security audits should review and examine a system's records and activities to determine the adequacy of system controls and ensure compliance with established security policy and procedures. Audits should also be used to detect breaches in security services and recommend changes, which may include making existing security controls more robust and/or adding new security controls.

Examples

Potential Impact

The Audit process is the only true measure to continuously evaluate the status of the implemented Security Program, from conformance to policy, the need to enhance both policy and/or procedures and evaluate security robustness of your implemented security technologies.

C.2.3.2. Inadequate Security Oversight by Management

Description

With no clear Senior Management ownership of a Security program, in the event of a policy being compromised or abused it then becomes almost impossible to enforce.

Examples

Potential Impact

Within a security program it will require the crossing of many organization operating groups, have impact on many business areas, requires an element of Human Recourses and legal involvement, without a senior management oversight/ownership it makes is very difficult to be successful. The biggest challenge is establishing this senior management oversight at the executive level within an organization.

C.2.3.3. Inadequate Continuity of Operations or Disaster Recovery Plan

Description

To ensure within the various plant/system disaster recovery plans that are in place that each highlight within their elements that if the disaster was created by a cyber related incident than part of the recovery process has to ensure elements that are focus on a cyber incident recovery. Here it is the added steps like, validating backups, ensuring devices being recovered are clean before installing the backups, incident reporting, etc…

Examples

Potential Impact

Longer than required of a possible plant or operational outage.

C.2.3.4. Inadequate Risk Assessment Process

Description

A documented assessment process, that includes consideration of business objectives, is necessary to ensure proper evaluation of risk.

Examples

- The NERC Critical Asset identification process

Potential Impact

Lack of risk assessment processes can lead to decisions made without basis in actual risk.

C.2.3.5. Inadequate Risk Management Process

Description

Unmanaged risk leads to unmanaged vulnerabilities in affected systems.

Examples

Potential Impact

Unmanaged risk and/or vulnerabilities can to lead to exploitation of impacted systems.

C.2.3.6. Inadequate Incident Response Process

Description

An incident response process is required to ensure proper notification and action in the event of an incident.

Examples

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 exposure.

C.3 PLATFORM SOFTWARE/FIRMWARE VULNERABILITIES

C.3.1 Software Development

Applications being developed for use in the Smart Grid should make use of a Secure Software Development Lifecycle. Vulnerabilities in this category can arise from a lack oversight in this area, leading to poor code implementation, leading to vulnerability.

C.3.1.1. Code Quality Vulnerability

Description

"Poor code quality 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" (OWASP page).

Examples

- Double Free
- Failure to follow guideline/specification
- Leftover Debug Code
- Memory leak
- Null Dereference
- Poor Logging Practice
- Portability Flaw
- Undefined Behavior
- Uninitialized Variable
- Unreleased Resource
- Unsafe Mobile Code
- Use of Obsolete Methods
- Using freed memory

Potential Impact

C.3.1.2. Arbitrary code execution Authentication Vulnerability

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

- Confidence tricks
- Remote technical tricks
- Local technical tricks
- Victim mistakes
- Implementation oversights
- Denial of service attacks
- Enrollment attacks (OWASP page "Comprehensive list of Threats to Authentication Procedures and Data")
- Allowing password aging
- Authentication Bypass via Assumed-Immutable Data
- Empty String Password
- Failure to drop privileges when reasonable
- Hard-Coded Password
- Not allowing password aging
- Often Misused: Authentication
- Reflection attack in an auth protocol
- Unsafe Mobile Code
- Using password systems
- Using referer field for authentication or authorization
- Using single-factor authentication

Potential Impact

Access granted without official permission

C.3.1.3. Authorization Vulnerability

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

- Code Permission Vulnerability
- Access control enforced by presentation layer
- File Access Race Condition: TOCTOU
- Least Privilege Violation
- Often Misused: Privilege Management
- Using referer field for authentication or authorization

Potential Impact

C.3.1.4. Cryptographic Vulnerability

Description

Cryptography is the use of mathematical principles 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 which allow an attacker to view, modify or forge encrypted data, or impersonate another party through digital signature abuse.

Examples

- Algorithm problems
- Key management problems
- Random number generator problems
- Addition of data-structure sentinel
- Assigning instead of comparing
- Comparing instead of assigning
- Deletion of data-structure sentinel
- Duplicate key in associative list
- Failure to check whether privileges were dropped successfully
- Failure to deallocate data
- Failure to provide confidentiality for stored data
- Guessed or visible temporary file
- Improper cleanup on thrown exception
- Improper error handling
- Improper temp file opening
- Incorrect block delimitation
- Misinterpreted function return value
- Missing parameter
- Omitted break statement
- Passing mutable objects to an un-trusted method
- Symbolic name not mapping to correct object
- Truncation error
- Undefined Behavior
- Uninitialized Variable
- Unintentional pointer scaling
- Use of sizeof() on a pointer type
- Using the wrong operator

Potential Impact

C.3.1.5. Environmental Vulnerability

Description

"This category 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." (OWASP page)

Examples

- ASP.NET Misconfigurations
- Empty String Password
- Failure of true random number generator
- Information leak through class cloning
- Information leak through serialization
- Insecure Compiler Optimization
- Insecure Transport
- Insufficient Session-ID Length
- Insufficient entropy in pseudo-random number generator
- J2EE Misconfiguration: Unsafe Bean Declaration
- Missing Error Handling
- Publicizing of private data when using inner classes
- Relative path library search
- Reliance on data layout
- Relying on package-level scope
- Resource exhaustion
- Trust of system event data

Potential Impact

C.3.1.6. Error Handling Vulnerability

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
- Catch NullPointerException
- Empty Catch Block
- Improper cleanup on thrown exception
- Improper error handling
- Information Leakage
- Missing Error Handling
- Often Misused: Exception Handling
- Overly-Broad Catch Block
- Overly-Broad Throws Declaration

- Return Inside Finally Block
- Uncaught exception
- Unchecked Error Condition

Potential Impact

C.3.1.7. General Logic Error

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
- Assigning instead of comparing
- Comparing instead of assigning
- Deletion of data-structure sentinel
- Duplicate key in associative list
- Failure to check whether privileges were dropped successfully
- Failure to deallocate data
- Failure to provide confidentiality for stored data
- Guessed or visible temporary file
- Improper cleanup on thrown exception
- Improper error handling
- Improper temp file opening
- Incorrect block delimitation
- Misinterpreted function return value
- Missing parameter
- Omitted break statement
- Passing mutable objects to an untrusted method
- Symbolic name not mapping to correct object
- Truncation error
- Undefined Behavior
- Uninitialized Variable
- Unintentional pointer scaling
- Use of sizeof() on a pointer type
- Using the wrong operator

Potential Impact

C.3.1.8. Input Validation

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".

Examples

- Buffer Overflow
- Format String
- Improper Data Validation
- Log Forging
- Missing XML Validation
- Process Control
- String Termination Error
- Unchecked Return Value: Missing Check against Null
- Unsafe JNI
- Unsafe Reflection
- Validation performed in client

Potential Impact

C.3.1.9. Logging and Auditing Vulnerability

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
- Log Corruption
- Lack of Regular Log Review
- Information Leakage
- Log Forging
- Log injection
- Poor Logging Practice
- Cross-site scripting via HTML log-viewers

Potential Impact

C.3.1.10. Password Management Vulnerability

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

Allowing password aging
Empty String Password
Hard-Coded Password
Not allowing password aging
Password Management: Hardcoded Password
Password Management: Weak Cryptography
Password Plaintext Storage
Password in Configuration File
Using password systems

Potential Impact

C.3.1.11. Path Vulnerability

Description

"This category 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" (OWASP page).

Examples

- Path Traversal Attack
- Relative Path Traversal Attack
- Virtual Files Attack
- Path Equivalence Attack
- Link Following Attack
- Virtual Files Attack

Potential Impact

C.3.1.12. Protocol Errors

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
- Failure to check for certificate revocation

- Failure to check integrity check value
- Failure to encrypt data
- Failure to follow chain of trust in certificate validation
- Failure to protect stored data from modification
- Failure to validate certificate expiration
- Failure to validate host-specific certificate data
- Key exchange without entity authentication
- Storing passwords in a recoverable format
- Trusting self-reported DNS name
- Trusting self-reported IP address
- Use of hard-coded password

Potential Impact

Compromise of security protocols such as TLS

C.3.1.13. Range and Type Error Vulnerability

Description

Range and type errors are common programming mistakes. This vulnerability class covers the various types of errors that have potential security consequences. (This seems like quite an umbrella vulnerability class. Is it too broad a scope.)

Examples

- Access control enforced by presentation layer
- Buffer Overflow
- Buffer underwrite
- Comparing classes by name
- Deserialization of untrusted data
- Doubly freeing memory
- Failure to account for default case in switch
- Format String
- Heap overflow
- Illegal Pointer Value
- Improper string length checking
- Integer coercion error
- Integer overflow
- Invoking untrusted mobile code
- Log Forging
- Log injection
- Miscalculated null termination
- Null Dereference
- Often Misused: String Management
- Reflection injection
- Sign extension error

- Signed to unsigned conversion error
- Stack overflow
- Truncation error
- Trust Boundary Violation
- Unchecked array indexing
- Unsigned to signed conversion error
- Using freed memory
- Validation performed in client
- Wrap-around error

Potential Impact

C.3.1.14. Sensitive Data Protection Vulnerability

Description

"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 lifecycles, 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" (OWASP page).

Examples

- Information leakage results from insufficient memory clean-up
- Inappropriate protection of cryptographic keys
- Clear-text Passwords in configuration files
- Lack of integrity protection for stored user data
- Hard-Coded Password
- Heap Inspection
- Information Leakage
- Password Management: Hardcoded Password
- Password Plaintext Storage
- Privacy Violation

Potential Impact

C.3.1.15. Session Management Vulnerability

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 as variables 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
- Session Fixation

Potential Impact

C.3.1.16. Concurrency, Synchronization and Timing Vulnerability

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
- Covert timing channel
- Failure to drop privileges when reasonable
- Failure to follow guideline/specification
- File Access Race Condition: TOCTOU
- Member Field Race Condition
- Mutable object returned
- Overflow of static internal buffer
- Race Conditions
- Reflection attack in an auth protocol
- State synchronization error
- Unsafe function call from a signal handler

Potential Impact

C.3.1.17. Insufficient Safeguards for Mobile Code

Description

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

Examples

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

Potential Impact

C.3.1.18. Buffer Overflow

Description

Software used to implement an ICS could be vulnerable to buffer overflows; adversaries could exploit these to perform various attacks. (SP 800-82)

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. (CWE)

Examples

- CVE-1999-0046
- buffer overflow in local program using long environment variable
- CVE-2000-1094
- buffer overflow using command with long argument
- CVE-2001-0191
- By replacing a valid cookie value with an extremely long string of characters, an attacker may overflow the application's buffers.
- CVE-2002-1337
- buffer overflow in comment characters, when product increments a counter for a ">" but does not decrement for "<"
- CVE-2003-0595
- By replacing a valid cookie value with an extremely long string of characters, an attacker may overflow the application's buffers (CWE).

Potential Impact

C.3.1.19. Mishandling of Undefined, Poorly Defined, or “Illegal” Conditions

Description

Some ICS implementations are vulnerable to packets that are malformed or contain illegal or otherwise unexpected field values (SP 800-82)

Examples

Potential Impact

C.3.1.20. Use of Insecure Protocols

Description

Protocols are expected patterns of behavior that allow communition 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 (SP 800-82).
- Use of clear text protocols such as FTP and Telnet
- Use of proprietary protocols lacking security features

Potential Impact

C.3.1.21. Weaknesses that Affect Files and Directories

Description

Weaknesses in this category affect file or directory resources (CWE).

Examples

- UNIX Path Link Problems
- Windows Path Link Problems
- Windows Virtual File Problems
- Mac Virtual File Problems
- Failure to Resolve Case Sensitivity
- Path Traversal
- Failure to Change Working Directory in chroot Jail
- Often Misused: Path Manipulation
- Password in Configuration File
- Improper Ownership Management
- Improper Resolution of Path Equivalence
- Information Leak Through Server Log Files
- Files or Directories Accessible to External Parties
- Improper Link Resolution Before File Access ('Link Following')

- Improper Handling of Windows Device Names
- Improper Sanitization of Directives in Statically Saved Code ('Static Code Injection')

Potential Impact

C.4.1. API USAGE AND IMPLEMENTATION

C.4.1.1. API Abuse

Description

"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" (OWASP page).

Examples

"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" (OWASP page).

- Dangerous Function
- Directory Restriction Error
- Failure to follow guideline/specification
- Heap Inspection
- Ignored function return value
- Object Model Violation: Just One of equals() and hashCode() Defined
- Often Misused: Authentication
- Often Misused: Exception Handling
- Often Misused: File System
- Often Misused: Privilege Management
- Often Misused: String Management

Potential Impact

C.4.1.2. Use of Dangerous API

Description

Use of an application programming interface (API) which is inherently dangerous or fraught with error.

Examples

- Dangerous Function such as the C function gets()
- Directory Restriction Error

- Failure to follow guideline/specification
- Heap Inspection
- Insecure Temporary File
- Object Model Violation: Just One of equals() and hashCode() Defined
- Often Misused: Exception Handling
- Often Misused: File System
- Often Misused: Privilege Management
- Often Misused: String Management
- Unsafe function call from a signal handler
- Use of Obsolete Methods

Potential Impact

C.4 PLATFORM VULNERABILITIES

C.4.1. DESIGN

C.4.1.1. Inadequate Security Architecture and Design

Description

This is more of a cause of vulnerabilities than a vulnerability in itself. Would it be appropriate to leave it out?

Examples

Potential Impact

C.4.2. IMPLEMENTATION

C.4.2.1. 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 (SP 800-82).

Examples

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

Potential Impact

C.4.2.2. Installed Security Capabilities Not Enabled by Default

Description

Security capabilities must obviously be turned on to be useful. There are many examples of operating systems (particularly Microsoft operating systems pre-Vista) 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.

Examples

Potential Impact

C.4.2.3. Absent or Deficient Equipment Implementation Guidelines

Description

Unclear implementation guidelines can lead to unexpected behavior.

A system will need to be configured correctly if it is 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 supposed to be for internal use may be more vulnerable than an interface that is supposed to be for external use. As such, guidelines for installers, operators and managers must 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.

Examples

Potential Impact

C.4.3. OPERATIONAL

C.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 exploit or close the loophole. The security of the system using the software therefore depends crucially 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.

Examples

Potential Impact

C.4.3.2. Unneeded Services Running

Description

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

Examples

Potential Impact

C.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 X number of meters are issued a remote power disconnect command within a certain time frame, alerts should also be sent.

Examples

- Inadequate network security architecture (800-82 3-8)
- Poorly configured security equipment (800-82 3-8)
- Inadequate firewall and router logs (800-82 3-11)
- No security monitoring on the network (800-82 3-11)
- Critical monitoring and control paths are not identified (800-82 3-12)

Potential Impact

- Failure to detect critical events
- Removal of Forensic Evidence
- Log Wipes

C.4.3.4. Inadequate Anomaly Tracking

Description

Alerts and logging are two useful techniques for detecting and mitigating the risk of anomalous events, but can themselves present security risks or become vulnerabilities if not done thoughtfully. Appropriate reaction to an event will vary according to the criticality of the event or a correlation of certain events, and may also need to be logged. A central logging facility may

also be necessary for correlating events. Appropriate event reactions could include automatic paging of relevant personnel in the event of persistent tamper messages or requiring positive acknowledgement to indicate supervisory approval before executing a potentially disruptive command such as simultaneously disconnecting many loads from the electrical grid or granting control access rights to hundreds of users.

Examples

Potential Impact

C.5 NETWORK

C.5.1 Inadequate Integrity Checking

Description

The integrity of message protocol and message data is should be verified before routing or processing. Devices receiving data that does not conform 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 it were correctly received.

This 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 logical bounds checking, such as preventing the shutdown of all power across an entire NAN.

Most functions of the smart grid, such as Demand Response, Load Shedding, AMR, ToU, and Distribution Automation require that data confidentiality and/or data integrity be maintained to ensure grid reliability, prevent fraud, and for 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 (800-82 3-12)
- Failure to detect and block malicious traffic in valid communication channels
- Inadequate network security architecture (800-82 3-8)
- Poorly configured security equipment (800-82 3-8)
- No security monitoring on the network (800-82 3-11)

Potential Impact

- Compromise of smart device, head node, or utility management servers.
- Buffer Overflows
- Covert Channels
- MitM
- DoS / DDoS

C.4.3.5. Inadequate Network Segregation

Description

Network architecture does a poor job at defining security zones and controlling traffic between security zones. Often this is considered a flat network that allows traffic from any portion of the network to communicate with any other portion of the network. Smart Grid examples might be 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 (800-82 3-10)
- Improperly Configured VLAN
- Inadequate access controls applied (800-82 3-8)
- Inadequate network security architecture (800-82 3-8)
- Poorly configured security equipment (800-82 3-8)
- Control networks used for non-control traffic (800-82 3-10)
- Control network services not within the control network (800-82 3-10)
- Critical monitoring and control paths are not identified (800-82 3-12)

Potential Impact

- Direct compromise of any portion of the network from any other portion of fhe 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

C.4.3.6. 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 man-in-the-middle 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.(800-82 3-12)
- Inadequate data protection between clients and access points (800-82 3-13)

Potential Impact

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

C.4.3.7. 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 (800-82 3-12)
- Insecure key storage
- Insecure key exchange
- Insufficient account lockout
- Inadequate authentication between clients and access points (800-82 3-13)
- Inadequate data protection between clients and access points (800-82 3-13)

Potential Impact

- DoS / DDoS
- MitM
- Session Hijacking
- Authentication Sniffing
- Session Injection

C.4.3.8. Insufficient Redundancy

Description

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

Examples

- Lack of redundancy for critical networks (800-82 3-9)

Potential Impact

- Denial of Service (DoS / DDoS)

C.4.3.9. 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 (800-82 3-9)
- Loss of environmental control (800-82 3-9)
- Non-critical personnel have access to equipment and network connections (800-82 3-9)

Potential Impact

- Malicious Configurations
- MitM
- EEPROM Dumping
- Micro Controller Dumping
- Bus Snooping
- Key Extraction

References

NIST Special Publication 800-82, Guide to Industrial Control Systems Security
http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

Open Web Application Security Project (OWASP)
http://www.owasp.org/index.php/Category:Vulnerability

NERC Critical Infrastructure Protection Standards
http://www.nerc.com/

APPENDIX D
Bottom Up Security Analysis of the Smart Grid

D.1 SCOPE OF THIS EFFORT

This effort, a subgroup of NIST's Cyber Security Coordination Task Group (CSCTG), is attempting to perform a bottom-up analysis of cyber security issues in the evolving Smart Grid. The goal is to identify specific protocols, interfaces, applications, best practices, etc. that could and should be developed to solve specific Smart Grid cyber security problems. The approach taken herein is **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 intends to complement the top-down efforts being followed elsewhere in the CSCTG. By proceeding with a bottom-up analysis, our hope is to more quickly identify fruitful areas for solution development, while leaving comprehensive gap analysis to other efforts of the CSCTG, and providing an independent completeness check for any top-down gap analyses.

This effort will proceed in several phases, not necessarily consecutively. First, we intend to capture a list of **evident** and **specific** security **problems** in the Smart Grid that are amenable to and *should* have **open** and **interoperable** solutions, but are not obviously solved by existing standards, de facto standards, or best practices. We include only cyber security problems that have some specific relevance to or uniqueness in the smart. Thus we do not list general 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.

Next, from the specific problems identified in this document, we intend to create a catalogue of design patterns that should identify common abstract issues and problems across the set of specific problems and solutions. This catalog of design patterns should 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.

In conjunction with development of the list of specific problems, we will develop a separate list of security issues that are not as specific as the problems in the first list. Considering these issues in specific contexts ought to lead to development of specific problems that can then be examined in detail.

The structure of this document is to give a brief definition of device classes for which the problems we mention apply to, and then to discuss specific device issues for which standard solutions may not be apparent. Finally we document non-specific cyber security issues that cut across field devices and systems. The document does not give an exhaustive treatment of each mentioned problem–the initial scope is to give an enumeration of issues and define them as briefly as possible. This document is not meant to be formal or rigid in its structure. It was developed within a context of free flowing ideas and brainstorming to build a foundation of field problems for security requirements. This document is to be treated as an interim work product. There are some apparent redundancies, but in the next iteration of the groups' analysis process these will be addressed as we start to classify issues for working towards the design patterns. The document continues to be open for further contributions as the authors feel the list of issues is not comprehensive enough.

D.2 DEVICE CLASS DEFINITIONS

The following device definitions are based on a classified NERC and DHS publication. The use of the definitions has been cleared, but the specific document reference cannot be given as it is classified in its own right. The issues that are discussed apply to these mentioned device classes.

Remote Terminal Units (RTU's) – In a SCADA system, an RTU is a device installed at a remote location to collect and code data in a transmittable format back to a central station or master. RTU's typically connect to input and output channels. Input channels are equipped to handle metering information and sensing changes. Output channels are equipped for control or alarms. Continuous communication to an RTU is accomplished through an internally-controlled or externally-provided serial or network connection. Typical environments can also include dial-up connections where continuous monitoring is not required.

Programmable Logic Controllers (PLC's) / Intelligent Electronic Devices (IEDs) / Relays – Most electric utilities have separate Distributed Control Systems (DCS) and Relay Protection Systems for their power plants and substation control systems. In a substation environment PLC's and IED's are used to protect transformers and customer equipment when a specific undesirable event occurs on the transmission or distribution system. In power plants, this type of equipment is used to protect associated generating equipment from internal and external system failures.

Smart Meters – A type of advanced meter that identifies consumption in more detail than a conventional meter. Communication to this type of meter is typically accomplished using the internet, wireless networks, local power lines, or fiber back to the local utility provider.

Specialized communication hardware – Internally-controlled communication networks such as microwave, fiber optic, or RF-based technologies are the platforms utilized by the electrical sector to connect remote devices to central stations or masters. Examples can include routers, gateways, switches, access points, and modems.

D.3 EVIDENT AND SPECIFIC CYBER SECURITY PROBLEMS

This section documents specific cyber security problems in the smart grid, as much 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.

D.4 OPENNESS AND ACCESSIBILITY OF SMART GRID STANDARDS

Many standards relevant to the smart grid are published by organizations such as IEEE, ANSI, IEC, etc. While the standards published by these organizations are open, they are not nearly as freely accessible as the IETF standards that define the Internet and World Wide Web. Many of the smart grid standards must be purchased, and the cost for a single standard can range into thousands of dollars. In many cases the license accompanying a standard restricts its use to a single individual, and in some cases electronic copies of the standard are protected by Digital Rights Management technology that locks the copy to a specific computer (e.g. ANSI C12.22).

Designing algorithms and protocols that operate correctly and are free of undiscovered flaws is difficult at best. There is general agreement in the security community that openly published and time-tested algorithms and protocols are less likely to contain security flaws than secretly developed ones because their publication enables scrutiny by the entire community. The limited

accessibility of smart grid standards discourages inspection and review by parties without strong motivation and financial backing, and increases the risk that smart grid standards may contain security vulnerabilities.

D.5 AUTHENTICATING AND AUTHORIZING USERS TO SUBSTATION IEDS

The problem 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 (ie. 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 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 with the role in question, possibly including non-utility 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 seldom changed.

Users may be utility employees, contractors, or vendor support engineers. Roles may include audit (read-only), user (read-write), administrator (add/remove/modify users), and security officer (change security parameters).

The 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 or wired network connection, or possibly wireless. The device may also be accessed remotely over a low-speed (dialup) 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 RADIUS or LDAP over this connection is probably not desirable, however, 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.

D.6 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 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. Users may be utility employees, contractors, or vendor support engineers. Roles may include audit (read-only), user (read-write), administrator (add/remove/modify users), and security officer (change security parameters).
Access will usually be local via wired connections, or near-local via short-range radio, although some devices may support true remote access.

D.7 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 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 (ie. not shared between users), and control of authentication and authorization can be centrally managed and updated reasonably promptly to ensure only intended users can authenticate to intended devices and perform authorized functions.

Users may be utility employees, contractors, or vendor support engineers. Roles may include audit (read-only), user (read-write), administrator (add/remove/modify users), and security officer (change security parameters). Consumer roles and users are considered separately in section D.8.

Access may be local through the optical port of a meter, or remote through the AMI infrastructure, or remote through the HAN gateway.

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).

D.8 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.

D.9 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.

D.10 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 to 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 pre-provisioned 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 demand response signals. It should not be possible for a broad DOS attack to cause a large number of HAN devices to fail to authenticate and thereby not respond to a DR event.

D.11 SECURING SERIAL SCADA COMMUNICATIONS

Many substations still use slow serial links for SCADA communications with control centers. 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 clear text form. Solutions that simply wrap a serial link message into protocols like SSL or IPSEC over 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.

D.12 SECURING ENGINEERING DIALUP ACCESS

Dialup 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.

D.13 SECURE END-TO-END METER TO HEAD END COMMUNICATION

Secure end-to-end communications protocols such as TLS 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 Demand Response control services.

D.14 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 paradigm to occur 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 systems by attackers that might have subtle mis-configurations 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 power grid infrastructure.

D.15 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 correct version and un-tampered firmware with appropriate settings, and has *always* been running un-tampered firmware. Remote attestation is particularly important for meters given the easy physical accessibility of meters to attackers.

D.16 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 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 802.11i 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, primarily because of the distributed nature of the system itself. They also generally lack schemes for authorizing and providing integrity protection for adjacencies in the routing system. Without routing security, attacks such as eavesdropping, impersonation, man-in-the-middle, and denial-of-service could be easily mounted on AMI traffic.

D.17 KEY MANAGEMENT FOR METERS

Where meters contain cryptographic keys for authentication, encryption, or other cryptographic operations, a key management scheme must provide for adequate protection of cryptographic materials as well as sufficient key diversity. That is, a meter, collector, or other power system device should not be subject to a break-once break-everywhere scenario due to one shared secret being used across the entire infrastructure. Each device should have unique credentials and key material such that compromise of one device does not impact other deployed devices. The key management system must also support an appropriate lifecycle of periodic re-keying and revocation.

There are existing cases of large deployed meter bases using the same symmetric key across all meters, and even in different States. In order to share network services, adjacent utilities may even share and deploy that key information throughout both utility AMI networks. Compromising a meter in one network could compromise all meters and collectors in both networks.

D.18 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 deprive that ability to the utility, effectively denying service. 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.

D.19 OUTSOURCED WAN LINKS

Many utilities are leveraging existing communications infrastructure from telecommunications communications to support communication from pole-top collectors to the head end systems back at the plant. This is particularly true for AMI, but it may also apply to distribution and transmission automation projects. Due to the highly distributed nature of AMI, it is more likely that the WAN link will be over a relatively low bandwidth medium such as cellular band wireless (e.g., EVDO, GPRS) or radio networks like FlexNet. In either case, these networks were not built with AMI issues in mind, particularly security or reliability. 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 using a VPN connection, which is a bit pointless as users of the telecommunication company's AirCard are no more trustworthy than normal Internet users. Given the proliferation of botnets, it is not far-fetched to imagine enough wireless users to be compromised and launch a denial of service via a collector modem. Additionally, like the mesh wireless portion, cellular networks are subject to intentional and unintentional interference and congestion. It would be interesting to know whether meter reads would be reliable where large crowds are gathering and using their cell phones.

D.20 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 assure 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 assure 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(s) in a peer-to-peer mesh environment and isolate and contain any

subsequent attempts to penetrate other devices. This is important, as one must assume that if an attacker has the capability to reverse engineer a device that any inbuilt protections can eventually be compromised. It is an open and challenging problem to do intrusion detection in a peer-to-peer mesh environment.

D.21 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 analysis of various types of electromagnetic radiation emitted by a CPU, display, keyboard, etc. Tempest attacks are nearly impossible to detect. Syringe attacks use a syringe needle 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. For all side channel attacks, it is not necessary for an attacker to determine the entire key, but only enough of the key to facilitate 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.

D.22 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.

D.23 NON-SPECIFIC CYBER SECURITY ISSUES

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

D.24 KEY MANAGEMENT AND PKI

Key management for Smart Grid devices that contain symmetric or asymmetric long-lived keys is essential. Standard PKI is not appropriate since many devices will not have connectivity to key servers, certificate authorities, OCSP servers, etc. The scale of the systems involved and their distribution is unprecedented, as it will involve millions of devices. There will also be issues of cross-certification across different domains and checking for validity of certificates within the context of this unprecedented scale.

Some communications channels are slow enough that exchanging large certificates is impractical if it occurs too frequently. If the initial certificate exchange is not time critical and is used to establish a shared symmetric key(s) that is used for an extended period of time, as with IKE, certificate exchange can be practical over even slow channels. If the certificate exchange is time critical, protocols like IKE that exchange multiple messages before arriving at a preshared key may be too expensive even if the size of the certificate is minimal. Standard PKI is based on a peer-to-peer model where any peer may need to communicate with any other, but for much of the smart grid this is neither necessary nor desirable from a security standpoint. Many connections between smart grid devices will have much longer lifetimes (often permanent) than connections on the Internet. Dropping or refusing to re-establish connections due to key or certificate expiration is likely to cause problems. If one endpoint of a secure communication is determined by a third party to have been compromised, the third party must have a way of informing the other endpoint. This is true whether the key management is PKI or symmetric key based. In a multi-vendor environment it may be most practical to use PKI-based mechanisms to remove compromised devices. The commercial organizations that act as CAs for the Internet should probably not be CAs for the smart grid, or at least not all of them.

Because of the long operational lifetimes of many kinds of smart grid devices, special consideration has to be given to keys and ciphers used. For example symmetric ciphers maybe preferred over asymmetric ciphers for key protection and other operations because of lifetime and cipher strength matching. For example, in regards to key strength and matching for asymmetric and symmetric ciphers, NIST SP800-57 recommends that ECC with a 160-bit key is appropriate for use only through the year 2010, but notes that AES-128 is appropriate for data beyond 2030. Any key management system used in the Smart Grid will need to meet requirements that were unforeseen by existing standards and practices.

D.25 IT VS. SMART GRID SECURITY

The differences between IT, industrial, and Smart Grid security needed to be accentuated in any standard, guide, or roadmap document. NIST SP800-82 can be used as a basis but more needs to be addressed as control system security operates in an industrial campus environment and is not the same as something that has the scale, complexity, and distributed nature of the Smart Grid.

D.26 PATCH MANAGEMENT

Specific devices such as IEDs, PLCs, Smart Meters, etc. will be deployed in a variety of environments and critical systems. Their accessibility for software upgrades or patches maybe a complex activity to undertake because of how distributed and isolated equipment can be. Also there are many unforeseen consequences that 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 lifecycle 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 needs 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 where by the risk and impact of vulnerability can be determined in order to prioritize upgrades. Also a security infrastructure needs to be in place that can mitigate possible threats until the upgrade can be qualified and deployed so that the reliability of the system can be maintained.

D.27 AUTHENTICATION

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

D.28 TRUST MODEL

There has to be a clear idea of elements of the system are trusted and to what level and why. Practically speaking there will always be something you have to trust in the system. We must 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 it has a basis of less risk. However, even this statement has its own dependencies based on the design and management of that network that would inform the trust that is being vested in it.

D.29 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.

D.30 DISTRIBUTED VS. CENTRALIZED MODEL OF MANAGEMENT

There are unique issues of how to manage something as distributed as the Smart Grid and yet maintain good efficiency and reliability factors that imply centralization. Many systems are highly distributed, 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 a hybrid approach that is necessary for the Smart Grid.

D.31 LOCAL AUTONOMY OF OPERATION

Any security system must have local autonomy, as for example one cannot always assume 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 to be taken.

D.32 INTRUSION DETECTION FOR POWER EQUIPMENT

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

D.33 NETWORK AND SYSTEM MONITORING AND MANAGEMENT FOR POWER EQUIPMENT

Power equipment does not necessarily use common and open monitoring protocols and management systems. They are often a fusion of proprietary or legacy based protocols with their own security issues. There is a need for a common information model and protocol 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 must also be secure, as early lessons with 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.

D.34 SECURITY EVENT MANAGEMENT

Building on more advanced forms of IDS 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 needs to be clear methods of incident response to events that is 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.

D.35 CROSS-UTILITY / CROSS-CORPORATE SECURITY

Unfortunately many smart grid deployments are going forward with not much thought to what happens behind the head end systems for AMI as well as further on down the line for SCADA and other real-time control systems backing up 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 demand response control centers will handle integration with head end systems. Moreover, in many markets, the company that controls the head end to 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, 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 implement threshold controls, so someone can't disconnect hundreds of homes in a matter of a few seconds accidentally or maliciously.

D.36 TRUST MANAGEMENT

Trust Management systems such as KeyNote may be helpful in expressing and enforcing security policies where the distributed, decentralized, and intermittently connected nature of smart grid systems must be taken into account.

D.37 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.

D.38 PASSWORD MANAGEMENT

Passwords for authentication and authorization have many problems when used with highly distributed, decentralized, and variedly connected systems such as the smart grid. Where possible, passwords should be avoided, but some use of passwords will be – and already is – inevitable. Suitable password management schemes need to be developed that take into account both the nature of smart grid systems and of users.

D.39 CIPHER SUITE

A cipher suite needs to be identified that is open (e.g. standards based, mature, and preferably patent free) and reasonably secure for wide application in Smart Grid systems. For example we should consider which block ciphers (e.g. 3DES, AES) are appropriate in which modes (CBC, CTR, etc.) and key sizes. We should also have to give consideration to Asymmetric ciphers (e.g. ECC, RSA, etc.) that could form the basis for many authentication operations. The FIPS standards and particularly FIPS-140-2 are a guide, as well as the NSA Suite B algorithms. Device profile, data temporality/criticality/value should also play a role in cipher and key strength selection.

D.40 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.

Federated identity/authentication management systems may be appropriate here due to the variety of different kinds of authentication systems that will need to be integrated.

D.41 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 website address. In web systems this problem is solved by SSL certificates that include the DNS name of the server.

D.42 ENTROPY

Many devices do not have access to sufficient sources of entropy to serve as good sources of randomness for cryptographic key generation and other cryptographic operations. This is a fundamental issue and has impacts on the key management and provisioning system that must be designed and operated in this case.

D.43 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 must 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.

D.44 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.

D.45 LEGACY EQUIPMENT WITH LIMITED RESOURCES

The lifecycle of equipment in the electricity sector typically extends beyond 20 years. Compared to IT systems, which typically see 3-5 year lifecycles, 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 is 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.

D.46 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 the cost versus the benefit of the security measure in the

risk mitigation and decision process can sometimes be prohibitive for the deployment if the cost outweighs the benefits of the deployment of the 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 lack of centralized and remote patch/firmware management solutions contribute 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. The extensive regression testing is extremely important to ensure that an upgrade to a device won't negatively impact reliability, but 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.

D.47 NON-FIPS APPROVED ENCRYPTION MODES

In general only approved FIPS modes of encryption should be used in any system. The unique requirements that some parts of the Smart Grid place on communications protocols can drive a genuine need for non-standard encryption modes or ciphers that have received less public scrutiny than FIPS-approved modes. Examples are PE Mode as used in IEEE P1711 and EAX as used in ANSI C12.22. There are open questions to address for non-approved modes. How can we ensure that sufficient attention is given to these cryptographic modes? Is this the right question to ask? Do we also need to look at IEEE 802.16.e (PHY/MAC), PKMv2, IETF EAP/TLS, IETF COPS-PR/TLS, and if so in what way?

Regardless of the unapproved mode, the case must be made for its use along the lines of resource constraints, unique nature of an application, or new security capabilities that approved modes cannot address. At minimum a non-FIPS mode should be open and published to a community of cryptographers for review and comment for a reasonable amount of time before being used.

D.48 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 data may get relayed back to data historians and/or maintenance management systems. Furthermore, as a matter of business policy, when faced with potential cyber security threats, electric utilities prioritize their obligation to maintain electric service over the requirements of 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 means 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 and the tools provided to maintain chain of custody, reduce the risk of spoliation, and ensure that its origin can be properly authenticated. Tools should be capable of retrieving data from meters, collectors, 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.

D.49 ROLES AND ROLE BASED ACCESS CONTROL

What roles are appropriate for RBAC in different Smart Grid environments?

Are the following roles appropriate and sufficient?

1. Auditors: users with the ability to only read/verify the state of the devices (this may include remote attestation).
2. Users: typical users whose API involves reading and writing data to the devices (but management access is restricted)
3. Administrators: users who can add, remove or modify the rights of other users
4. Security officers: users who are able to change the security parameters of the device (e.g. update firmware)

D.50 LIMITED SHARING OF VULNERABILITY AND/OR INCIDENT INFORMATION

There is a significant reticence to sharing information about vulnerabilities or incidents in any critical infrastructure industry. This is based on many sound reasons. The least of which is the fact 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 3rd party be it government or private institution.

D.51 DATA FLOW CONTROL VULNERABILITY ISSUE

The grid will encompass many networks and sub-networks 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 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.

D.52 PUBLIC VS. PRIVATE NETWORK USE

There is on-going debate in the industry over the use of public network infrastructure such as the Internet, leased lines, or public WiMax networks telecommunication companies might provide. A public network is not be confused with the use of the Internet Protocol (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 cyber security 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), this carries significantly more risk of intrusion, disruption, tampering, and general reliability regardless of countermeasure. This is by

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 facts should be self evident 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, is 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)
- Identifying countermeasure systems (e.g. firewalls, IDS/IPS, SEM, Encrypted links & 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.

D.53 TRAFFIC ANALYSIS

Traffic Analysis is the examination of characteristics of encrypted communications to glean information. 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
- 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 FERC 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.

D.54 POOR SOFTWARE ENGINEERING PRACTICES

The meter worm reported on by IOActive appears to exploit a buffer overflow. According to IOActive, "one deficiency common among many of the meters is the use of insecure programming functions, such as memcpy() and strcpy(), which are two of the most common sources of exploitable software bugs". Thus it appears that meter software is likely to suffer many of the same software engineering problems as other software.

D.55 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.

One common problem that is sometimes wrongly ascribed to the security system is failure of an RJ-45 connector. Standard RJ-45 connectors as commonly used for Ethernet are not particularly good for industrial environments. Dust can contaminate connections. Moisture and water can corrode connections. Vibration tends to wear the gold plating off connection pins. There are many proprietary solutions in the form of seals that can be used with standard RJ-45 connectors and alternative types of connectors. Are there any that are or could be standardized?

APPENDIX E

MEMBERSHIP LISTS

E.1 THE CYBER SECURITY COORDINATION TASK GROUP AND WORKING GROUP MEMBERS

	Name	Organization
1.	Alrich, Tom	ENCARI
2.	Anderson, Dwight	Schweitzer Engineering Labs
3.	Ascough, Jessica	Harris
4.	Bacik, Sandy	Conservation Solutions
5.	Barclay, Steve	
6.	Barnett, Bruce	GE Global Research
7.	Bass, Len	Software Engineering Institute Carnegie Mellon University
8.	Batz, David	Edison Electric Institute
9.	Bell, Ray	Grid Net
10.	Bell, Will	Grid Net
11.	Bender, Klaus	Utilities Telecom Council
12.	Benn, Jason	Hawaiian Electric Company
13.	Berkowitz, Don	S&C Electric Company
14.	Beroset, Ed	Elster Group
15.	Berrett, Dan E.	DHS Standards Awareness Team (SAT)
16.	Berrey, Adam	General Catalyst Partners
17.	Biggs, Doug	Infogard
18.	Biggs, Les	Infogard
19.	Bochman, Andy	
20.	Braendle, Markus	ABB
21.	Brown, Bobby	EnerNex Corporation
22.	Brown, Kevin	EnerNex Corporation
23.	Bucciero, Joe	Buccerio Consulting
24.	Campagna, Matt	Certicom Corp.
25.	Cam-Winget, Nancy	Cisco Systems, Inc.
26.	Carpenter, Matthew	Inguardians
27.	Chasko, Stephen	Landis+Gyr
28.	Chow, Edward	U of Colorado at Colorado Springs
29.	Cioni, Mark V.	MV Cioni Associates, Inc.
30.	Clements, Samuel	Pacific Northwest National Laboratory
31.	Cleveland, Frances	Xanthus Consulting International
32.	Coop, Mike	heyCoop, LLC
33.	Cornish, Kevin	Enspiria

	Name	Organization
34.	Cortes, Sarah	Inman TechnologyIT
35.	Cosio, George	Florida Power and Light
36.	Cragie, Robert	Jennic LTD
37.	Crane, Melissa	Tennessee Valley Authority
38.	Cui, Stephen	Microchip Technology
39.	Dagle, Jeff	Pacific Northwest National Laboratory
40.	Dalva, Dave	Cisco Systems, Inc.
41.	De Petrillo, Nick	Industrial Defender
42.	Dion, Thomas	DHS
43.	Dodson, Greg	Dominion Resources Services, Inc.
44.	Drummond, Rik	Drummond Group
45.	Dutta, Prosenjit	Utilities AMI Practice
46.	Eggers, Matthew	U.S. Chamber of Commerce
47.	Emelko, Glenn	ESCO
48.	Engels, Mark	Dominion Resources Services, Inc.
49.	Ennis, Greg	Wi-Fi Alliance
50.	Estefania, Maria	
51.	Eswarahally, Shrinath	
52.	Ewing, Chris	Schweitzer Engineering Labs
53.	Faith, Nathan	American Electric Power
54.	Fennell, Kevin	Landis+Gyr
55.	Franz, Matthew	SAIC
56.	Fredebeil, Karlton	Tennessee Valley Authority
57.	Freund, Mark	PGE
58.	Gailey, Mike	CSC
59.	Gerber, Josh	San Diego Gas and Electric
60.	Gerbino, Nick	Dominion Resources Services, Inc.
61.	Gering, Kip	Itron
62.	Ghansahi, Isaac	California State University Sacramento
63.	Gillmore, Matt	CMS Energy
64.	Goff, Ed	Progress Energy
65.	Gooding, Jeff	Southern California Edison
66.	Goodson, Paul	ISA
67.	Greenberg, Alan M.	Boeing
68.	Greenfield, Neil	American Electric Power, Inc.
69.	Greer, David	University of Tulsa
70.	Gulick, Jessica	SAIC
71.	Gunter, Carl	U. of Illinois
72.	Gussin, L.D.	Clean-motive Strategies
73.	Halbgewachs, Ronald D.	Sandia National Laboratories
74.	Hambrick, Gene	Carnegie Mellon University

	Name	Organization
75.	Hammond, Virgil	Argonne National Laboratory
76.	He, Donya	BAE Systems
77.	Herold, Rebecca	Privacy Professor Rebecca Herold & Associates, LLC
78.	Heron, George L.	BlueFin Security
79.	Hertzog, Christine	Smart Grid Library
80.	Highfill, Darren	SCE
81.	Hilber, Del	Constellation Energy
82.	Houseman, Doug	Capgemini Consulting
83.	Huber, Robert	Critical Intelligence
84.	Hughes, Joe	EPRI
85.	Hussey, Laura	Schweitzer Engineering Laboratories, Inc.
86.	Ibrahim, Erfan	EPRI
87.	Iga, Yoichi	NEC Electronics Corp.
88.	Ivers, James	SEI
89.	Jin, Chunlian	Pacific Northwest National Laboratory
90.	Johnson, Freemon	NIST
91.	Jones, Barry	Sempra
92.	Jones, Ernie	Charon Consulting
93.	Kahl, Steve	North Dakota
94.	Kanda, Mitsuru	Toshiba
95.	Kellogg, Shannon	EMC
96.	Kenchington, Henry	DOE
97.	Kerber, Jennifer	TechAmerica
98.	Khurana, Himanshu	University of Illinois
99.	Kim, Jin	Risk Management Consulting, CRA International
100.	Kimura, Randy	General Electric
101.	Klein, Stanley A.	Open Secure Energy Control Systems, LLC
102.	Klerer, Mark	
103.	Koliwad, Aja	General Electric
104.	Kotting, Chris	Public Utilities Commission of Ohio
105.	Kube, Nate	Wurldtech
106.	Kuruganti, Phani Teja	EMC2
107.	LaMarre, Mike	Austin Energy ITT
108.	Lauriat, Nicholas A.	Network and Security Technologies
109.	Lawson, Barry	NRECA
110.	Levinson, Alex	Lockheed Martin Information Systems and Global Solutions
111.	Lilley, John	Sempra
112.	Lima, Claudio	Sonoma Innovation
113.	Lipson, Howard	CERT, Software Engineering Institute

	Name	Organization
114.	Maciel, Greg	Uniloc USA
115.	Magda, Wally	Industrial Defender
116.	Manjrekar, Madhav	Siemens
117.	Manwani, Leena	GridNet Inc
118.	Martinez, Catherine	DTE Energy
119.	Martinez, Ralph	BAE Systems
120.	McBride, Sean	Critical Intelligence
121.	McComber, Robert	Telvent
122.	McDonald, Jeremy	Southern California Edison
123.	McGinnis, Douglas	IT Utility Solutions
124.	McGurk, Sean	DHS
125.	McQuade, Rae	NAESB
126.	Melton, Ron	Pacific Northwest National Laboratory
127.	Mertz, Michael	Southern California Edison
128.	Metke, Anthony	Motorola
129.	Mirza, Wasi	Motorola
130.	Molina, Jesus	Fujitsu Ltd.
131.	Molitor, Paul	NEMA
132.	Mollenkopf, Jim	CURRENT Group
133.	Mulberry, Karen	Neustar
134.	Nahas, John	ICF International
135.	Navid, Nivad	Midwest ISO
136.	Noel, Paul	ASI
137.	Norton, Dave	Entergy
138.	Nutaro, James J.	Southern California Edison
139.	O'Neill, Ivan	Southern California Edison
140.	Okunami, Peter M.	Hawaiian Electric Company, Inc.
141.	Old, Robert	Siemens Building Technologies, Inc.
142.	Overman, Thomas M.	Boeing
143.	Pace, James	Silver Spring Networks
144.	Papa, Mauricio	University of Tulsa
145.	Patel, Chris	EMC Technology Alliances
146.	Pearce, Thomas C. II	Public Utilities Commission of Ohio
147.	Peters, Mike	FERC
148.	Pyles, Ward	Southern Company
149.	Qin, Jason	Skywise Systems
150.	Radgowski, John	Dominion Resources Services, Inc
151.	Ragsdale, Gary L.	Southwest Research Institute
152.	Rakaczky, Ernest A.	Invensys Global Development
153.	Ray, Indrakshi	
154.	Reddi, Ramesh	Intell Energy

	Name	Organization
155.	Revill, David	Georgia Transmission Corp.
156.	Roberts, Don	Southern Company Transmission
157.	Roberts, Jeremy	LonMark International
158.	Robinson, Charley	International Society of Automation
159.	Robinson, Eric	ITRON
160.	Rodriguez, Gene	IBM
161.	Rutfield, Craig	NTRU Cryptosystems, Inc.
162.	Rutkowski, Tony	Yaana Technologies
163.	Saint, Bob	National Rural Electric Cooperative Association
164.	Sconzo, Mike	Electric Reliability Council of Texas
165.	Searle, Justin	InGuardians
166.	Shaw, Vishant	Enernex
167.	Shein, Robert	EDS
168.	Shetty, Ram	General Electric
169.	Shin, Mark	Senior Security Engineer, CISSP
170.	Shpantzer, Gal	
171.	Silverstone, Ariel	
172.	Singer, Bryan	Kenexis
173.	Skare, Paul	Siemens
174.	Smith, Brian	EnerNex
175.	Smith, Rhett	Schweitzer Engineering Labs
176.	Smith, Ron	ESCO Technologies Inc.
177.	Sood, Kapil	Intel Labs
178.	Sorebo, Gilbert	SAIC
179.	Stammberger, Kurt	Mocana
180.	Starr, Christopher H.	General Dynamics Advanced Information Systems
181.	Stevens, James	Software Engineering Institute
182.	Stitzel, Jon	
183.	StJohns, Michael	
184.	Stouffer, Keith	NIST
185.	Struthers, Brent	NeuStar
186.	Suchman, Bonnie	Troutman Sanders LLP
187.	Sullivan, Kevin	Microsoft
188.	Sung, Lee	Fujitsu
189.	Sushilendra, Madhava	EPRI
190.	Tallent, Michael	Tennessee Valley Authority
191.	Thanos, Daniel	General Electric
192.	Thompson, Daryl L.	Thompson Network Consulting
193.	Thomson, Matt	General Electric
194.	Tiffany, Eric	Liberty Alliance

	Name	Organization
195.	Toecker, Michael	Burns & McDonnell
196.	Truskowski, Mike	Cisco
197.	Uhrig, Rick	Electrosoft
198.	Veltsos, Christophe	Minnesota State University
199.	Vettoretti, Paul	SBC Global
200.	Wacks, Ken	MIT
201.	Walters, Ryan	TerraWi Communications
202.	Weiss, Joe	
203.	Wepman, Joshua	SAIC Commercial Business Services
204.	West, Andrew C	Invensys Process Systems
205.	Weyer, John A.	John A. Weyer and Associates
206.	White, Jim	Uniloc USA, Inc.
207.	Whyte, William	
208.	Williams, Terron	Elster Electricity
209.	Wingo, Harry	Google
210.	Wolf, Dana	RSA
211.	Worden, Michael	
212.	Wright, Andrew	N-Dimension Solutions
213.	Yardley, Tim	University of Illinois
214.	Yoo, Kevin	Wurldtech

E.2 THE ADVANCED SECURITY ACCELERATION PROJECT – SMART GRID

Bobby Brown
Kevin Brown
Matthew Carpenter
Darren Highfill
James Ivers
James Stevens
Len Bass
Teja Kuruganti
Howard Lipson
Jim Nutaro
Justin Searle
Vishant Shah
Brian Smith

APPPENDIX F

ACRONYMS

ACRONYMS	
AMI	Advanced Metering Infrastructure
ASAP-SG	Advanced Security Acceleration Project-Smart Grid
B2B	Business to Business
BAN	Business Area Network
DER	Distributed Energy Sources
DMS	Distribution Management System
DNP	Distributed Network Protocol
DOMA	Distribution Operations Model and Analysis
DR	Demand Response
EMS	Energy Management System
ES	Electric Storage
ESI	Energy Services Interface
ET	Electric Transportation
EUMD	End Use Measurement Device
EVSE	Electric Vehicle Service Element
FLIR	Fault Location, Isolation, Restoration
GAPP	Generally Accepted Principles
GIS	Geographic Information System
GRPS	General Packet Radio Service
HAN	Home Area Network
HMI	Human-Machine Interface
I2G	Industry to Grid
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
ISO	Independent System Operator
LAN	Local Area Network
LMS/DRMS	Load Management System/ Distribution Resource Management System
MDMS	Meter Data Management System
MFR	Multi-Feeder Reconnection
OMS	Outage Management System
PEV	Plug-In Electric Vehicle
PI	Process Information

RTO	Regional Transmission Operator
RTO/ISO	Regional Transmission Operator/Independent System Operator
SCATA	Supervisory Control and Data Acquisition
VVWS	Volt-Var-Watt
WAMS	Wide-Area Measurement System
WAN	Wide Area Network
WASA	Wide Area Situational Awareness
WLAN	Wireless Local Area Network
WMS	Work Management System