UCAIUG: AMI-SEC-ASAP

AMI System Security Requirements

V1.01

ASAP

12/17/2008

Executive Summary

This document provides the utility industry and vendors with a set of security requirements for Advanced Metering Infrastructure (AMI). These requirements are intended to be used in the procurement process, and represent a superset of requirements gathered from current cross-industry accepted security standards and best practice guidance documents.

This document provides substantial supporting information for the use of these requirements including scope, context, constraints, objectives, user characteristics, assumptions, and dependencies. This document also introduces the concept of requirements for security states and modes, with requirements delineated for security states.

These requirements are categorized into three areas: 1) Primary Security Services, 2) Supporting Security Services and 3) Assurance Services. The requirements will change over time corresponding with current security threats and countermeasures they represent. The AMI-SEC Task Force presents the current set as a benchmark, and the authors expect utilities and vendors to tailor the set to individual environments and deployments.

While these requirements are capable of standing on their own, this document is intended to be used in conjunction with other 2008 deliverables from the AMI-SEC Task Force, specifically the Risk Assessment, the Architectural Description, the Component Catalog (in development as of this writing), and the Implementation Guide (to be developed late 2008). This document also discusses the overall process for usage of this suite.

Acknowledgements

The AMI-SEC Task Force would like to acknowledge the work of the primary authors, contributing authors, editors, reviewers, and supporting organizations. Specifically, the Task Force would like to thank:

- The AMI Security Acceleration Project (ASAP)
  - The Architectural Team including resources from Consumers Energy, EnerNex Corporation, InGuardians, The Software Engineering Institute at Carnegie Mellon University, and Southern California Edison
  - Supporting organizations including The Electric Power Research Institute and The United States Department of Energy
  - Participating utilities, including American Electric Power, Austin Energy, BC Hydro, Consumers Energy, Duke Energy, Kansas City Power & Light, Oncor, Pacific Gas & Electric, San Diego Gas & Electric, Southern California Edison
- The utilities, vendors, consultants, national laboratories, higher education institutions, governmental entities, and other organizations that have actively contributed to and participated in the activities of the AMI-SEC Task Force

The AMI-SEC Task Force would also like to thank the Department of Homeland Security Cyber Security Division, National Institute of Standards and Technology Computer Security Division, North American Reliability Corporation and The Common Criteria for the works that they have produced that served as reference material for the AMI Systems Security Requirements document.

Authors

Bobby Brown
Brad Singletary
Bradford Willke
Coalton Bennett
Darren Highfill
Doug Houseman
Frances Cleveland
Howard Lipson
James Ivers
Jeff Gooding
Jeremy McDonald
Neil Greenfield
Sharon Li

Table of Contents

Table of Figures

1. Introduction

As a key element in the evolution of the Smart Grid, the Advanced Metering Infrastructure (AMI) is the convergence of the power grid, the communications infrastructure, and the supporting information infrastructure. AMI security must exist in the real world with many interested parties and overlapping responsibilities. This document focuses on the security services that are important to secure the power grid, communications infrastructure and supporting information infrastructure.

1.1 Purpose

The purpose of the AMI Security Specification is to provide the utility industry along with supporting vendor communities and other stakeholders a set of security requirements that should be applied to AMI implementations to ensure the high level of information assurance, availability and security necessary to maintain a reliable system and consumer confidence. While this specification focuses on AMI, the security requirements contained in the document may be extended to other network-centric, Smart Grid solutions.

1.1.1 Strategic Importance

Utility companies of the future will deliver energy and information to customers through a "smart" energy supply chain created by the convergence of electric, communication and information technologies that are highly automated for responding to the changing environment, electricity demands and customer needs. The building blocks of this Smart Grid include AMI, advanced transmission and distribution automation, distributed generation, electric vehicle refueling infrastructure and renewable energy generation projects of today.

The emergence of this new class of Smart Grid systems holds tremendous promise and requires innovation and deployment of new technologies, processes and policies. Composed of many independent systems, the Smart Grid will evolve by integrating existing islands of automation to achieve value through the delivery of information to customers, grid operators, utility companies and other stakeholders. A reliable and secure Smart Grid holds the promise of enabling automated demand response, providing customers a myriad of options to manage their energy costs through technology enabled programs along with limiting outages with a self-healing resilient transmission and distribution network and other strategically important functions.

The challenge of providing both a reliable and secure AMI solution lies in the diversity of technologies, processes and approaches used to realize this vision. Managing change rising from the complexity of diverse solutions with an effective and efficient systems integration process will enable the AMI system. This requires a commitment to standards, best practices and a high degree of architectural discipline. This document specifies platform independent security requirements, services and guidance required to implement secure, resilient AMI solutions.

1.1.2 Problem Domain

As the utility industry's capabilities increase to serve the needs of a rapidly growing information society, the breadth and sophistication of the threat environment these Smart Grid solutions operate in also increases. By bridging heterogeneous networks capable of exchanging information seamlessly across the AMI older proprietary and often manual methods of securing utility services will disappear as each is replaced by more open, automated and networked solutions. The benefits of this increased connectivity depends upon robust security services and implementations that are necessary to minimize disruption of vital services and provide increased reliability, manageability and survivability of the electric grid.

Recognizing the unique challenges of AMI enabled Smart Grid solutions is imperative to deploying a secure and reliable solution. Unique characteristics of AMI implementations that set them apart from other utility project include the following:

- AMI touches every consumer
- AMI is a command and control system
- AMI has millions of nodes
- AMI touches almost every enterprise system
- Many current AMI solutions are narrowband solutions

These network-centric characteristics, coupled with a lack of a composite set of cross industry AMI security requirements and implementation guidance, is the primary motivation for the development of this document. The problem domains needing to be addressed within AMI implementations are relatively new to the utility industry, however there is precedence for implementing large scale, network-centric solutions with high information assurance requirements. The defense, cable and telecommunication industries offer a number of examples of requirements, standards and best practices directly applicable to AMI implementations.

The challenge is to secure AMI in a holistic manner, noting that such an approach requires the buy-in of many stakeholders. Stakeholders can be viewed in three groups:

- Stakeholders within the enterprise who have an interest in generating value from technology investments:
    - Those who make investment decisions
    - Those who decide about requirements
    - Those who use technology services
- Internal and external stakeholders who provide technology services:
    - Those who manage the technology organization and processes
    - Those who develop capabilities
    - Those who operate the services
- Internal and external stakeholders who have a control/risk responsibility:
    - Those with security, privacy and/or risk responsibilities
    - Those performing compliance functions
    - Those requiring or providing assurance services

To meet the requirements of the stakeholder community, a security framework for AMI technology governance and control should:

- Provide a business focus to enable alignment between business and technology objectives
- Establish a process orientation to define the scope and extent of coverage, with a defined structure enabling easy navigation of content
- Be generally acceptable by being consistent with accepted technology good practices and standards and independent of specific technologies

- Supply a common language with a set of terms and definitions that are generally understandable by all stakeholders
- Help meet regulatory requirements by being consistent with generally accepted corporate governance standards (e.g., Committee of Sponsoring Organizations of the Treadway Commission) and technology controls expected by regulators and external auditors.

As such, this document provides security requirements for the purposes of procurement, design input, validation and certification. It is not the intent of this document to describe AMI architecture. The satisfaction of requirements identified in this document implies a need for coherent architecture, policies, procedures, etc… none of which is prescribed in this document.

AMI security involves a system of systems approach in design and operations, and therefore security responsibility must extend to stakeholders and parties outside and in addition to the electric utility. While security requirements for the broader AMI may or may not be within the scope of a single utility's responsibility, imposing the requirements upon cooperating interconnecting systems and the corresponding capabilities will meet or support some aspects of AMI security objectives. Moreover, interdependencies among the power grid, the communications infrastructure, and the information infrastructure pose a particularly serious challenge to the design of a secure and survivable AMI.

1.1.3 Intended Audience

The intended audience for this document includes utility companies seeking AMI implementation and policy guidance; vendors seeking product design requirements and input; policy makers seeking to understand the requirements of reliable and secure AMI solutions; and any reader who wishes to find information related to AMI security requirements. While this document is intended for use by security professionals, solution architects and product designers, much of the document is written for a broader audience seeking to understand AMI security challenges, requirements and potential solutions. Lastly, this specification may provide a foundation for security requirements in the procurement and implementation of AMI solutions.

This document is intended to be a living specification to be updated as the industry evolves, with a focus on AMI security functionality. As such, one of the benefits of this document is to create a baseline document for the utility industry that provides AMI security requirements and identifies gaps between current requirements and capabilities available in the market. Ideally, the AMI security specification will be referenced and reused throughout the utility industry, providing a common set of semantics for enabling the development and implementation of robust, reliable AMI solutions.

1.1. Scope

AMI Security is simply defined as those means and measures concerned with securing an AMI system. For the purpose of this document, the definition of AMI is:

> *The communications hardware and software and associated system and data management software that creates a network between advanced meters and utility business systems and which allows collection and distribution of information to customers and other parties such as competitive retail providers, in addition to*

> *providing it to the utility itself. AMI is further defined as: 1) The hardware and software residing in, on, or closest to the customer premise for which the utility or its legal proxies are primarily responsible for proper operation; and 2) The hardware and software owned and operated by the utility or its legal proxies which has as its primary purpose the facilitation of Advanced Metering.*

This document presents security requirements for AMI systems. This document does not address business functional or other non-security related requirements.

A further understanding of the scope requires an understanding of the utility business systems and associated functionality. Section 2.1 of this document discusses Utility Business Systems and services. In general, this specification is a tool that can be applied broadly as defined above and to peripheral systems using AMI communication services. Each individual utility should decide the boundary distinction. The boundary definition and document applicability includes system security maturity of the associated connecting system, organizational responsibility and procurement scope.

The AMI-SEC Task Force considered HAN use cases in the development of this document and it is reasonable to assume utility edge application requirements can be applied to HAN applications (e.g., requirements applied to utility applications can also be applied to consumer applications). Imposing requirements on the HAN requires additional considerations associated with control and ownership that are outside the scope of this document.

1.2. Document Overview

This section describes how this document relates to the Architectural Description, Risk Assessment, Component Catalog and Implementation Guide.

The path that a particular utility follows through these documents (Risk Assessment, System Security Requirements, Architectural Description, Component Catalog and Implementation Guide) depends upon the level of resources the utility chooses to put toward the effort. In the drawing below, this level of resources tracks the “Entry Points” on the right side of the drawing. For the descriptions below (Figure 1), the utility will define Architectural Elements, i.e., hardware and software.

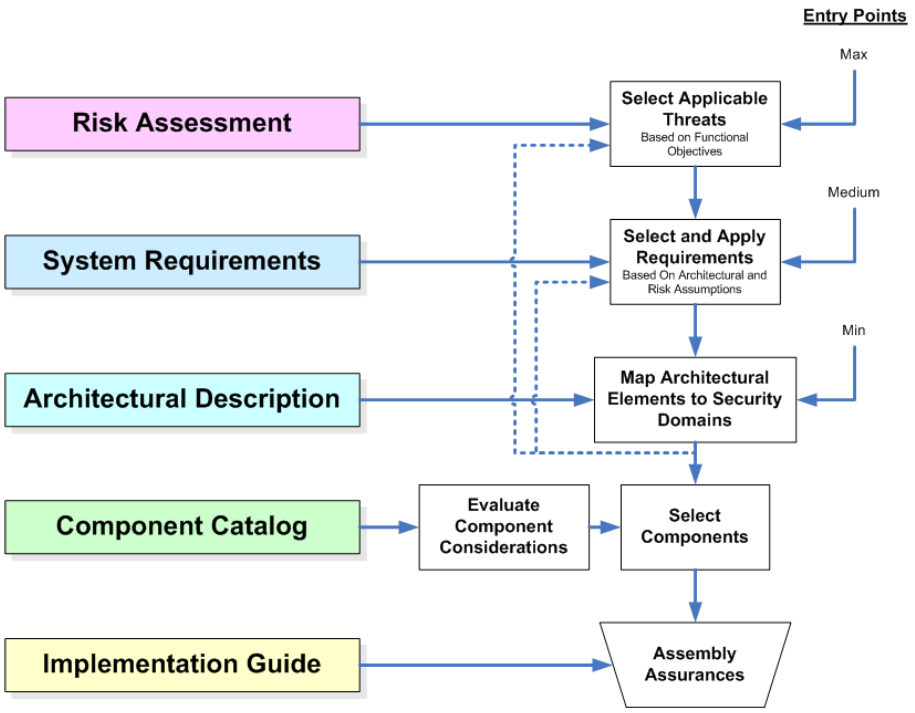
Entry Points
Max
Medium
Min
Risk Assessment
System Requirements
Architectural Description
Component Catalog
Implementation Guide
Select Applicable Threats
Based on Functional Objectives
Select and Apply Requirements
Based On Architectural and Risk Assumptions
Map Architectural Elements to Security Domains
Evaluate Component Considerations
Select Components
Assembly Assurances

Figure 1 – Deliverables Process Flow

Maximum Level of Resources. For a utility with the ability to apply the maximum level of resources, the process to take is the following:

Step 1 The utility will tailor the AMI-SEC Risk Assessment to their particular environment, constraints, and risk acceptance limits.

Step 2 The utility selects which requirements apply to their potential solution architecture by combing through the AMI-SEC System Security Requirements document and assigning priority to the requirements they need in order to adequately mitigate risks.

Step 3 The utility maps the significant Architectural Elements of potential solutions against the defined Security Domains and places selected and prioritized requirements on Architectural Elements according to the elements' placement within the Security Domains.

Medium Level of Resources. For a utility with a moderate ("medium") level of resources, the process to undertake is the following:

Step 1 The utility will review the System Security Requirements document and select which requirements apply to their potential solution architecture.

Step 2 The utility maps the significant Architectural Elements of potential solutions against the defined Security Domains.

Step 3 The utility accepts the AMI-SEC Risk Assessment without any modification or customization, but bears the responsibility for combing through the AMI-SEC System Security Requirements document

Step 4 The utility assigns priority to the requirements they need to adequately mitigate risks.

Step 5 Once the utility has selected and prioritized requirements, the requirements are placed on Architectural Elements according to the elements' placement within the Security Domains.

Minimum Level of Resources. For a utility looking to utilize the minimal level of resources, the process to undertake is the following:

Step 1 The utility will review the Architectural Description document and map the significant Architectural Elements of potential solutions against the defined Security Domains.

Step 2 The utility accepts the AMI-SEC Risk Assessment without any modification or customization.

Step 3 The utility accepts the AMI-SEC System Security Requirements as a whole without selecting any particular subset as applicable to their environment.

Step 4 Requirements are placed on Architectural Elements according to the elements' placement within the Security Domains. In this scenario, the utility pushes the entire set of requirements on to the vendor. The onus lies with the vendor to push back and indicate where requirements are applicable and where they are not.

1.3. Definitions, acronyms, and abbreviations

Rather than produce an exhaustive list of AMI and security terms, links have been provided to well known, extensively used definitions, acronyms and abbreviations. Other terminology is addressed as encountered throughout this document.

Resource	Location
SmartGridipedia	http://www.smartgridipedia.org
NIST IR 7298 - Glossary of Key Information Security Terms	http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf
International Electrotechnical Commission 62351-2 Security Terms	http://std.iec.ch/terms/terms.nsf/ByPub?OpenView&Count=-1&RestrictToCategory=IEC%2062351-2
Electropedia	http://www.electropedia.org/

Table 1 - Terminology References

1.4. References

Advanced Metering Infrastructure (AMI) Program – AMI Use Case (Draft). 2006. Southern California Edison. Retrieved from http://www.sce.com/PowerandEnvironment/smartconnect/open-innovation/usecasechart.htm

Clements, P.; Bachmann, F.; Bass, L.; Garlan, D.; Ivers, J.; Little, R.; Nord, R.; & Stafford, J. *Documenting Software Architectures: Views and Beyond*. 2002. Boston, MA: Addison-Wesley.

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/

Federal Information Processing Standard (FIPS) 140-2. 2004, March 24. National Institute of Standards and Technology Information Technology Library – Computer Security Division – Computer Security Resource Center Cryptographic Module Validation Program (CMVP). Retrieved from http://csrc.nist.gov/groups/STM/cmvp/

Houseman, Doug and Frances Cleveland. 2008. Scope of Security Requirements for Business Processes. Retrieved from http://osgug.ucaiug.org/utilisec/amisec/Reference%20Material/Forms/AllItems.aspx

IEEE Standard 1471-2000. 2000. IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, by IEEE Computer Society.

National Institute of Standards and Technology. 2007, December. NIST SP 800-53 Rev. 2 - Recommended Security Controls for Federal Information Systems. NIST Information Technology Library – Computer Security Division – Computer Security Resource Center Special Publications. Retrieved from http://csrc.nist.gov/publications/PubsSPs.html

National Institute of Standards and Technology. 2007, September 28. NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security (2nd DRAFT). NIST Information Technology Library – Computer Security Division – Computer Security Resource Center Special Publications (SP). Retrieved from http://csrc.nist.gov/publications/PubsSPs.html

North American Electric Reliability Corporation. 2006, June 1. NERC Critical Infrastructure Protection (CIP). Retrieved from http://www.nerc.com/page.php?cid=2|20

The Common Criteria. 2007, September. Common Criteria v3.1 – Part 2: Security Functional Requirements Release 2. The Common Criteria. Retrieved from http://www.commoncriteriaportal.org/thecc.html

The Common Criteria. 2007, September. Common Criteria v3.1 – Part 3: Security Assurance Requirements Release 2. The Common Criteria. Retrieved from http://www.commoncriteriaportal.org/thecc.html

2. General system description

2.1. Use Cases

AMI Use Cases have been organized into five different categories consistent with the primary value streams they support. These five categories/value streams are:

- Billing

- Customer
- Distribution System
- Installation
- System

Reference 2.A - Business Functions as Stakeholders in AMI Systems provides additional extensions to the use cases presented here, as well as describing business functions and scenarios.

2.1.1. Billing

There are four primary use cases in the Billing category.

1. Multiple Clients Read Demand and Energy Data Automatically from Customer Premises
2. Utility remotely limits usage and/or connects and disconnects customer
3. Utility detects tampering or theft at customer site
4. Contract Meter Reading (or Meter Reading for other Utilities)

1 and 4 are directly related to the electronic capture and processing of time-based energy and demand data from customer meters to support the core Billing process of the electric utility (1) or, on a contract basis, for a gas or water utility (4) . The other Billing Use Cases explore other functionality that can be leveraged from having installed AMI meters in the field. Use case 2 explores utilization of the remote connect/disconnect functionality of AMI meters. Use case 3 considers how AMI meters and the data they capture can be leveraged to support the detection of energy theft.

Business value in the Billing area is created in several different ways. By automating the collection of time-based energy usage and demand, the utility is able to significantly transform the process for collecting energy and demand information to support the billing process. The traditional process for collecting meter data (manually recording meter dial settings on a monthly basis) is replaced by a fully automated, electronic capture process. Because the energy data is captured in intervals of time (typically 15 minute intervals), AMI systems enable time-based rates. Time-based billing rates vary throughout the day, reflecting changes in the balance between energy supply and demand. Although the primary implementers of AMI have been electric utilities, the potential exists for the infrastructure to be leveraged to capture gas and water meter data as well – either for the host utility if they deliver those commodities or for another utility (on a contract basis).

Other business value accrues from functionality that the AMI meters can provide. AMI meters typically are outfitted with remote connect and remote disconnect capability. This allows the utility to initiate or terminate service remotely, without having to send a field technician. This functionality supports the routine Move-In/Move-Out processes as well as the credit/collections processes. Disconnects for non-payment (and subsequent reconnects) can be accomplished remotely rather than requiring on on-site presence. AMI meters also come with functionality that can help utilities identify potential meter tampering or energy theft/diversion.

Finally, AMI provides a wealth of data that various entities within the utility to use to create additional business value. These areas include the following:

- Distribution system design – granular data on actual customer energy usage can be utilized for more optimal design of distribution system components
- Distribution planning – the utility has a wealth of usage and demand data by circuit that can be analyzed to better target investments in new distribution facilities to meet growth in demand
- Distribution operations and maintenance – the Distribution organization has a wealth of data for improved state estimation, contingency planning, and asset management
- Marketing – AMI data can be analyzed to develop energy services/products to meet customer needs

The following table summarizes the major business processes supported by the Billing Use Cases and the key areas of business value that they enable.

Use Case 1: Auto-Capture Customer Energy and Demand Data		
Major Processes Supported	**Business Value**	**Security Concerns**
• Read Meters • Validate Meter Reads • Generate Customer Bills	• Eliminate meter reader labor cost and meter reading infrastructure cost • Increase billing accuracy • Enable time-based rates • Enable improved o Distribution system design o Distribution planning o Distribution operations and maintenance o Marketing	Confidentiality (privacy) of customer data Integrity of meter data Availability of meter data (for remote read)
Use Case 2: Remote Connect/Disconnect		
Major Processes Supported	**Business Value**	**Security Concerns**
• Establish service • Terminate service • Manage credit/collection	• Reduce field service truck rolls o Labor o Transportation • Reduce bad debt • Reduce energy losses	Integrity of signal (correct message and location) Confidentiality (privacy) of signal Availability of connect/disconnect service
Use Case 3: Tamper Detection		
Major Processes Supported	**Business Value**	**Security Concerns**
• Protect revenue; reduce energy theft	• Reduce lost revenue	Integrity of tamper indication Availability of tamper indication Confidentiality (privacy) of location data
Use Case 4: Meter Reading for Other Utilities		
Major Processes Supported	**Business Value**	**Security Concerns**
• Read gas/water meters	• Eliminate meter reader labor cost and meter reading	Confidentiality (privacy) of customer data

• Read gas/water meters (other utilities) • Transfer meter reading data to other utility	infrastructure cost • Create additional source of revenue • Leverage AMI investment	Integrity of meter data Availability of meter data (for remote read) Availability of meter data to contracting utility through B2B infrastructure

Table 2 – Billing Use Cases

2.1.2. Customer

Four Use Cases have also been defined under the category of Customer:

1. Customer reduces their usage in response to pricing or voluntary load reduction events
2. Customer has access to recent energy usage and cost at their site
3. Customer prepays for electric services
4. External clients use the AMI to interact with devices at customer site

Use Case 1 explores how the AMI system, working together with customers, can create mutually-beneficial programs to manage energy demand/consumption. Use Case 2 is related to 1 in that it describes ways that customers can access information about their energy costs and consumption, and how they can receive messaging from the utility informing the customer of an upcoming peak energy event, requiring/requesting customer load reductions. Customer Use Case 4 is directly related to the previous use cases as well in that it describes how a customer's energy cost/consumption data can be shared with a third party energy service provider to outsource the customer's energy consumption. Use Case 3 describes how AMI functionality can be leveraged to enable customer pre-payment for energy.

The primary business value in the Customer Use Cases comes from an enhanced ability to manage peak load on the distribution network. By communicating pricing signals and upcoming peak load events to customers, customers can modify their energy consumption behavior to reduce their energy costs. The utility benefits by reducing the potential for outages resulting from overload of the system and deferring new capital investments to provide increased capacity.

Another source of business value unique to Use Case 3 (Customer Prepayment) accrues to the utility through reduction in bad debt and improved cash flow.

The following table summarizes the major business processes supported by the Customer Use Cases and the key areas of business value that they enable.

Use Case 1: Demand Response / Load Reduction		
Major Processes Supported	**Business Value**	**Security Concerns**
• Manage Energy Demand/Consumption	• Reduce peak load o Defer new construction o Green benefits o Reduce outages	Confidentiality (access control) of customer equipment Integrity of control messaging and message information Availability of customer devices
Use Case 2: Customer Access to Energy Data		
Major Processes Supported	**Business Value**	**Security Concerns**
• Provide Energy	• Customer energy awareness	Confidentiality (access control)

Information to Customers and Third Parties	• Reduce peak load	of customer equipment via price signals and messages Integrity of control messaging and message information Availability of customer devices
Use Case 3: Customer Prepayment		
Major Processes Supported	**Business Value**	**Security Concerns**
• Collect Revenue from Energy Sales	• Reduce bad debt • Improve cash flow • Improve customer convenience/satisfaction	Confidentiality (privacy) of customer data and payments Integrity of control messaging and message information containing prepayment data Availability of customer payment data and usage balances
Use Case 4: Third Party Energy Management		
Major Processes Supported	**Business Value**	**Security Concerns**
• Manage Energy Demand/Consumption	• Reduce peak load • Customer satisfaction	Confidentiality (privacy) of customer data Integrity of usage data, rate information Availability of usage data, rate information

Table 3 - Customer Use Cases

2.1.3. Distribution System

Four Use Cases have been defined for the Distribution System category:

1. Distribution Operations curtails customer load for grid management
2. Distribution Engineering or Operations optimize network based on data collected by the AMI system
3. Customer Provides Distributed Generation
4. Distribution Operator locates Outage Using AMI Data and Restores Service

Distribution System Use Case 1 is similar to Customer Use Case 1. Both use cases describe the process to send signals to customers for the purpose of reducing load on the system, typically during a system peak. Customer Use Case 1 describes demand response events that the customer can voluntarily participate in using a price signal or a load control signal that the customer may ignore. Distribution System Use Case 1 describes demand response events that are non-voluntary using load control signals or meter disconnection commands. Distribution Use Case 2 explores how data gathered by the AMI system can be utilized (either online or offline) to improve power quality and the overall performance of the distribution network. Distribution Use Case 3 describes how the AMI system can interface with distributed generation (small, customer-owned generation) to improve network operations and reduce off-system energy purchases. Use Case 4 investigates how the AMI system can be leveraged to support the identification of outages on the system and to facilitate the restoration of power following an outage.

The primary areas of business value in the Distribution System Use Cases are related to improving network operations. Optimizing network operations can result in reduced energy losses, reduced outage frequency, and increased customer satisfaction (improved power quality). In addition, Use Case 4 explicitly describes processes to reduce outage duration and, therefore, customer satisfaction.

The following table summarizes the major business processes supported by the Distribution System Use Cases and the key areas of business value that they enable.

Use Case 1: Emergency Demand Response		
Major Processes Supported	**Business Value**	**Security Concerns**
• Manage Energy Demand/Consumption	• Reduce peak load o Defer new construction o Reduce outages	Confidentiality (access control) of customer equipment (including remote service switch and HAN devices) Integrity of control messaging and message information Availability of customer devices
Use Case 2: Distribution Network Optimization		
Major Processes Supported	**Business Value**	**Security Concerns**
• Manage Power Quality • Optimize Distribution Network • Manage Outages	• Customer satisfaction • Reduce energy losses • Improve outage performance	Integrity of system data Availability of system data Confidentiality of system data
Use Case 3: Distributed Generation		
Major Processes Supported	**Business Value**	**Security Concerns**
• Optimize Distribution Network • Manage/Dispatch Distributed Resources	• Network Optimization • Reduced Off-System Energy Purchases	Integrity of system data Availability of system data Confidentiality of system data
Use Case 4: Outage Location and Restoration		
Major Processes Supported	**Business Value**	**Security Concerns**
• Manage outages	• Reduced outage duration • Customer satisfaction	Availability of system data Integrity of system data Confidentiality of system data

Table 4 - Distribution Use Cases

2.1.4. Installation

Three Use Cases have been defined for the Installation category:

1. Utility installs, provisions, and configures the AMI system
2. Utility Manages End-to-End Lifecycle of the Meter System
3. Utility upgrades AMI to address future requirements.

Use Case 1 describes the process for deploying an AMI system, including the initial deployment plan, the forecasting and procurement process, logistical support, and field installation/testing/configuration. Use Case 2 focuses on managing the AMI system components through their life cycle, including maintenance and asset retirement. Use Case 3 explores future upgrades to the AMI system functionality and performance with particular attention to future deployment and integration of customer Home Area Network (HAN).

The key areas of business value in the Installation Use Cases include optimization of deployment costs and schedule for AMI system implementation, minimizing AMI operations and maintenance costs, maintaining billing accuracy, minimizing risk, and accommodating future growth and development within the AMI infrastructure.

The following table summarizes the major business processes supported by the Distribution System Use Cases and the key areas of business value that they enable.

Use Case 1: AMI System Deployment		
Major Processes Supported	**Business Value**	**Security Concerns**
• Deploy AMI system	• Optimize deployment costs/schedule	Integrity of system data for registration Availability of system data supporting deployment and registration Confidentiality of system data
Use Case 2: AMI System Maintenance		
Major Processes Supported	**Business Value**	**Security Concerns**
• Maintain AMI system	• Minimize AMI O&M costs • Maintain billing accuracy	Integrity of system data for remote diagnostics Availability of system data supporting maintenance and work orders Confidentiality of system data
Use Case 3: AMI System Upgrade		
Major Processes Supported	**Business Value**	**Security Concerns**
• Upgrade/enhance AMI system functionality/performance • Deploy/support customer HAN	• Minimize risk • Accommodate growth and future functionality	Integrity of system data for registration of new devices and remote firmware upgrades Availability of system data supporting deployment and remote upgrades Confidentiality of system data and customer data

Table 5 - Installation Use Cases

2.1.5. System

The final Use Case category is System. Only one Use Case has been defined for this category:

1. AMI system recovers after outage, communications or equipment failure.

System Use Case 1 explores how the AMI system responds and recovers to individual component failures, communications failures, and broader outages/disasters. The primary business value in this use case comes from maintaining AMI system integrity through unplanned equipment failures or distribution system outages.

Use Case 1: AMI System Recovery		
Major Processes Supported	**Business Value**	**Security Concerns**
• Recover from AMI component and telecommunications failures • Recover from major area outages/disasters	• Maintain system integrity	Integrity of system data Availability of system data Confidentiality of system data

Table 6 - AMI System Use Cases

2.2. System Context

AMI is the convergence of the power grid, the communications infrastructure, and the supporting information infrastructure. However, AMI security must exist in the real world with many stakeholders, other interested parties and overlapping responsibilities.

Consider an individual system that is part of an AMI solution to be made up of: 1) Software; 2) Hardware; 3) People and; 4) Information. Now, consider the entire AMI solution to be made up of a collection of various systems, each made up of software, hardware, workers and information – a system of systems. Systems-of-Systems are hierarchical in nature, that is, they naturally break down into parts.

The value of a logical decomposition comes from its ability to view a complex system at multiple levels of abstraction (decomposition) while maintaining forward and reverse traceability through the different levels of decomposition. Logical decomposition is can also be mapped to physical decomposition to correlate the model elements. The security domain model shown below (Figure 2) was developed to boundary the complexity of specifying the security required to implement a robust, secure AMI solution as well as serve as a tool to guide utilities in applying the security requirements in this document to their AMI implementation.

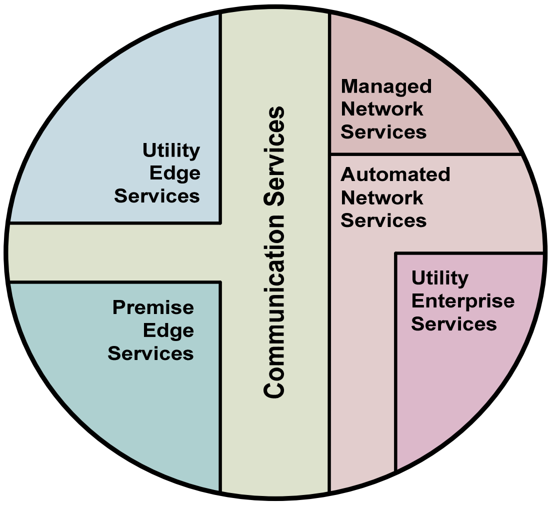

Figure 2 – AMI Security Domain Model

The following "services" are a description of each of the six security domains shown in the model above.

Security Domain	Description
Utility Edge Services	All field services applications including monitoring, measurement and control controlled by the Utility
Premise Edge Services	All field services applications including monitoring, measurement and control controlled by the Customer (Customer has control to delegate to third party)
Communications Services	are applications that relay, route, and field aggregation, field communication aggregation, field communication management information
Management Services	attended support services for automated and communication services (includes device management)
Automated Services	unattended collection, transmission of data and performs the necessary translation, transformation, response, and data staging
Business Services	core business applications (includes asset management)

Table 7 - AMI Security Domain Descriptions

Each utility's AMI implementation will vary based on the specific technologies selected, the policies of the utility company and the deployment environment. The application of the security requirements should guide the AMI system's capabilities.

Advanced Metering Infrastructure system use can be mapped across applicable security domains based on the collection of capabilities that enable use of the AMI. Security requirements in this document shall map to specific security domains based on the location of an enabling capability that enables a particular use for the AMI system. For any particular use of the AMI system, in the context of the enabling capability, the security requirements for that domain should be applied.

For example: If the use of the AMI system is "Remote Service Switch Operation" to support a customer "move-in" or "move-out" event then the analysis of which security requirements would apply for this use would be to map sequence of capabilities to domains.
(Note: there are a number of intermediate steps related to account updates, customer verification, policy enforcements and validations as well as error conditions not shown in this example.)

Process step	Enabling Capabilities (components)	Security Domain
Triggering event – Move-out request received from customer for a particular time and date	Request received via call center or via web (IVR or Company Website)	Utility Enterprise Services
Switch operation scheduled and validated	Customers Information System (CIS) or Meter Data Management Systems (MDMS)	Utility Enterprise Services
Command messages generated at scheduled time	CIS or MDMS	Utility Enterprise Services
Command received by head-end system	Network Management System (aka DCA or head-end)	Automated Network Services
Grid protection module validates command against rules (i.e. how many total service switch commands are pending in the next 10 min.)	Network Management System	Automated Network Services
Command transmitted to Meter	Network Management System	Automated Network Services
Command routed to the customer's meter	Wide-Area Network, Neighborhood Area Network (aka LAN)	Communication Services
Command received by meter	Meter	Utility Edge Services
Service Switch "opened"	Meter	Utility Edge Services
Acknowledgement message created	Meter	Utility Edge Services
Acknowledgement message transmitted	Wide-Area Network, Neighborhood Area Network (aka LAN)	Communications Services
Acknowledgement message	Network Management System	Automated Network Services

received		
Account status updated	CIS and or MDMS	Utility Enterprise Services

Table 8 - Mapping of AMI Security Domain Services to Utility Processes

It should be noted that this specification and the method of mapping security requirements to specific domains based on use is lifecycle agnostic. Meaning, some uses of the system (i.e. key placement in devices) may happen prior to the commencement of operations.

2.3. System Constraints

A number of system constraints need to be taken into account when satisfying security requirements found in this document. The requirements described do not prescribe which of a range of solutions (e.g., the use of narrow- or wide-band communications technologies) is most appropriate in a given setting. Such a decision is typically based on making prudent trade-offs among a collection of competing concerns, such as the following

- Other business or non-functional requirements
  - Performance (e.g., response time)
  - Usability (e.g., complexity of interactions for users)
  - Upgradability (e.g., ease of component replacement)
  - Adaptability (e.g., ease of reconfiguration for use in other applications)
  - Effectiveness (e.g., information relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner)
  - Efficiency (e.g., the provision of information through the most productive and economical use of resources)
  - Confidentiality (e.g., protection of sensitive information from unauthorized disclosure)
  - Integrity (e.g., accuracy, completeness and validity of information in accordance with business values and expectations)
  - Availability (e.g., information being available when required by the business process)
  - Compliance – (e.g., complying with the laws, regulations and contractual arrangements)
  - Reliability (e.g., the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities)

It is important to consider system constraints when developing applying security requirements. The requirements themselves do not take into account the trade-offs involved with design phase of AMI. Therefore, satisfying these requirements should not be done in isolation from the design.

- Constraints
  - Computational (e.g., available computing power in remote devices)
  - Networking (e.g., bandwidth, throughput, or latency)
  - Storage (e.g., required capacity for firmware or audit logs)
  - Power (e.g., available power in remote devices)

  - Personnel (e.g., impact on time spend on average maintenance)
  - Financial (e.g., cost of bulk devices)
  - Temporal (e.g., rate case limitations)
  - Technology
  - Availability
  - Maturity
  - Integration / Interoperability (e.g., legacy systems)
  - Lifecycle
  - Interconnectedness of infrastructure
  - Applications (e.g., the automated user systems and manual procedures that process the information)
  - Information (e.g., the data, in all their forms, input, processed and output by the information systems in whatever form is used by the business)
  - Infrastructure (e.g., the technology and facilities i.e., hardware, operating systems, database management systems, networking, multimedia, and the environment that houses and supports them, that enable the processing of the applications.)
  - People (e.g., the personnel required to plan, organize, acquire, implement, deliver, support, monitor and evaluate the information systems and services. They may be internal, outsourced or contracted as required.)
  - Time
  - Financial
  - Technical
  - Operational
  - Cultural
  - Ethical
  - Environmental
  - Legal
  - Ease of Use

- Regulatory requirements
  - Scope / sphere of influence
  - Acceptance vs. transference

2.4. Security States and Modes

This section discusses the states and modes that may apply to the system as a whole and/or the component level. A component may be a sub-system or individual element of the system. Security modes and states are considered in the evaluation of security requirements because they pose special circumstances for which the requirements may change. Evaluating these special circumstances is important because in any given state or mode the risk of a system or sub-system component may increase or decrease, thus needing supplemental requirement treatment (less or more).

Definitions of terms:

- State – a temporal condition of a system or component; implies a “snapshot”.
  - Typically within a time-based consideration
  - Sometimes overlap

- Mode – describes operational intent (implies action taken).

2.4.1. System States

The term s*tate* for the purposes of this document implies a snapshot of the system. The goal is to identify the state as they relate to security.

The System State Flow Diagram (Figure 3) assists in understanding the transition between states and the direction in which changes in state are allowed to occur. The System State Flow Diagram is used in defining the AMI system transitions. It is important to understand and control state flow in order to prevent an undesired, inadvertent system state. Transition of states for security components should be defined and understood with respect to defining requirements. The Sanitation State is also a shown as a path where high assurance is required.

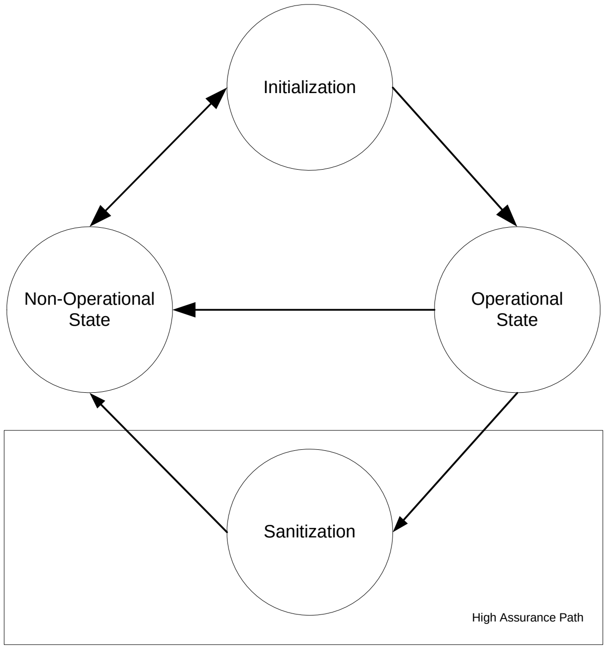

Figure 3 - Example of a System State Flow Diagram

System State	Description
Operational	Includes all functionality supportive of on-going operations (set by policy)
Non-operational	Not performing functionality indicative of on-going operations
Initialization	Used to configure system prior to operation
Sanitization	Removal and/or storing of information representative or residual of any running condition (e.g., sensitive data)

Table 9 - System States

2.4.1.1. System State Security Requirements

State.1 Activities allowed during non-operational state shall be limited to system activities needed to enter initialization. (Excludes interactions w/stakeholders, execution of business functions, etc.)

State.2 Activities allowed during initialization state shall be limited to system activities needed to enter operations. (Excludes interactions w/stakeholders, execution of business functions, etc.)

State.3 Activities allowed during initialization state shall include management functions necessary for element configuration.

State.4 Activities allowed during the initialization state shall include policy establishment (i.e., creation and configuration).

State.5 Activities allowed during the initialization state shall include security domain establishment.

State.6 A system shall transition into the operational state only upon completion of the critical initialization activities.

State.7 An operational system shall perform only those activities conformant to policy.

State.8 A system shall be capable of operating in a degraded mode while in an operational state. In this mode, “degraded” refers to a system that has non-operational or impaired components/elements. While services may be denied to some components/elements in the degraded mode, critical functions and security features of the system are still in force for the remaining components/elements.

State.9 A system shall transition into the non-operational state upon detection of a critical failure.

State.10 Supporting activities pertaining to the health of the system (e.g., diagnostics, maintenance, training, etc.) shall only be allowed during the operational state. Support activities may be performed in other system states, however they will be performed by systems external to the SUD.

2.4.2. System Modes

At the highest level, a system or component can be placed into a “normal” or “limited” mode of operation. At a minimum, modes should be taken into consideration during Protection Profile development. In a Protection Profile, criteria for entering and exiting each mode should be defined (pay close attention to risk associated with transition between modes – i.e., target mode must be defined before leaving current mode). For a more granular analysis, one may consider the following refinement examples:

- On-Line/Off-Line – system or element is accessible (or non-accessible) from a communication point of view
- Lock – certain functions are not accessible / intentionally disabled
- Maintenance – configuring / patching
- Diagnostics – monitoring for purposes of problem resolution (i.e., debugging)
- Commissioning/Decommissioning – initialization/establishment of functionality or service (decommissioning is reverse)
- Learning – acquiring new parameters and/or functionality for purposes of optimization
- Training – utilizing system functions for purposes of familiarization and simulation. (“Real” outputs are not engaged.)
- Sleep/Power saving – certain functions are temporarily disabled or degraded for decreased energy consumption.
- Special/Emergency – configurations based on criticality of function and preferential and/or prioritized treatment of certain operations. (Example needed, i.e., impending natural disaster.)

2.5. Security Objectives

As currently envisioned, Smart Grid services promise unprecedented levels of automation, situational awareness, and fine-grained control of the generation, transmission, distribution and use of electric power. If fully realized, such services should significantly increase the effectiveness, efficiency and reliability of the electric power system providing lower operating costs associated with many of today's labor-intensive tasks and would provide the incentives and technical capability for customers to automatically manage their usage patterns. Customers would specify demand-response usage policies based on pricing signals from the market or would permit direct supplier control of end-user load (automatically shedding load to reduce peak demand or mitigate emergency situations). In conjunction with end-user control, demand response would make the most efficient use of available generating capacity, while supporting conservation and environmental efforts.

Smart Grid services typically require complex distributed applications (some with near real-time constraints), communication over highly-networked information infrastructures, that include a broad range of Internet technologies. For the vision of the Smart Grid to be realized, system security must be maintained at a consistently high levels of assurance. Security concerns must be addressed from the outset of any Systems Development Life Cycle (SDLC) activity throughout every systems engineering, including architecture, acquisition, implementation, integration, deployment, operations, maintenance, and decommissioning. Security solutions must be comprehensive or *holistic* in nature (obligatory clichés: you’re only as strong as your weakest line” and "the devil is in the details") and capable of evolving in response to changes in the threat or technological environment.

The Smart Grid's primary (cyber) security objectives are as follows:

- Protect all Smart Grid services from malicious attack[1] and unintended adverse cyber and physical events that threaten the mission of the service (i.e., *security events*).
    - Ensure that sufficient information about a security events are available when and where needed to support the decision making necessary to protect (or minimize the disruption to) the mission of the affected Smart Grid service. This includes the collection and delivery of the real-time data needed for situational awareness as well as the collection and protection of forensics data needed for post-mortem analysis to improve the security and survivability of the system in the face of future security events.
    - Ensure the integrity, availability, and (where appropriate) the confidentiality of the information regarding security services, survivability services and mechanisms used to protect the Smart Grid services. These security and survivability services and mechanisms shall not provide an attack vector or incorrectly respond to malicious or benign stimuli in a manner that would create or worsen a security event.
- Prevent security incidents associated with a Smart Grid service from contributing to or complicating the safety and protection of personnel, stakeholders, stakeholder services and the electrical system.
    - Do not allow any Smart Grid service or its associated technology (e.g., communications networks and gateways) to be used as a stepping stone or conduit for attacks (or amplifying the effects of attacks) on other Smart Grid services, end users, external service providers (e.g., cell phone networks, ISPs), or any other interconnected entity.
    - Smart Grid services shall not amplify the adverse effects of any accident, natural disaster, or human error.
- Provide sufficient evidence to support the assurance of justifiable confidence (i.e., trust) in the integrity, confidentiality, and availability of Smart Grid services. (For example, provide evidence to support public trust in the accuracy of billing statements, the safety and reliability of electricity services, and the fairness of energy markets.)

Smart Grid security involves a system of systems approach in engineering design and operations, which requires that security responsibility be extend beyond the Smart Grid. While security requirements for the broader Smart Grid may or may not be within the scope of a single utility's responsibility, imposing the requirements through agreements and/or regulatory mandates upon cooperating interconnecting systems and corresponding capabilities will meet and/or support some aspects of the Smart Grid security objectives. Moreover, interdependencies among the power grid, the communications infrastructure, and the information infrastructure pose a particularly serious challenge to the design of a secure and survivable Smart Grid.

As an example, AMI system security must protect the missions of all AMI business functions and must not be allowed to be used as a conduit for attacking some method of control of the grid. This does not imply that AMI security architects are solely responsible for ensuring this, but rather that responsibility must be assigned for a systems of systems perspective wherein potential AMI impacts on the larger grid are analyzed, anticipated, and defended against in some portion of the overall system of systems (SoS) architecture and implementation.

Here are a few examples of what the Smart Grid security objectives are meant to prevent:

[1] Includes cyber and physical attacks, such as attempts to physically tamper with a meter, and disruption of the supporting communications infrastructure.

- Reputational Loss - Attacks or accidents that destroy trust in Smart Grid services, including their technical and economic integrity
- Business Attack - Theft of money or services or falsifying business records
- Gaming the system - Ability to collect, delay, modify, or delete information to gain an unfair competitive advantage (e.g., in energy markets)
- Safety - Attack on safety of the grid, its personnel or users
- Assets - Damaging physical assets of the grid or assets of its users
- Short-term Denial or Disruption of Service
- Long-term Denial or Disruption of Service (including significant physical damage to the grid)
- Privacy violations
- Hijacking control of neighbor's equipment
- Physical and logical tampering
- Subverting situational awareness so that operators take fatal actions that disrupt the system
- Cause automated system to waste resources on false alarms.
- Hijacking services
- Using Smart Grid services or the supported communication mechanisms to attack end users residential or industrial networks (e.g., allowing end-users to compromise other end-users' networked systems.)

2.5.1. Holistic Security

The magnitude of the challenge posed by melding the complexity of the power grid with open, distributed, highly networked technologies, crossing multiple organizational and administrative boundaries, in the presence of intelligent adversaries, is such that traditional security approaches alone are insufficient to meet them.

The primary concern is with protecting the business missions embodied in each of the Smart Grid services individually and collectively, not merely in enforcing security requirements or protecting IT components. *Survivability* is the capability of a system to fulfill its mission in a timely manner despite attack, accident or subsystem failure. Survivability is a blend of security and business risk management that builds upon traditional security approach by adding domain-specific strategies and tactics to create a holistic perspective. The characteristics of a survivable system include its ability to prevent or resist attacks, accidents, other forms of stress, recognize a survivability event and the state of the system under stress and to recover from the adverse impact of a survivability event in a timely manner. Survivability is marked by graceful degradation under stress, with essential services maintained.

2.6. User Characteristics

Many of the security requirements within this document are written with respect to a generic notion of an actor or user, rather than identifying specific users such as a maintenance engineer or residential customer. When such a requirement is applied to an architectural element, it should be tailored to specific types of users by taking into account the characteristics of each type of user and how that informs the requirement.

Typical classes of users (at a high level) include (refer to the Contextual View for insight into these classes of users)

- Utility
- Customer
- Third-party

Some of the characteristics that distinguish these classes of users, and even different types of users within these classes, are:

- Organizational responsibility
- Organizational authority
- Ability to delegate authority
- Privileges within the domain
- Access of users

When tailoring a requirement, one might generate several versions of a requirement, each of which differs by identifying a different user and requiring slightly different responses (e.g., level of access control required for a given behavior).

2.7. Assumptions and Dependencies

This document is an ad hoc security specification, and as such does not contain requirements pertaining to business (functional) requirements or quality of service (non-functional) requirements (e.g., performance, usability, or maintainability issues). It is assumed that business requirements have already been established for deploying an AMI solution. It does contain a collection of security requirements that have been drawn from industry best practices and government sources documenting best practices for security.

It is not the intent of this document to specify the security requirements for any particular AMI system. Instead, the goal is to provide guidance likely to be suitable across a variety of different AMI implementations. No assumptions are made regarding context specific characteristics such as available computing, software and/or infrastructure resources, unless specifically cited. No assumptions are made regarding the presence or absence of specific business requirements.

This document contains high-level requirements, not detailed specifications. Details such as specific interfaces, algorithms, protocols, and technology solutions are not addressed. These requirements should provide the impetus for the creation of more detailed specifications for AMI systems, the specifics of which depend on each AMI system's context (e.g., actual assets and information flows, business requirements, and detailed risk assessments).

3. System Security Requirements

The requirements found throughout this section are fine grained. A given section may contain related requirements addressing the same need that differ in terms of the strength of mechanism, rigor and protection each offers.

Requirements are given a lettering scheme as follows:

- Requirements that begin with an “F” are functional requirements.
- Requirements that end with an “S” are supporting services to functional requirements.
- Requirements that begin with an “A” are assurance requirements.
- Remaining letters in the identifier help associate the requirement to its requirement class.

3.1. Primary Security Services

This area uses business/mission needs to define requirements. It answers the question, “What security is needed?”

3.1.1. Confidentiality and Privacy (FCP)

This class contains confidentiality and privacy requirements. These requirements provide a user, service or object protection against discovery and misuse of identity by other users/subjects.

FCP.1	The security function shall ensure that [assignment: set of unauthorized users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects].
FCP.2	The security function shall provide [selection: an authorized user, [assignment: list of trusted subjects]] a capability to determine the user identity based on the provided alias only under the following [assignment: list of conditions].
FCP.3	The security function shall be able to provide [assignment: number of aliases] aliases of the real identity (e.g., user name) to [assignment: list of subjects].
FCP.4	The security function shall [selection, choose one of: determine an alias for a user, accept the alias from the user] and verify that it conforms to the [assignment: alias metric].
FCP.5	The security function shall provide an alias to the real user name which shall be identical to an alias provided previously under the following [assignment: list of conditions] otherwise the alias provided shall be unrelated to previously provided aliases.
FCP.6	The security function shall ensure that [assignment: list of users and/or subjects] are unable to determine whether [assignment: list of operations][selection: were caused by the same user, are related as follows[assignment: list of relations]].
FCP.7	The security function shall ensure that [assignment: list of users and/or subjects] are unable to observe the operation [assignment: list of operations] on [assignment: list of objects] by [assignment: list of protected users and/or subjects].
FCP.8	The security function shall allocate the [assignment: unobservability related information] among different parts of the module such that the following conditions hold during the lifetime of the information: [assignment: list of conditions].
FCP.9	The security function shall provide [assignment: list of services] to [assignment: list of subjects] without soliciting any reference to [assignment: privacy related information (e.g., real username)].
FCP.10	The security function shall provide [assignment: list of authorized users] with the capability to observe the usage of [assignment: list of resources and/or services].
FCP.11	The security function shall prevent unauthorized and unintended information transfer via shared system resources.
FCP.12	The functions provided by the security function to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [assignment: quantification] for loss of security function data or objects under the control of the module's security function.
FCP.13	The security function shall protect security function data from unauthorized disclosure when it is transmitted between separate parts of the system.
FCP.14	The security function shall identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries.
FCP.15	The authentication mechanisms in the system shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.
FCP.16	The security function shall ensure that the security attributes, when exported outside the system, are

	unambiguously associated with the exported user data.

3.1.2. Integrity (FIN)

"Maintaining a control 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 control 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 control 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]

FIN.1	The security function shall preserve a secure state when the following types of failures occur: [List of types of failure in the module]
FIN.2	The security function shall provide the capability to detect modification of all security function data during transmission between the security function and another trusted IT product within the following metric: [assignment: a defined modification metric].
FIN.3	The security function shall provide the capability to verify the integrity of all security function data transmitted between the security function and another trusted IT product and perform [assignment: action to be taken] if modifications are detected.
FIN.4	The security function shall provide the capability to correct [assignment: type of modification] of all security function data transmitted between the security function and another trusted IT product.
FIN.5	The security function shall be able to detect [selection: modification of data, substitution of data, re-ordering of data, deletion of data, [assignment: other integrity errors]] for security function data transmitted between separate parts of the module.
FIN.6	Upon detection of a data integrity error, the security function shall take the following actions: [assignment: specify the action to be taken].
FIN.7	The security function shall provide detection of physical tampering that might compromise the module's security function.
FIN.8	The security function shall provide the capability to determine whether physical tampering with the module's security function's devices or module's security function's elements has occurred.
FIN.9	For [assignment: list of security function devices/elements for which active detection is required], the security function shall monitor the devices and elements and notify [assignment: a designated user or role] when physical tampering with the module's security function's devices or module's security function's elements has occurred.
FIN.10	The security function shall resist [assignment: physical tampering scenarios] to the [assignment: list of security function devices/elements] by responding automatically such that the integrity is maintained.
FIN.11	After [assignment: list of failures/service discontinuities] the security function shall enter a [assignment: mode (e.g., maintenance mode)] where the ability to return to a secure state is provided.
FIN.12	For [assignment: list of failures/service discontinuities], the security function shall ensure the return of the module to a secure state using automated procedures.
FIN.13	When automated recovery from [assignment: list of failures/service discontinuities] is not possible, the security function shall enter [assignment: mode (e.g., a maintenance mode)] where the ability to

	return to a secure state is provided.
FIN.14	The utility provided by the security function to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [assignment: quantification] for loss of module's security function data or objects under the control of the module's security function.
FIN.15	If the security function and/or system experience failure or service discontinuity, the security function shall provide the capability to determine the objects that were or were not capable of being recovered; as a result, the following actions should be taken [assignment: action to be taken].
FIN.16	The security function shall detect replay for the following entities: [assignment: list entities].
FIN.17	The security function shall use [assignment: list of interpretation rules to be applied by the module's security function] to consistently interpret security function data from another trusted IT product.
FIN.18	The security function shall run a suite of tests [selection: during initial start-up, periodically during normal operation, at the request of an authorized user, [assignment: other conditions]] to check the fulfillment of [assignment: list of properties of the external entities]. If the test fails, the security function shall [assignment: action(s)].
FIN.19	The security function shall ensure that security function data is consistent when replicated between [assignment: parts of the system].
FIN.20	When parts of the module containing replicated security function data are disconnected, the security function shall ensure the consistency of the replicated security function data upon reconnection before processing any requests for [assignment: list of functions dependent on security function data replication consistency].
FIN.21	The security function shall run a suite of *self-tests* during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-test should occur] to demonstrate the correct operation of [selection: [assignment: parts of security function (e.g. key management)], the module's security function.
FIN.22	The security function shall provide authorized users with the capability to verify the integrity of [selection: [assignment: parts of module's security function], security function data].
FIN.23	The security function shall provide authorized users with the capability to verify the integrity of stored security function executable code.
FIN.24	The security function shall verify the correct operation of security utilities [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies [assignment: user, etc. (e.g., system administrator), shuts the system down, restarts the system] when anomalies are discovered.
FIN.25	The security function shall detect and protect against unauthorized changes to software and information.
FIN.26	The security function shall restrict the capability to input information to the information system to authorized personnel.
FIN.27	The security function shall check information for accuracy, completeness, validity, and authenticity.
FIN.28	The organization shall handle and retain output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
FIN.29	The organization shall develop, disseminate, and periodically review/update: 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 of the system and information integrity policy and associated system and information integrity controls.
FIN.30	The organization shall identify, report, and remediate control system flaws per organizational, legal, and/or regulatory policies.

FIN.31	The security function employs malicious code protection.
FIN.32	The security function shall verify the correct operation of security functions within the control system upon system startup and restart; upon command by user with appropriate privilege; periodically; and/or at defined time periods. The security function notifies the [assignment: system administrator, system component, etc.] when anomalies are discovered.
FIN.33	The security function shall monitor and detect unauthorized changes to software and information.
FIN.34	The security function shall implement security measures to restrict information input to the control system to authorized personnel only.
FIN.35	The security function shall employ mechanisms to check information for accuracy, completeness, validity, and authenticity.
FIN.36	The organization shall handle and retain output from the security function in accordance with applicable laws, regulations, standards, and organizational policy, as well as operational requirements of the control process.
FIN.37	The security function shall protect the integrity of transmitted information.
FIN.38	The security function shall reliably associate [assignment: security parameters] with information exchanged between [assignment: information systems].
FIN.39	The security function 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 sources when requested by client systems.
FIN.40	The security function that collectively provides name/address resolution service for an organization shall be fault tolerant and implement role separation.
FIN.41	The security function shall protect security function data from modification when it is transmitted between separate parts of the system.
FIN.42	The security function shall mark output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.
FIN.43	The security function shall provide [assignment: list of subjects] with the ability to verify evidence of the validity of the indicated information and the identity of the [assignment: user, object, etc.] that generated the evidence.

3.1.3. Availability (FAV)

This involves the ability of the system to continue to operate and satisfy business/mission needs under diverse operating conditions, including but not limited to peak load conditions, attacks, maintenance operations, and normal operating conditions.

FAV.1	The security function shall ensure the operation of [assignment: list of system’s capabilities] when the following failures occur: [assignment: list of type of failures].
FAV.2	The security function shall assign a priority to each subject in the system's security function in terms of availability.
FAV.3	The security function shall ensure that each access to [assignment: controlled resources] shall be mediated on the basis of the subjects assigned priority.
FAV.4	The security function shall ensure that each access to all shareable resources shall be mediated on the basis of the subjects assigned priority.
FAV.5	The security function shall enforce maximum quotas of the following resources: [assignment: controlled resources] that [selection: individual user, defined group of users, subjects] can use [selection: simultaneously, over a specified period of time].

FAV.6	The security function shall ensure the provision of minimum quantity of each [assignment: controlled resource] that is available for [selection: an individual user, defined group of users, subjects] to use [selection: simultaneously, over a specified period of time].
FAV.7	The security function shall protect against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].
FAV.8	The security function shall limit the use of resources by priority.
FAV.9	The functions provided by the security function to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [assignment: quantification] for loss of security function data or objects under the control of the module's security function.
FAV.10	The security function shall ensure the availability of [assignment: list of types of security function data] provided to another trusted IT product within [assignment: a defined availability metric] given the following conditions [assignment: conditions to ensure availability].

3.1.4. Identification (FID)

This section covers requirements around who an actor claims to be.

FID.1	The security function shall require each user to be successfully identified before allowing any other system's security function-mediated actions on behalf of that user unless is one of the following: [list of system's security function-mediated actions] that may be allowed before the user is identified.
FID.2	The security function shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: list of user security attributes].
FID.3	The security function shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initial association of attributes].
FID.4	The security function shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].
FID.5	The security function shall uniquely identify (and authenticate) [assignment: users, processes acting on behalf of users, devices, etc.] before establishing a connection.
FID.6	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. Issuing the user identifier to the intended party; 5. Disabling the user identifier after [Assignment: organization-defined time period] of inactivity; and 6. Archiving user identifiers.
FID.7	The security function shall have mechanisms to uniquely identify (and authenticate) [assignment: users, processes acting on behalf of users, etc.].
FID.8	The security function shall appropriately label information in storage, in process and in transmission.

3.1.5. Authentication (FAT)

This section covers requirements around the proof of identity of an actor.

FAT.1	After a predetermined period of inactivity, the 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.
FAT.2	The security function shall employ a mechanism to authenticate specific devices before establishing a connection.
FAT.3	The security function 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.
FAT.4	The security function shall have mechanisms to authenticate users (or processes acting on behalf of users).
FAT.5	The security function enforces assigned authorizations for controlling access to the system in accordance with applicable policy.
FAT.6	The security function 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.
FAT.7	The security function shall enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
FAT.8	The security function shall enforce the most restrictive set of rights and privileges or accesses needed by [assignment: users, processes acting on behalf of users, etc.] for the performance of specified tasks.
FAT.9	The security function shall (identify and) authenticate specific devices before establishing a connection.
FAT.10	The security function shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and unauthorized use.
FAT.11	The security function shall uniquely authenticate [assignment: users, processes acting on behalf of users, etc.].
FAT.12	The organization shall authorize all methods of remote access to the system.
FAT.13	The organization shall develop and enforce policies and procedures for system users concerning the generation and use of passwords. These policies stipulate rules of complexity, based on the criticality level of the systems to be accessed.
FAT.14	The organization shall develop, disseminate and periodically review and update: 1. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
FAT.15	The organization shall develop, disseminate and periodically review and update: 1. A formal, documented, authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated authentication controls.
FAT.16	The organization shall employ mechanisms in the design and implementation of a system to restrict public access to the system from the organization's enterprise network.
FAT.17	The organization shall establish terms and conditions for authorized individuals to: 1. Access the information system from an external information system; and 2. Process, store, and/or transmit organization-controlled information using an external information system.
FAT.18	The organization shall identify and document specific user actions (authorizations) that can be performed on the information system without identification or authentication.

FAT.19	The organization shall manage information system authenticators by: 1. Defining initial authenticator content; 2. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; 3. Changing default authenticators upon information system installation; and 4. Changing/refreshing authenticators periodically
FAT.20	The organization shall supervise and review the activities of users with respect to the enforcement and usage of system access controls.
FAT.21	The organization shall: 1. Establish usage restrictions and implementation guidance for [assignment: devices (e.g., wireless technologies, portable and mobile devices and media)]; and, 2. Authorize, monitor and control access to the system. 3. Document, monitor, log, and limit access of these devices to the organization's system. 4. Appropriate organizational officials shall authorize the use of these devices per organization's established security policy and procedures.
FAT.22	The security function authenticates specific devices before establishing a connection.
FAT.23	The security function shall [selection: detect, prevent] use of authentication data that has been copied or forged by any actor of the system.
FAT.24	The security function shall allow [assignment: list of security function mediated actions] on behalf of the user to be performed before the user is authenticated.
FAT.25	The security function shall allow the [assignment: the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created.
FAT.26	The security function shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].
FAT.27	The security function shall be able to associate [assignment: users] with roles.
FAT.28	The security function shall be able to enforce the use of security function generated secrets for [assignment: list of functions].
FAT.29	The security function shall enforce the [assignment: access control security function policy] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the security function's policy.
FAT.30	The security function shall enforce the [assignment: access control security function policy] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated security function policy, and for each, the security function policy-relevant security attributes, or named groups of security function policy-relevant security attributes].
FAT.31	The security function shall enforce the [assignment: access control security function policy(s), information flow control security function policy(s)] to restrict the ability to [selection: change, default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles].
FAT.32	The security function shall enforce the [assignment: access control security function policy, information flow control security function policy] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the security function policy.
FAT.33	The security function shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].
FAT.34	The security function shall enforce the rules [assignment: specification of revocation rules].
FAT.35	The security function shall ensure that all operations between any subject controlled by the security function and any object controlled by the security function are covered by an access control security function policy.

FAT.36	The security function shall ensure that the conditions [assignment: conditions for the different roles] are satisfied.
FAT.37	The security function shall explicitly [selection: authorize, deny] an information flow based on the following rules: [assignment: rules, based on security attributes that explicitly [selection: authorize, deny] information flows].
FAT.38	The security function shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes that explicitly deny access of subjects to objects].
FAT.39	The security function shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].
FAT.40	The security function shall maintain the roles: [assignment: authorized identified roles].
FAT.41	The security function shall prevent reuse of authentication data related to [assignment: identified authentication mechanism(s)].
FAT.42	The security function shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.
FAT.43	The security function shall provide a mechanism to *generate* secrets that meet [assignment: a defined quality metric].
FAT.44	The security function shall provide a mechanism to *verify* that secrets meet [assignment: a defined quality metric].
FAT.45	The security function shall provide only [assignment: list of feedback] to the user while the authentication is in progress.
FAT.46	The security function shall re-authenticate the user under the conditions [assignment: list of conditions under which re-authentication is required].
FAT.47	The security function shall require an explicit request to assume the following roles: [assignment: the roles].
FAT.48	The security function shall require each user to be successfully authenticated before allowing any other system's security function-mediated actions on behalf of that user.
FAT.49	The security function shall restrict the ability to [selection: change, default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of security function data] to [assignment: the authorized identified roles].
FAT.50	The security function shall restrict the ability to [selection: determine the behavior of, disable, enable, modify the behavior of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].
FAT.51	The security function shall restrict the ability to revoke [assignment: list of security attributes] associated with the [selection: users, subjects, objects, [assignment: other additional resources]] under the control of the security function to [assignment: the authorized identified roles].
FAT.52	The security function shall restrict the capability to specify an expiration time for [assignment: list of security attributes for which expiration is to be supported] to [assignment: the authorized identified roles].
FAT.53	The security function shall restrict the specification of the limits for [assignment: list of security function data] to [assignment: the authorized identified roles].
FAT.54	The security function shall use the following rules to set the value of security attributes: [assignment: rules for setting the values of security attributes]
FAT.55	Based on the criticality level of the systems to be accessed, the organization shall develop and enforce policies and procedures for system users concerning the generation, use and rules of complexity for passwords.
FAT.56	The security function shall prevent further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity, and the session lock remains in effect

	until the user reestablishes access using appropriate identification and authentication procedures.
FAT.57	When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the security function shall [assignment: list of actions].

3.1.6. Authorization (FAZ)

Authorization is the approval of an actor to perform an action.

FAZ.1	The security function shall enforce assigned authorizations for controlling access to the system in accordance with applicable policy.
FAZ.2	The security function shall enforce separation of duties through assigned access authorizations.
FAZ.3	The security function shall enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
FAZ.4	The organization shall document authorization and approval policies and procedures and maintains a list of personnel authorized to perform maintenance on the control system. Only authorized and qualified organization or vendor personnel perform maintenance on the system.
FAZ.5	The organization shall develop and keep current a list of personnel with authorized access to the facility where [assignment: type of system (e.g., control system, information system)] resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].
FAZ.6	The organization shall control all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization shall control access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
FAZ.7	The organization shall review information system and facility access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions
FAZ.8	The organization shall limits physical access to all control system facilities and assets and verifies individual access authorizations before granting access. The organization shall limit access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
FAZ.9	The organization shall authorize (i.e., accredit) the system for processing before operations and periodically update the authorization [assignment: organization-defined frequency] or when there is a significant change to the system. A senior organizational official shall sign and approve the security accreditation.
FAZ.10	The security function shall enforce the most restrictive set of rights, privileges or accesses needed by users or workstations (or processes acting on behalf of users) for the performance of specified tasks.
FAZ.11	The security function shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes that explicitly authorize access of subjects to objects].
FAZ.12	The security function shall enforce a limit of [assignment: organization-defined number] consecutive invalid access attempts by a user during a [assignment: organization-defined time period] time period. The security function shall automatically [Selection: locks the account/node for an [assignment: organization-defined time period], delays next login prompt according to [assignment: organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is exceeded.

FAZ.13	The security function automatically terminates a remote session after [assignment: defined period of inactivity] for [assignment: workstations, servers, etc.] that are used for [assignment: system monitoring, maintenance activities, etc.] based on the risk assessment of the system and the organization’s security policy.
FAZ.14	The security function shall limit the number of concurrent sessions for any user to [assignment: organization-defined number of sessions] on the system.

3.1.7. Non-Repudiation (FNR)

Non-repudiation is the ability to irrefutably, tie an actor to an action.

FNR.1	The security function shall be able to generate evidence of origin for transmitted [assignment: list of information types] at the request of the [selection: originator, recipient, [assignment: list of third parties]].
FNR.2	The security function shall be able to relate the [assignment: list of attributes] of the originator of the information, and the [assignment: list of information fields] of the information to which the evidence applies.
FNR.3	The security function shall provide a capability to verify the evidence of origin of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of origin].
FNR.4	The security function shall enforce the generation of evidence of origin for transmitted [assignment: list of information types] at all times.
FNR.5	The security function shall be able to generate evidence of receipt for received [assignment: list of information types] at the request of the [selection: originator, recipient, [assignment: list of third parties]].
FNR.6	The security function shall be able to relate the [assignment: list of attributes] of the recipient of the information, and the [assignment: list of information fields] of the information to which the evidence applies.
FNR.7	The security function shall provide a capability to verify the evidence of receipt of information to [selection: originator, recipient, [assignment: list of third parties]] given [assignment: limitations on the evidence of receipt].
FNR.8	The security function shall enforce the generation of evidence of receipt for received [assignment: list of information types] at all times.
FNR.9	The security function shall provide mechanisms to protect the authenticity of communications sessions.
FNR.10	The security function shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: list of objects or information types].
FNR.11	The security function shall provide the capability to determine whether a [assignment: given individual, system, etc.] took a particular [assignment: action].

3.1.8. Accounting (FAC)

This section covers the recording of activity by actors/elements throughout the system. Accounting requirements provide the means to perform a successful audit of events that occur on the system.

FAC.1	The security function shall take [assignment: list of actions] upon detection of a potential security

	violation.
FAC.2	The security function shall be able to generate an accounting record of the following auditable events: 1. Start-up and shutdown of the audit functions; 2. All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and 3. [assignment: other specifically defined auditable events]
FAC.3	The security function shall generate audit records, at a minimum, for the following events whether or not the attempts were successful: 1. Attempts to logon; 2. Attempts to change local account attributes such as privileges; 3. Attempts to change local security policy
FAC.4	The security function shall provide [assignment: authorized users] with the capability to read [assignment: list of audit information] from the audit records.
FAC.5	The security function shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
FAC.6	The security function shall ensure that [assignment: metric for saving audit records] stored audit records will be maintained when the following conditions occur: [selection: audit storage exhaustion, failure, attack]
FAC.7	The security function shall generate audit records for the following events: [Assignment: organization-defined auditable events].
FAC.8	The security function shall record within each accounting record at least the following information: 1. Date and time of the event, type of event, subject identity and/or source of the event, and the outcome (e.g., success or failure) of the event; and 2. For each audit event type [assignment: other audit relevant information].
FAC.9	For audit events resulting from actions of identified users, the security function shall be able to associate each auditable event with the identity of the user that caused the event.
FAC.10	The security function shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the security function requirements.
FAC.11	The security function shall enforce the following rules for monitoring audited events: 1. Accumulation or combination of [assignment: subset of defined auditable events] known to indicate a potential security violation; 2. [assignment: any other rules]
FAC.12	The security function shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [assignment: the profile target group].
FAC.13	The security function shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.
FAC.14	The security function shall be able to indicate a possible violation of the enforcement of the security function requirements when a user's suspicion rating exceeds the following threshold conditions [assignment: conditions under which anomalous activity is reported by the module's security function].
FAC.15	The security function shall be able to maintain an internal representation of the following signature events [assignment: a subset of system events] that may indicate a violation of the enforcement of the security function requirements.
FAC.16	The security function shall be able to compare the signature events against the record of system activity discernible from an examination of [assignment: the information used to determine system activity].

FAC.17	The security function shall be able to indicate a potential violation of the enforcement of the security function requirements when a system event is found to match a signature event or event sequence that indicates a potential violation of the enforcement of the security function requirements.
FAC.18	The security function shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios [assignment: list of sequences of system events whose occurrence are representative of known penetration scenarios] and the following signature events [assignment: a subset of system events] that may indicate a potential violation of the enforcement of the security function requirements.
FAC.19	The security function shall be able to compare the signature events and event sequences against the record of system activity discernible from an examination of [assignment: the information to be used to determine system activity].
FAC.20	The security function shall provide the audit records in a manner suitable for the user to interpret the information.
FAC.21	The security function shall provide the ability to apply [assignment: methods of selection and/or ordering] of audit data based on [assignment: criteria with logical relations].
FAC.22	The security function shall be able to select the set of audited events from the set of all auditable events based on the following attributes: 1. [selection: object identity, user identity, subject identity, host identity, event type] 2. [assignment: list of additional attributes that audit selectivity is based upon]
FAC.23	The security function shall be able to [selection, choose one of: prevent, detect] unauthorized modifications to the stored audit records in the audit trail.
FAC.24	The security function shall protect audit information and audit tools from unauthorized access, modification, and deletion.
FAC.25	The security function shall [assignment: actions to be taken in case of possible audit storage failure] if the audit trail exceeds [assignment: pre-defined limit].
FAC.26	The security function shall [selection, choose one of: “ignore audited events”, “prevent audited events, except those taken by the authorized user with special rights”, “overwrite the oldest stored audit records”] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.
FAC.27	The organization shall allocate sufficient audit record storage capacity and configures auditing to reduce the likelihood of exceeding storage capacity.
FAC.28	The security function shall alert appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].
FAC.29	The security function shall provide an audit reduction and report generation capability.
FAC.30	The security function shall provide time stamps for use in audit record generation.
FAC.31	The security function/system 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.
FAC.32	The security function shall display an approved, system use notification message before granting system access informing potential users: 1. That the user is accessing a [assignment: name of organization’s information system]; 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; and 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 associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

3.2. Supporting Security Services

Supporting Security Services requirements are how security is realized for primary security requirements. Each requirement in this section maps to requirements in Section 3.1. The mapping should indicate which requirements from Section 3.1 are satisfied (in whole or in part) given satisfaction of the identified 3.2 requirement. The litmus test for inclusion in this section is simple. If any requirement in this section cannot be mapped to at least two requirements across confidentiality, integrity and availability (CIA), then it should appear in Section 3.1.
Policy requirements can appear in this section, so long as they are relevant to a specific supporting security service area.

3.2.1. Anomaly Detection Services (FAS)

Detection services detect events outside of the bounds of normally anticipated or desired behavior such as attacks, intrusions, or errors.

FAS.1	Upon detection of a data integrity error, the security function shall take the following actions: [assignment: specify the action to be taken].
FAS.2	The security function shall provide unambiguous detection of physical tampering that might compromise the module's security function.
FAS.3	For [assignment: list of security function devices/elements for which active detection is required], the security function shall monitor the devices and elements and notify [assignment: a designated user or role] when physical tampering with the module's security function's devices or module's security function's elements has occurred.
FAS.4	The security function shall take [assignment: list of actions] upon detection of a potential security violation.
FAS.5	The organization shall employ and maintain fire suppression and detection devices/systems that can be activated in the event of a fire.
FAS.6	The organization shall implement and maintain fire suppression and detection devices/systems that can be activated in the event of a fire.
FAS.7	The organization shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
FAS.8	The organization shall implement control system incident handling capabilities for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

3.2.2. Boundary Services (FBS)

This section provides requirements around boundary services. Boundary services provide isolation between system elements or between the system and external entities. Boundary services explain what occurs at the transition between two separate security domains such as examination or changing constraints on the border relationship.
Boundary requirements are oriented towards maintaining the strength and integrity of the boundary (isolation) between inside and outside of the system boundary. The requirements for a firewall configuration are one set of examples.

FBS.1	The security function shall restrict the scope of the session security attributes [assignment: session security attributes], based on [assignment: attributes].

FBS.2	The security function shall restrict the maximum number of concurrent sessions that belong to the same user.
FBS.3	The security function shall enforce, by default, a limit of [assignment: default number] sessions per user.
FBS.4	The security function shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [assignment: rules for the number of maximum concurrent sessions].
FBS.5	The security function shall lock an interactive session after [assignment: time interval of user inactivity] by: a) clearing or overwriting display devices, making the current contents unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session.
FBS.6	The security function shall require the following events to occur prior to unlocking the session: [assignment: events to occur].
FBS.7	The security function shall allow user-initiated locking of the user's own interactive session, by: a) clearing or overwriting display devices, making the current contents unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session.
FBS.8	The security function shall terminate an interactive session after a [assignment: time interval of user inactivity].
FBS.9	The security function shall allow user-initiated termination of the user's own interactive session.
FBS.10	Before establishing a user session, the security function shall display an advisory warning message regarding unauthorized use of the module.
FBS.11	Upon successful session establishment, the security function shall display the [selection: date, time, method, location] of the last successful session establishment to the user.
FBS.12	Upon successful session establishment, the security function shall display the [selection: date, time, method, location] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.
FBS.13	The security function shall not erase the access history information from the user interface without giving the user an opportunity to review the information.
FBS.14	The security function shall be able to deny session establishment based on [assignment: attributes].
FBS.15	The security function shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FBS.16	The security function shall permit [selection: the module's security function, another trusted IT product] to initiate communication via the trusted channel.
FBS.17	The security function shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required].
FBS.18	The security function shall provide a communication path between itself and [selection: remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]].
FBS.19	The security function shall permit [selection: the module's security function, local users, remote users] to initiate communication via the trusted path.
FBS.20	The security function shall require the use of the trusted path for [selection: initial user authentication, [assignment: other services for which trusted path is required]].

FBS.21	The organization shall develop, implement, and periodically review and update: 1. A formal, documented, control system security policy that addresses: a. The purpose of the security program as it relates to protecting the organization's personnel and assets; b. The scope of the security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to implement the security policy and associated requirements. A control system security policy considers controls from each of the families contained in this document.
FBS.22	The organization shall establish policies and procedures to define roles, responsibilities, behaviors, and practices for the implementation of an overall security program.
FBS.23	The organization shall define a framework of management leadership accountability. This framework establishes roles and responsibilities to approve cyber security policy, assign security roles, and coordinate the implementation of cyber security across the organization.
FBS.24	Baseline practices that organizations employ for organizational security include, but are not limited to: 1. Executive management accountability for the security program; 2. Responsibility for control system security within the organization includes sufficient authority and an appropriate level of funding to implement the organization's security policy; 3. The organization's security policies and procedures that provide clear direction, accountability, and oversight for the organization's security team. The security team assigns roles and responsibilities in accordance with the organization's policies and confirms that processes are in place to protect company assets and critical information; 4. The organization's contracts with external entities that address the organization's security policies and procedures with business partners, third-party contractors, and outsourcing partners; 5. The organization's security policies and procedures ensure coordination or integration with the organization's physical security plan. Organization roles and responsibilities are established that address the overlap and synergy between physical and control system security risks.
FBS.25	The organization's security policies and procedures shall delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a security incident.
FBS.26	The organization shall hold external suppliers and contractors that have an impact on the security of the control center to the same security policies and procedures as the organization's own personnel; and shall ensure security policies and procedures of second- and third-tier suppliers comply with corporate cyber security policies and procedures if they will impact control system security.
FBS.27	The organization shall establish procedures to remove external supplier access at the conclusion/termination of the contract.
FBS.28	The security function shall monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.

3.2.3. Cryptographic Services (FCS)

Cryptographic services include encryption, signing, key management and key revocation. The security function may employ cryptographic functionality to help satisfy several high-level security objectives. These include, but are not limited to identification and authentication, non-repudiation, trusted path, trusted channel and data separation. This class is used when the security component implements cryptographic functions, the implementation of which could be in hardware, firmware and/or software.

The FCS: Cryptographic support class is composed of two families: Cryptographic key management (FCS_CKM) and Cryptographic operation (FCS_COP). The Cryptographic key management (FCS_CKM) family addresses the management aspects of cryptographic keys, while the Cryptographic operation (FCS_COP) family is concerned with the operational use of those cryptographic keys. [DHS]

FCS.1	The security function shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].
FCS.2	The security function shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: cryptographic key distribution method] that meets the following: [assignment: list of standards].
FCS.3	The security function shall perform [assignment: type of cryptographic key access] in accordance with a specified cryptographic key access method [assignment: cryptographic key access method] that meets the following: [assignment: list of standards].
FCS.4	The security function shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards].
FCS.5	The security function shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].
FCS.6	For information requiring cryptographic protection, the information system shall implement cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

3.2.4. Notification and Signaling Services (FNS)

Notification and signaling services are oriented towards providing system activity information and command result logging.

FNS.1	For [assignment: list of security function devices/elements for which active detection is required], the security function shall monitor the devices and elements and notify [assignment: a designated user or role] when physical or logical tampering with the module's security function's devices or module's security function's elements has occurred.
FNS.2	The security function verifies the correct operation of security utility [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered.
FNS.3	The organization shall verify the correct operation of security functions within the control system upon system startup and restart; upon command by user with appropriate privilege; periodically; and/or at defined time periods. The security function notifies the system administrator when anomalies are discovered.
FNS.4	The security function 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.
FNS.5	The security function shall display an approved, system use notification message before granting system access informing potential users: 1. That the user is accessing a [assignment: organization] information system; 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;

	and 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 associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.
FNS.6	The security function shall perform [assignment: list of specific actions] when replay is detected.

3.2.5. Resource Management Services (FRS)

This section covers resource management services requirements. Resources Management Services include management of runtime resources, such as network/communication paths, processors, memory or disk space (e.g., for audit log capacity), and other limited system resources.

FRS.1	The organization shall develop, disseminate, and periodically review and update: 1. A formal, documented system and communication protection policy that addresses: a. The purpose of the system and communication protection policy as it relates to protecting the organization's personnel and assets; b. The scope of the system and communication protection policy as it applies to all the organizational staff and third-party contractors; c. 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 control system and communication protection policy and associated systems and communication protection controls
FRS.2	The security function shall separate telemetry/data acquisition services from management port functionality.
FRS.3	The security function shall isolate security functions from non-security functions.
FRS.4	The security function shall prevent unauthorized or unintended information transfer via shared system resources.
FRS.5	The security function shall protect against or limits the effects of denial-of-service attacks based on an organization's defined list of types of denial-of-service attacks.
FRS.6	The security function shall limit the use of resources by priority.
FRS.7	The organization shall define the external boundary(ies) of the control system. Procedural and policy security functions 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 control system monitors and manages communications at the operational system boundary and at key internal boundaries within the system.
FRS.10	The security function shall establish a trusted communications path between the user and the system.
FRS.11	When cryptography is required and employed within the system, the organization shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.
FRS.12	The organization shall develop and implement a policy governing the use of cryptographic mechanisms for the protection of control system information. The organization shall ensure all cryptographic mechanisms comply with applicable laws, regulatory requirements, directives, policies, standards, and guidance.
FRS.13	The use of collaborative computing mechanisms on control system is strongly discouraged and provides an explicit indication of use to the local users.

FRS.14	The system shall reliably associate security parameters (e.g., security labels and markings) with information exchanged between the enterprise information systems and the system.
FRS.15	The organization shall issue public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.
FRS.16	The organization shall: 1. Establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the control system if used maliciously; 2. Document, monitor, and manage the use of mobile code within the control system. Appropriate organizational officials should authorize the use of mobile code.
FRS.17	The organization shall: 1. Establish 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 2. Authorize, monitor, and limit the use of VOIP within the control system.
FRS.18	All external system and communication connections shall be identified and adequately protected from tampering or damage.
FRS.19	The system design and implementation shall specify the security roles and responsibilities for the users of the system.
FRS.20	The system shall provide mechanisms to protect the authenticity of device-to-device communications.
FRS.21	The system’s devices that collectively provide name/address resolution services for an organization shall be fault tolerant and implement address space separation.
FRS.22	The system resource (i.e., authoritative DNS server) that provides name/address resolution service shall provide additional artifacts (e.g., digital signatures and cryptographic keys) along with the authoritative DNS resource records it returns in response to resolution queries.
FRS.23	The 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.
FRS.24	The security function shall restrict the ability to [selection: determine the behavior of, disable, enable, modify the behavior of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].
FRS.25	The security function shall enforce the [assignment: access control security function policy(s), information flow control security function policy(s)] to restrict the ability to [selection: change, default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles].
FRS.26	The security function shall ensure that only secure values are accepted for [assignment: list of security attributes].
FRS.27	The security function shall enforce the [assignment: access control security function policy, information flow control security function policy] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the security function policy.
FRS.28	The security function shall allow the [assignment: the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created.
FRS.29	The security function shall use the following rules to set the value of security attributes: [assignment: rules for setting the values of security attributes]
FRS.30	The security function shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of security function data] to [assignment: the authorized identified roles].
FRS.31	The security function shall restrict the specification of the limits for [assignment: list of security function data] to [assignment: the authorized identified roles].

FRS.32	The security function shall take the following actions, if the security function data are at, or exceed, the indicated limits: [assignment: actions to be taken].
FRS.33	The security function shall ensure that only secure values are accepted for [assignment: list of security function data].
FRS.34	The security function shall restrict the ability to revoke [assignment: list of security attributes] associated with the [selection: users, subjects, objects, [assignment: other additional resources]] under the control of the security function to [assignment: the authorized identified roles].
FRS.35	The security function shall enforce the rules [assignment: specification of revocation rules].
FRS.36	The security function shall restrict the capability to specify an expiration time for [assignment: list of security attributes for which expiration is to be supported] to [assignment: the authorized identified roles].
FRS.37	For each of these security attributes, the security function shall be able to [assignment: list of actions to be taken for each security attribute] after the expiration time for the indicated security attribute has passed.
FRS.38	The security function shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the module's security function].
FRS.39	The security function shall maintain the roles [assignment: the authorized identified roles].
FRS.40	The security function shall be able to associate users with roles.
FRS.41	The security function shall maintain the roles: [assignment: authorized identified roles].
FRS.42	The security function shall ensure that the conditions [assignment: conditions for the different roles] are satisfied.
FRS.43	The security function shall require an explicit request to assume the following roles: [assignment: the roles].
FRS.44	The security function shall terminate the network session at the end of a session or after [Assignment: organization-defined time period] of inactivity.

3.2.6. Trust and Certificate Services (FTS)

Description of relationships between entities and the faith placed on the relationship certificates that have uses outside of cryptography for example, material relating to creation, storage, and revocation of certificates.

FTS.1	The security function shall issue public key certificates based on an appropriate certificate policy or obtain public key certificates under an appropriate certificate policy from an [assignment: approved service provider].
FTS.2	When cryptography is required and employed within the security function, the organization shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

3.3. Assurance

3.3.1. Development Rigor (ADR)

Not all solutions are created equal. Differing degrees of care and consideration can go into developing solutions that satisfy any given security requirement. This section contains requirements regarding the activities involved in developing smart grid system solutions. Topics including:

- acquisition issues
- configuration management
- development practices

This is about the creation of smart grid systems, not their deployment, operation, or maintenance.

ADR.1	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
ADR.2	The organization shall schedule, perform, document and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
ADR.3	The organization shall approve, control and monitor the use of information system maintenance tools and maintains the tools on an ongoing basis.
ADR.4	The organization shall authorize, monitor and control any remotely executed maintenance and diagnostic activities, if employed.
ADR.5	The organization shall allow only authorized personnel to perform maintenance on the information system.
ADR.6	The organization shall obtain maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure.
ADR.7	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
ADR.8	The organization shall determine, document and allocate as part of its capital planning and investment control process, the resources required to adequately protect the information system.
ADR.9	The organization shall manage the information system using a system development life cycle methodology that includes information security considerations.
ADR.10	The organization shall include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.
ADR.11	The organization shall obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system.
ADR.12	The organization shall comply with software usage restrictions.
ADR.13	The organization shall enforce explicit rules governing the installation of software by users.
ADR.14	The organization shall design and implement the information system using security engineering principles.
ADR.15	The organization shall: 1. Requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies,

	regulations, standards, guidance, and established service-level agreements; and 2. Monitors security control compliance
ADR.16	The organization shall require that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.
ADR.17	The organization shall require that information system developers create a security test and evaluation plan, implement the plan, and document the results.
ADR.18	The organization shall develop, disseminate and periodically review/update: 1. A formal, documented, system and services acquisition policy that addresses: a. The purpose of the security program as it relates to protecting the organization's personnel and assets; b. The scope of the security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
ADR.19	The organization shall implement a process to determine, document, approve, and allocate the resources required to adequately protect the control system as part of its capital planning and investment control process.
ADR.20	The organization shall manage the control system using a system development life-cycle methodology that includes control system security considerations.
ADR.21	The organization shall include security requirements and/or security specifications, either explicitly or by reference, in control system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.
ADR.22	The organization shall ensure that adequate documentation for the control system and its constituent components are available, protected when required, and are accessible to authorized personnel.
ADR.23	The organization's security program shall deploy policy and procedures to enforce compliance with software license usage restrictions.
ADR.24	The organization shall implement policies and procedures to enforce explicit rules and management expectations governing user installation of software.
ADR.25	The organization shall design and implement the control system using security engineering principles and best practices.
ADR.26	The organization shall ensure that third-party providers of control system services employ adequate security mechanisms in accordance with established service-level agreements and monitor compliance.
ADR.27	The control system vendor shall create and implement a configuration management plan and procedures that limit changes to the control system during design and installation. This plan tracks security flaws. The vendor shall obtain the organization's written approval for any changes to the plan. The vendor shall provide documentation of the plan and its implementation.
ADR.28	The control system vendor shall develop a security test and evaluation plan. The vendor shall submit the plan to the organization for approval and implements the plan once written approval is obtained. The vendor shall then documents the results of the testing and evaluation and submits them to the organization for approval.
ADR.29	The control system vendor shall adopt appropriate software development life-cycle practices to eliminate common coding errors that affect security, particularly with respect to input data validation and buffer management.
ADR.30	The organization shall develop, disseminate, and periodically review and update:

	1. A formal, documented Configuration Management policy that addresses: a. The purpose of the configuration management policy as it relates to protecting the organization’s personnel and assets; b. The scope of the configuration management policy as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure contained in the configuration management policy to ensure compliance with the organization’s security policy and other regulatory commitments 2. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. 3. The personnel qualification levels required to make changes, the conditions under which changes are allowed, and what approvals are required for those changes.
ADR.31	The organization shall develop, document, and maintain a current baseline configuration of the control system and an inventory of the system’s constituent components.
ADR.32	The organization shall authorize, document and manage changes to the control system.
ADR.33	The organization shall implement a process to monitor changes to the control system and conducts security impact analyses to determine the effects of the changes.
ADR.34	The organization shall: 1. Approves individual access privileges and enforces physical and logical access restrictions associated with configuration changes to the control system; 2. Generates, retains, and reviews records reflecting all such changes.
ADR.35	The organization shall: 1. Establishes mandatory configuration settings for IT products employed within the control system; 2. Configures the security settings of control systems technology products to the most restrictive mode consistent with control system operational requirements; 3. Documents the changed configuration settings.
ADR.36	The organization shall configure the control system to provide only essential capabilities and specifically prohibit and/or restrict the use of functions, ports, protocols, and/or services as defined in an organizationally generated “prohibited and/or restricted” list.
ADR.37	The organization shall create and maintains a list of all end-user configurable assets and the configurations of those assets used by the organization.
ADR.38	The organization shall implement policy and procedures to address the addition, removal, and disposal of all control system equipment. All control system assets and information shall be documented, identified and tracked so that their location and function are known.
ADR.39	The organization shall change all factory default authentication credentials on control system components and applications upon installation.
ADR.40	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, control system maintenance 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 control system maintenance policy and associated system maintenance controls.
ADR.41	The organization shall develop policies and procedures to upgrade existing legacy control systems to include security mitigating measures commensurate with the organization’s risk tolerance and the risk to the system and processes controlled.
ADR.42	The organization shall conduct periodic security vulnerability assessments according to the risk management plan. Then, the control system shall be updated to address any identified vulnerabilities in accordance with organization’s control system maintenance policy.
ADR.43	The organization shall make and secure backups of critical system software, applications and data

	for use if the control system operating system software becomes corrupted or destroyed.
ADR.44	The organization shall review and follow security requirements for a control system before undertaking any unplanned maintenance activities of control system components (including field devices). Documentation includes the following: 1. The date and time of maintenance; 2. The name of the individual(s) performing the maintenance; 3. The name of the escort, if necessary; 4. A description of the maintenance performed; 5. A list of equipment removed or replaced (including identification numbers, if applicable).
ADR.45	The organization shall schedule, perform and document routine preventive and regular maintenance on the components of the control system in accordance with manufacturer or vendor specifications and/or organizational policies and procedures.
ADR.46	The organization shall approve, manage, protect and monitor the use of control system maintenance tools and maintains the integrity of tools on an ongoing basis.
ADR.47	The organization shall document authorization and approval policies and procedures and maintains a list of personnel authorized to perform maintenance on the control system. Only authorized and qualified organization or vendor personnel shall perform maintenance on the control system.
ADR.48	The organization shall authorize, manage, and monitor remotely executed maintenance and diagnostic activities on the control system. When remote maintenance is completed, the organization (or control system in certain cases) shall terminate all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization shall change the password following each remote maintenance service.
ADR.49	The organization shall acquire maintenance support and spare parts for key control system components within a specified time period of failure.
ADR.50	The organization shall: 1. Establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and 2. Authorize, monitor, and control the use of mobile code within the information system.
ADR.51	The security function shall separate user data from security function data when such data is transmitted between separate parts of the module.
ADR.52	The organization shall require that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

3.3.2. Organizational Rigor (AOR)

This section contains requirements regarding the policies employed by the organization(s) with access to assets of a deployed smart grid system. These requirements reflect on an organization's ability to continue to operate a smart grid system reliably over time. Topics include

- training procedures
- personnel security
- strategic planning
- monitoring and reviewing security policies

AOR.1	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
AOR.2	The organization shall provide basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [Assignment: organization-defined frequency, at least annually] thereafter.
AOR.3	The organization shall identify personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: 1. Before authorizing access to the system or performing assigned duties; 2. When required by system changes; and 3. [Assignment: organization-defined frequency] thereafter
AOR.4	The organization shall document and monitor individual information system security training activities including basic security awareness training and specific information system security training.
AOR.5	The organization shall establish and maintain contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.
AOR.6	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.
AOR.7	The organization shall restricts access to information system media to authorized individuals.
AOR.8	The organization shall: 1. Affix external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and 2. Exempt [Assignment: organization-defined list of media types or hardware components] from labeling so long as they remain within [Assignment: organization-defined protected environment].
AOR.9	The organization shall physically control and securely store information system media within controlled areas.
AOR.10	The organization shall protect and control information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.
AOR.11	The organization shall sanitize information system media, both digital and non-digital, prior to disposal or release for reuse.
AOR.12	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

AOR.13	The organization shall develop and keep a current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization shall review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].
AOR.14	The organization shall control all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization shall control access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization’s assessment of risk.
AOR.15	The organization shall control physical access to information system distribution and transmission lines within organizational facilities.
AOR.16	The organization shall control physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.
AOR.17	The organization shall monitor physical access to the information system to detect and respond to physical security incidents.
AOR.18	The organization shall control physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.
AOR.19	The organization shall maintain visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: 1. Name and organization of the person visiting; 2. Signature of the visitor; 3. Form of identification; 4. Date of access; 5. Time of entry and departure; 6. Purpose of visit; and 7. Name and organization of person visited. Designated officials within the organization shall review the visitor access records [Assignment: organization-defined frequency].
AOR.20	The organization shall protect power equipment and power cabling for the information system from damage and destruction.
AOR.21	The organization shall provide, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.
AOR.22	The organization shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.
AOR.23	The organization shall employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.
AOR.24	The organization shall employ and maintain fire suppression and detection devices/systems that can be activated in the event of a fire.
AOR.25	The organization shall regularly maintain, within acceptable levels, and monitor the temperature and humidity within the facility where the information system resides.
AOR.26	The organization shall protect the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.
AOR.27	The organization shall authorize and control information system-related items entering and exiting the facility and maintains appropriate records of those items.

AOR.28	The organization shall employ appropriate management, operational, and technical information system security controls at alternate work sites.
AOR.29	The organization shall position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
AOR.30	The organization shall protect the information system from information leakage due to electromagnetic signals emanations.
AOR.31	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.
AOR.32	The organization shall develop and implement a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization shall review and approve the plan
AOR.33	The organization shall review the security plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.
AOR.34	The organization shall establish and make readily available to all information system users, a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization shall receive signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.
AOR.35	The organization shall conduct a privacy impact assessment on the information system in accordance with regulatory and the organization's policy.
AOR.36	The organization shall plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.
AOR.37	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls
AOR.38	The organization shall assign a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization shall review and revise position risk designations [Assignment: organization-defined frequency].
AOR.39	The organization shall screen individuals requiring access to organizational information and information systems before authorizing access.
AOR.40	The organization, upon termination of individual employment, shall terminate information system access, conducts exit interviews, retrieves all organizational information system-related property, and provide appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.
AOR.41	The organization shall review information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions
AOR.42	The organization shall complete appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [Assignment: organization-defined frequency].

AOR.43	The organization shall establish personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.
AOR.44	The organization shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.
AOR.45	The organization shall develop, disseminate, and periodically review and update: 1. A formal, documented, personnel security policy that addresses: a. The purpose of the security program as it relates to protecting the organization’s personnel and assets; b. The scope of the security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization’s security policy and other regulatory commitments; 2. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. 3. Formal procedure to review and document list of approved personnel with access to control systems.
AOR.46	The organization shall assign a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization shall review and revise position risk designations periodically based on the organization’s requirements or regulatory commitments.
AOR.47	The organization shall screen individuals requiring access to the control system before access is authorized.
AOR.48	When an employee is terminated, the organization shall revoke logical and physical access to control systems and facilities and ensure all organization-owned property is returned and that organization-owned documents and/or data files relating to the control system that are in the employee’s possession be transferred to the new authorized owner within the organization. Complete execution of this control shall occur within 24 hours for employees or contractors terminated for cause.
AOR.49	The organization shall review logical and physical access permissions to control systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions. Complete execution of this control shall occur within 7 days for employees or contractors who no longer need to access control system resources.
AOR.50	The organization shall complete appropriate agreements for control system access before access is granted. This requirement applies to all parties, including third parties and contractors, who desire access to the control system. The organization shall review and update access agreements periodically.
AOR.51	The organization shall enforce security controls for third-party personnel and monitors service provider behavior and compliance.
AOR.52	The organization shall employ a formal accountability process for personnel failing to comply with established control system security policies and procedures and clearly documents potential disciplinary actions for failing to comply.
AOR.53	The organization shall provide employees and contractors with complete job descriptions and unambiguous and detailed expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities.
AOR.54	The organization develops, implements, and periodically reviews and updates: 1. A formal, documented physical security policy that addresses: a. The purpose of the physical security program as it relates to protecting the organization’s personnel and assets; b. The scope of the physical security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure of the physical security program to ensure compliance with the organization’s security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the physical and

	environmental protection policy and associated physical and environmental protection controls.
AOR.55	The organization shall develop and maintain lists of personnel with authorized access to facilities containing control systems (except for areas within facilities officially designated as publicly accessible) and issue appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization shall review and approve the access list and authorization credentials at least annually.
AOR.56	The organization shall limit physical access to all control system facilities and assets and verify individual access authorizations before granting access. The organization shall limit access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization’s assessment of risk.
AOR.57	The organization shall monitor physical access to the control system facilities to detect and respond to physical security incidents.
AOR.58	The organization shall limit physical access to control systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.
AOR.59	The organization shall maintain visitor access records to the control system facility (except for those areas within the facility officially designated as publicly accessible) that include: Name and organization of the person visiting; 1. Signature of the visitor; 2. Form of identification; 3. Date of access; 4. Time of entry and departure; 5. Purpose of visit; 6. Name and organization of person visited.
AOR.60	The organization shall retain all physical access logs for as long as dictated by any applicable regulations or based on an organization-defined period by approved policy.
AOR.61	For specific locations within a facility containing concentrations of control system resources (e.g., control centers, server rooms), the organization shall provide the capability of shutting off power to any component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without compromising personnel safety.
AOR.62	The organization shall provide a short-term Uninterruptible Power Supply (UPS) to facilitate an orderly shutdown of non-critical control system components in the event of a primary power source loss.
AOR.63	The organization shall employ and maintain automatic emergency lighting systems that activate in the event of a power outage or disruption and includes lighting for emergency exits and evacuation routes.
AOR.64	The organization shall implement and maintain fire suppression and detection devices/systems that can be activated in the event of a fire.
AOR.65	The organization shall regularly monitors the temperature and humidity within facilities containing control system assets and ensures they are maintained within acceptable levels.
AOR.66	The organization shall protect the control systems from water damage resulting from broken plumbing lines, fire control systems or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.
AOR.67	The organization shall authorize and limit the delivery and removal of control system components (i.e., hardware, firmware, software) from control system facilities and maintain appropriate records and control of that equipment. The organization shall document policies and procedures governing

	the delivery and removal of control system assets in the control system security plan.
AOR.68	The organization shall establish an alternate control center with proper equipment and communication infrastructure to compensate for the loss of the primary control system worksite. The organization shall implement appropriate management, operational, and technical security measures at alternate control centers.
AOR.69	The organization shall monitor and prohibit the use of unapproved portable media use on the control system.
AOR.70	The organization shall implement asset location technologies to track and monitor the movements of personnel and vehicles within the organization's controlled areas to ensure they stay in authorized areas, to identify personnel needing assistance, and to support emergency response.
AOR.71	The organization shall locate control system assets to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
AOR.72	The organization shall protect the control system from information leakage.
AOR.73	The organization shall protect control system power equipment and power cabling from damage and destruction.
AOR.74	The organization shall employ hardware (cages, locks, cases, etc.) to detect and deter unauthorized physical access to control system devices.
AOR.75	The organization shall develop, disseminate, and periodically review and update: 1. A formal, documented, planning policy that addresses: a. The purpose of the strategic planning program as it relates to protecting the organization's personnel and assets; b. The scope of the strategic planning program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities, and management accountability structure of the strategic planning program to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the strategic planning policy and associated strategic planning controls.
AOR.76	The organization shall develop and implement a security plan for the control system that provides an overview of the security requirements for the system and a description of the security measures in place or planned for meeting those requirements. Designated officials within the organization shall review and approve the control system security plan.
AOR.77	The organization shall identify potential interruptions and classify them as to "cause," "effects," and "likelihood."
AOR.78	The organization's control system security plan shall define and communicate the specific roles and responsibilities in relation to various types of incidents.
AOR.79	The organization shall include training on the implementation of the control system security plans for employees, contractors, and stakeholders into the organization's planning process.
AOR.80	The organization shall regularly test security plans to validate the control system objectives.
AOR.81	The organization shall include investigation and analysis of control system incidents in the planning process.
AOR.82	The organization shall include processes and mechanisms in the planning to ensure that corrective actions identified as the result of a cyber security and system incidents are fully implemented.
AOR.83	Risk-reduction mitigation measures shall be planned and implemented and the results monitored to ensure effectiveness of the organization's risk management plan.
AOR.84	The organization shall regularly, at prescribed frequencies, review the security plan for the control system and revise the plan to address system/organizational changes or problems identified during system security plan implementation or security controls assessment.

AOR.85	The organization shall establish and make readily available to all control system users a set of rules that describes their responsibilities and expected behavior with regards to control system usage. The organization shall obtain signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the control system.
AOR.86	The organization shall plan and coordinate security-related activities affecting the control system before conducting such activities to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, or individuals.
AOR.87	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
AOR.88	The organization shall provide basic security awareness training to all control system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and at least annually thereafter. The effectiveness of security awareness training, at the organization level, shall be reviewed at a minimum [assignment: once a year, etc.].
AOR.89	The organization shall identify and train personnel with significant control system security roles and responsibilities. The organization shall document the roles and responsibilities and provide appropriate control system security training before authorizing access to the system, when required by system changes, and with periodic training thereafter.
AOR.90	The organization shall document, maintain, and monitor individual control system security training activities, including basic security awareness training and specific information and control system security training in accordance with the organization's records retention policy.
AOR.91	The organization shall establish, participate with, and maintain contacts with special interest groups, industry vendor forums, specialized public or governmental forums, or professional associations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.
AOR.92	The organization shall document and test the knowledge of personnel on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing the control system.
AOR.93	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, media protection 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 media protection policy and associated media protection controls.
AOR.94	The organization shall ensure that only authorized users have access to information in printed form or on digital media, whether integral to or removed from the control system.
AOR.95	The organization shall review and classify all removable information storage media and the control system output to determine distribution limitations [assignment: public, confidential, classified, etc.].
AOR.96	The organization shall affix external labels to removable information system media and to the control system output that indicate the distribution limitations [assignment: public, confidential, classified, etc.] and handling caveats of the information. The organization may exempt specific types of media or hardware components from labeling as long as they remain within a secure environment (as defined by the organization).
AOR.97	The organization shall physically manage and securely store control system media within protected areas. The sensitivity of the material delineates how the media is stored.
AOR.98	The organization shall develop security measures for paper and digital media extracted from the control system and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.

AOR.99	The organization shall sanitize control system digital and non-digital media, before disposal or release for reuse.
AOR.100	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, monitoring and reviewing control system security 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 monitoring and reviewing control system security management policy and associated audit and accountability controls.
AOR.101	The organization's security program shall implement continuous improvement practices to ensure that industry lessons-learned and best practices are incorporated into control system security policies and procedures.
AOR.102	The organization shall include a process for monitoring and reviewing the performance of their cyber security policy.
AOR.103	The organization shall incorporate industry best practices into the organization's security program for control systems.
AOR.104	The organization shall authorize (i.e., accredit) the control system for processing before operations and periodically updates the authorization based on organization-defined frequency or when there is a significant change to the system. A senior organizational official shall sign and approve the security accreditation.
AOR.105	The organization shall conduct an assessment of the security mechanisms in the control system to determine the extent to which the security measures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
AOR.106	The organization shall establish policies and procedures to define roles, responsibilities, behaviors, and practices for the implementation of an overall security program.
AOR.107	The organization shall define a framework of management leadership accountability. This framework establishes roles and responsibilities to approve cyber security policy, assign security roles, and coordinate the implementation of cyber security across the organization.
AOR.108	Baseline practices that the organization shall employ for organizational security include, but are not limited to: 1. Executive management accountability for the security program; 2. Responsibility for control system security within the organization includes sufficient authority and an appropriate level of funding to implement the organization's security policy; 3. The organization's security policies and procedures that provide clear direction, accountability, and oversight for the organization's security team. The security team assigns roles and responsibilities in accordance with the organization's policies and confirms that processes are in place to protect company assets and critical information; 4. The organization's contracts with external entities that address the organization's security policies and procedures with business partners, third-party contractors, and outsourcing partners; 5. The organization's security policies and procedures ensure coordination or integration with the organization's physical security plan. Organization roles and responsibilities are established that address the overlap and synergy between physical and control system security risks.
AOR.109	The organization's security policies and procedures shall delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a security incident.
AOR.110	The organization shall hold external suppliers and contractors that have an impact on the security of the control center to the same security policies and procedures as the organization's own personnel. The organization shall ensure security policies and procedures of second- and third-tier suppliers comply with corporate cyber security policies and procedures if they will impact control system security.

AOR.111	The organization shall establish procedures to remove external supplier access at the conclusion/termination of the contract.
AOR.112	The organization shall: 1. Establish 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 2. Authorize, monitor, and control the use of VoIP within the information system.
AOR.113	The organization shall display an approved system use notification (message) before granting access to the system.
AOR.114	The organization shall develop a formal written policy and appropriate security procedures to address and protect against the risks of remote access to the system, field devices, and communication facilities.
AOR.115	The organization shall restrict the use of personally owned information copied to the system or system user workstation that is used for official organization business. This includes the processing, storage, or transmission of organization business and critical 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 organization's system; 2. The maximum security category of information that can processed, stored, and transmitted; 3. How other users of the personally owned system 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).
AOR.116	The organization shall develop, disseminate and periodically review and update: 1. A formal, documented identification policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the identification policy and associated identification controls.
AOR.117	The organization shall develop, disseminate, and periodically review and 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.
AOR.118	The organization shall manage system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews system accounts at least [assignment: period of time (e.g., annually)].
AOR.119	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the accountability policy and associated audit and accountability controls.
AOR.120	The organization shall regularly review and analyze information system audit records: 1. For indications of inappropriate or unusual activity 2. To investigate suspicious activity or suspected violations 3. To report findings to appropriate officials, and 4. Take necessary actions.

AOR.121	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.
AOR.122	The organization's audit program shall specify auditor qualifications in accordance with the organization's documented training program.
AOR.123	The organization under the audit program shall specify strict rules and careful use of audit tools when auditing control system functions.
AOR.124	The organization shall demonstrate compliance to the organization's security policy through audits in accordance with the organization's audit program.

3.3.3. Handling/Operating Rigor (AHR)

This section contains requirements regarding the activities involved in the day-to-day operation of deployed smart grid systems. Topics include

- information and document management policies
- incident response procedures
- maintenance procedures
- physical and environmental security
- media protection

AHR.1	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
AHR.2	The organization shall develop and implement a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization shall review and approve the contingency plan and distribute copies of the plan to key contingency personnel.
AHR.3	The organization shall train personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].
AHR.4	The organization shall: 1. Test and/or exercise the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and 2. Review the contingency plan test/exercise results and initiates corrective actions.
AHR.5	The organization shall review the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

AHR.6	The organization shall identify an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.
AHR.7	The organization shall identify an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable.
AHR.8	The organization shall identify primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.
AHR.9	The organization shall conduct backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and protects backup information at the storage location.
AHR.10	The organization shall employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.
AHR.11	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
AHR.12	The organization shall train personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].
AHR.13	The organization shall test and/or exercise the incident response capability for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.
AHR.14	The organization shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
AHR.15	The organization tracks and documents information system security incidents on an ongoing basis.
AHR.16	The organization promptly reports incident information to appropriate authorities.
AHR.17	The organization shall provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incident (The support resource is an integral part of the organization's incident response capability).
AHR.18	The organization shall develop, disseminate and periodically review/update: 1. A formal, documented, control 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 control system information and document management policy and associated system maintenance controls.
AHR.19	The organization shall manage control system related data, including establishing retention policies and procedures for both electronic and paper data, and manages access to the data based on formally assigned roles and responsibilities.
AHR.20	Organization implemented policies and procedures detailing the handling of information shall be developed and periodically reviewed and updated.
AHR.21	All information shall be classified to indicate the protection required commensurate with its sensitivity and consequence.
AHR.22	Formal contractual and confidentiality agreements shall be established for the exchange of

	information and software between the organization and external parties.
AHR.23	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 the control system.
AHR.24	The organization shall develop policies and procedures that provide details of the retrieval of written and electronic records, equipment, and other media for the control system in the overall information and document management policy.
AHR.25	The organization shall develop policies and procedures detailing the destruction of written and electronic records, equipment, and other media for the control system, without compromising the confidentiality of the data.
AHR.26	The organization shall perform periodic reviews of compliance with the control system information and document security management policy to ensure compliance with any laws and regulatory requirements.
AHR.27	The control system shall automatically marks data output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.
AHR.28	The control system shall automatically label information in storage, in process and in transmission.
AHR.29	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
AHR.30	The organization shall develop and implement a continuity of operations plan dealing with the overall issue of maintaining or re-establishing production in case of an undesirable interruption for a control system. The plan shall address roles, responsibilities, assigned individuals with contact information, and activities associated with restoring system operations after a disruption or failure. Designated officials within the organization shall review and approve the continuity of operations plan.
AHR.31	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 control system incidents.
AHR.32	The organization shall train personnel in their continuity of operations plan roles and responsibilities with respect to the control system. The organization shall provide refresher training at least annually. The training covers employees, contractors, and stakeholders in the implementation of the continuity of operations plan.
AHR.33	The organization shall test the continuity of operations plan to determine its effectiveness and documents the results. Appropriate officials within the organization shall review the documented test results and initiate corrective actions if necessary. The organization shall test the continuity of operations plan for the control 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.
AHR.34	The organization shall review the continuity of operations plan for the control system at least annually and updates the plan to address system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing.
AHR.35	The organization shall implement control system incident handling capabilities for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
AHR.36	The organization shall track and document control system network security incidents on an ongoing basis.
AHR.37	The organization shall promptly report cyber and control system security incident information to the appropriate authorities.

AHR.38	The organization shall provide an incident response support resource that offers advice and assistance to users of the control system for the handling and reporting of security incidents (The support resource is an integral part of the organization's incident response capability).
AHR.39	The organization shall document its policies and procedures to show that investigation and analysis of incidents are included in the planning process. The procedures shall ensure that the control system is capable of providing event data to the proper personnel for analysis and for developing mitigation steps. The organization shall ensure that a dedicated group of personnel is assigned to periodically review the data at a minimum monthly.
AHR.40	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.
AHR.41	The organization shall identify an alternate storage site and initiates necessary agreements to permit the storage of control system configuration information.
AHR.42	The organization shall identify alternate command/control methods for the control system and initiates necessary agreements to permit the resumption of operations for the safe operation of the control system within an organization-defined time period when the primary system capabilities are unavailable.
AHR.43	The organization shall identify an alternate control center, necessary telecommunications, and initiates necessary agreements to permit the resumption of control system operations for critical functions within [assignment: an organization-prescribed time period] when the primary control center is unavailable.
AHR.44	The organization shall conduct backups of critical control system information, including state of the user-level and system level information, process formulas, system inventories, etc., contained in the control system, on a regular schedule as defined by the organization, and stores the information at an appropriately secured location.
AHR.45	The organization shall employ mechanisms with supporting procedures to allow the control system to be recovered and reconstituted to the system's original state after a disruption or failure.
AHR.46	The control system shall have the ability to execute an appropriate fail safe procedure upon the loss of communications with the control system or the loss of the control system itself.
AHR.47	The organization shall retain audit records for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

3.3.4. Accountability (AAY)

"Security auditing involves recognizing, recording, storing, and analyzing information related to security relevant activities (i.e. activities controlled by the TSF). The resulting audit records can be examined to determine which security relevant activities took place and whom (which user) is responsible for them." [CC]

AAY.1	The organization shall manage control system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization shall review control system accounts [assignment: time period (e.g., at least annually)].
AAY.3	The organization shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization shall review information system accounts [Assignment: organization-defined frequency, at least annually].
AAY.4	The information system shall enforce a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] time period. The information system automatically [Selection: locks the account/node for an [Assignment: organization-defined time period], delays next login prompt according to [Assignment: organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is

	exceeded.
AAY.5	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; and 2. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
AAY.6	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.
AAY.7	The control system shall generate audit records, at a minimum, for the following events whether or not the attempts were successful: 1. Attempts to logon; 2. Attempts to change local account attributes such as privileges; 3. Attempts to change local security policy.
AAY.8	The organization shall develop, implement, and periodically review and update: 1. A formal, documented, control system security policy that addresses: a. The purpose of the security program as it relates to protecting the organization's personnel and assets; b. The scope of the security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization's security policy and other regulatory commitments. 2. Formal, documented procedures to implement the security policy and associated requirements. A control system security policy considers controls from each of the families contained in this document.
AAY.9	The organization shall define a framework of management leadership accountability. This framework establishes roles and responsibilities to approve cyber security policy, assign security roles, and coordinate the implementation of cyber security across the organization.
AAY.10	Baseline practices that organizations employ for organizational security shall include, but are not limited to: 1. Executive management accountability for the security program; 2. Responsibility for control system security within the organization includes sufficient authority and an appropriate level of funding to implement the organization's security policy; 3. The organization's security policies and procedures that provide clear direction, accountability, and oversight for the organization's security team. The security team assigns roles and responsibilities in accordance with the organization's policies and confirms that processes are in place to protect company assets and critical information; 4. The organization's contracts with external entities that address the organization's security policies and procedures with business partners, third-party contractors, and outsourcing partners; 5. The organization's security policies and procedures ensure coordination or integration with the organization's physical security plan. Organization roles and responsibilities are established that address the overlap and synergy between physical and control system security risks.
AAY.11	The organization shall develop, disseminate, and periodically review and update: 1. A formal, documented system and communication protection policy that addresses: a. The purpose of the system and communication protection policy as it relates to protecting the organization's personnel and assets; b. The scope of the system and communication protection policy as it applies to all

	the organizational staff and third-party contractors; c. 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 control system and communication protection policy and associated systems and communication protection controls.
AAY.12	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, system and services acquisition policy that addresses: a. The purpose of the security program as it relates to protecting the organization’s personnel and assets; b. The scope of the security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure of the security program to ensure compliance with the organization’s security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
AAY.13	The organization shall develop, disseminate, and periodically review and update: 1. A formal, documented Configuration Management policy that addresses: a. The purpose of the configuration management policy as it relates to protecting the organization’s personnel and assets; b. The scope of the configuration management policy as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure contained in the configuration management policy to ensure compliance with the organization’s security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. 3. The personnel qualification levels required to make changes, the conditions under which changes are allowed, and what approvals are required for those changes.
AAY.14	The organization shall develop, disseminate, and periodically review and update: 1. A formal, documented, personnel security policy that addresses: a. The purpose of the security program as it relates to protecting the organization’s personnel and assets; b. The scope of the security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities, and management accountability structure of the security program to ensure compliance with the organization’s security policy and other regulatory commitments; 2. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. 3. Formal procedure to review and document list of approved personnel with access to control systems.
AAY.15	The organization shall employ a formal accountability process for personnel failing to comply with established control system security policies and procedures, and clearly document potential disciplinary actions for failing to comply.
AAY.16	The organization shall develop, implement, and periodically review and update: 1. A formal, documented physical security policy that addresses: a. The purpose of the physical security program as it relates to protecting the organization’s personnel and assets; b. The scope of the physical security program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities and management accountability structure of the physical security program to ensure compliance with the organization’s security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection

	controls.
AAY.17	The organization shall develop, disseminate, and periodically review and update: 1. A formal, documented, planning policy that addresses: a. The purpose of the strategic planning program as it relates to protecting the organization’s personnel and assets; b. The scope of the strategic planning program as it applies to all the organizational staff and third-party contractors; c. The roles, responsibilities, and management accountability structure of the strategic planning program to ensure compliance with the organization’s security policy and other regulatory commitments. 2. Formal, documented procedures to facilitate the implementation of the strategic planning policy and associated strategic planning controls.
AAY.18	The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, monitoring and reviewing control system security 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 monitoring and reviewing control system security management policy and associated audit and accountability controls.
AAY.19	Baseline practices that the organization employs for organizational security shall include, but are not limited to: 1. Executive management accountability for the security program; 2. Responsibility for control system security within the organization includes sufficient authority and an appropriate level of funding to implement the organization’s security policy; 3. The organization’s security policies and procedures that provide clear direction, accountability, and oversight for the organization’s security team. The security team assigns roles and responsibilities in accordance with the organization’s policies and confirms that processes are in place to protect company assets and critical information; 4. The organization’s contracts with external entities that address the organization’s security policies and procedures with business partners, third-party contractors, and outsourcing partners; 5. The organization’s security policies and procedures ensure coordination or integration with the organization’s physical security plan. Organization roles and responsibilities are established that address the overlap and synergy between physical and control system security risks.

3.3.5. Access Control (AAC)

"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 activity. 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 device, as a prerequisite for granting access to resources in a control system. Identification could be a password, a token, or a fingerprint. Authentication is the challenge process to prove (validate) the identification provided. An example would be using a fingerprint (identification) to access a computer via a biometric device (authentication). The biometric device authenticates the identity of the fingerprint." [DHS]

AAC.1	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.
AAC.2	The organization shall supervise and review the activities of users with respect to the enforcement and usage of control system access control.
AAC.3	The security function shall enforce the [assignment: access control security function policy] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the security function policy].
AAC.4	The security function shall enforce the [assignment: access control security function policy] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the security function policy.
AAC.5	The security function shall ensure that all operations between any subject controlled by the security function and any object controlled by the security functionare covered by an access control security function policy.
AAC.6	The security function shall enforce the [assignment: access control security function policy] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated security function policy, and for each, the security function policy-relevant security attributes, or named groups of security function policy-relevant security attributes].
AAC.7	The security function shall enforce the [assignment: access control security function policy(s) and/or information flow control security function policy(s)] when exporting user data, controlled under the security function policy(s), outside of the module.
AAC.8	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; and 2. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
AAC.9	The organization shall supervise and review the activities of users with respect to the enforcement and usage of information system access controls.
AAC.10	The security function shall enforce the [assignment: access control security function policy(s), information flow control security function policy(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles].
AAC.11	The security function shall enforce the [assignment: access control security function policy, information flow control security function policy] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the security function policy.
AAC.12	The organization shall review logical and physical access permissions to control systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions. Complete execution of this control occurs within [Assignment: time period (e.g., 7 days)] for employees or contractors who no longer need to access control system resources.
AAC.13	The organization shall supervise and review the activities of users with respect to the enforcement and usage of system access control.

Appendix A: Architectural Description

This appendix contains information that is non-formative to the architecture of AMI security, but provides useful background and understanding.

A.1. Scope

Advanced Metering Infrastructure (AMI) Security Architecture as defined by the AMI-SEC taskforce is:

The communications hardware and software and associated system and data management software that creates a network between advanced meters and utility business systems and which allows collection and distribution of information to customers and other parties such as competitive retail providers, in addition to providing it to the utility itself. AMI is further defined as: 1) The hardware and software residing in, on, or closest to the customer premise for which the utility or its legal proxies are primarily responsible for proper operation; and 2) The hardware and software owned and operated by the utility or its legal proxies which has as its primary purpose the facilitation of Advanced Metering.

The goal of this document is to describe the abstract (logical, platform-agnostic) mitigation plan for addressing requirements identified in the Risk Assessment / System Requirements Document.

The following approach has been taken in designing the system:

Approach

- Architectural Representation of Security Systems
- Logical Function Descriptions
- System, Subsystem, and Function Boundaries
- Reference: IEEE 1471-2000

This document is intended to focus on security architecture, and is not intended to cover enterprise level AMI architecture, except to describe a security concept. The objective of architecting is to decompose the system into its primary views in order to describe the system enough to complete the mission of AMI security. The architecture does not extend beyond the external visible properties of the elements of the system. That is, non-visible properties are left to the designers, implementers and integrators of the system.

The following image represents the 10,000 foot view of AMI. This document begins by explaining the interactions between external actors and the AMI system (see section 3.1). The next view zooms in on the AMI system by describing the system with a decomposition view (section 3.2). Each iteration provides deeper granularity and traceability between views.

AMI-SEC is developing other relevant documentation in parallel that supports the Architectural Description (AD) including the AMI Risk Analysis and System Security Requirements (SSR) documents. The Risk Analysis walks the utility through a method of determining a risk-to-value of an asset. Assets in terms of these documents are considered to be the business level value streams to the utility. The appendix of the AMI Risk Analysis includes catalogues for assets, vulnerabilities, and threats. The SSR document includes AMI-SEC's approach to conducting a requirements assessment and applying requirements. Traceability between views in the AD and requirements defined in the SSR are maintained for consistency and rationale.

This document develops security around commonly known AMI use cases selected from use cases shared by utilities to AMI-SEC. It is assumed that AMI will evolve supporting additional uses and variants, but these uses cannot be predicted. Therefore, a goal of this AD is to group use cases that possess commonality in security treatment in order to support the evolution of AMI.

A.2. Mission

The mission of the AMI Security Architecture is to provide understanding of AMI security, communication among stakeholders and serve as a basis for system analysis. It is important to understand that the task of this architecture is not to provide the groundwork to build the entire AMI system, but to secure it, which is inherently nontrivial.

The information contained in this document will provide an introduction to AMI Security to interested parties. Newcomers will find this document a starting point for understanding the elements, interfaces, and structure of AMI security.

This document will serve to provide communication among stakeholders including designers of the system, implementers, integrators, testers and operators. All architecture is design, but not all design is considered architecture. The mission in communication is to produce sufficient guidance for stakeholders so that they understand the architecture well enough to perform their role.

The architecture will also serve to provide information needed the support analysis performed for security objectives including availability, integrity, confidentiality, access control and accounting.

The architecture will cross-check with information contained in the Requirements document to provide reasoning for requirements selection.

A.3. Stakeholders & Concerns

This section describes the stakeholders and their concerns. A stakeholder is any individual or group of individuals with interests or concerns associated with the system. All actors of the system are stakeholders, but not all stakeholders are actors. For example, an investor may have a stake in the success of the AMI system, but may not interact directly with the AMI system.

Stakeholders identified to be relevant to the security architecture are:

- Customer Users of the system
- Operators of the system
- Responsible Entities of the systems
- Developers of the system
- Implementers of the system
- Maintainers of the system

Concerns that stakeholders may have from a security perspective for the entire AMI system

General Stakeholder Concerns:

- Integrity of the system
- Availability of the system

- Confidentiality of the system
- The purpose or missions of the system as pertains to security
- The appropriateness of the system for use in fulfilling its missions to security
- The feasibility of constructing the system
- The risks of system development and operation to users, acquirers, and developers of the system
- Maintainability, deploy-ability, and evolve-ability of the system

Each viewpoint defined for AMI security possesses specific concerns defined with each viewpoint under the following section.

Potential examples of AMI security concerns by stakeholders:

STAKEHOLDER	SECURITY CONCERN
Residential Customer	Privacy
Utility Operator	Integrity of information and system control
Regulators	Integrity of system and compliance with regulations
Telecom Provider	Compliance with contractual obligations and regulations

Table 10 – Stakeholder Security Concerns

A.4. Security Analysis Approach

The security analysis approach is to evaluate each view under the security principles of availability, integrity, confidentiality, access control and accountability. The high level models are in the form of Use Cases. At least one security objective is identified with each Use Case by evaluating against these security principles.

- Availability
  - Ensure the desired resource is available at the time it is needed.
  - Ensure the desired resource is accessible in the intended manner by the appropriate entity.
- Integrity
  - Ensure the desired resource contains accurate information.
  - Ensure the desired resource performs precisely as intended.
- Confidentiality
  - Ensure the desired resource is only accessible to the desired targets.
  - Ensure the desired resource is only accessible under the designated conditions.
- Access Control
  - Ensure resource access follows the designated procedure.

  - Ensure access mechanisms provide sufficient management capabilities to establish, modify, and remove desired criteria.

- Accountability
  - Ensure system activities can be reconstructed, reviewed, and examined from transaction inception to output of final results.
  - Ensure system controls are provably compliant with established policy and procedures.

A.5. Architecture Description Approach

This section is an introduction to the approach of describing the AMI architecture based on IEEE 1471-2000, *IEEE Recommended Practice for Architectural Description of Software-Intensive Systems*. This section serves as a Roadmap for appendix A and provides a guide for where to locate information.

This section introduces templates and patterns that will be used in subsequent sections. Each view describes:

- What viewpoint it realizes
  - Name & definition of the viewpoint (external pointer or brief definition)
  - What stakeholders and concerns it addresses (and to what extent)
  - Language/notation to be used
- One or more models, where a model includes:
  - Context diagram (i.e., how it relates to AMI as a whole or to other models within the same view)
  - A picture or other primary presentation, always with a key or legend
  - Brief descriptions (or pointers to such) for each element and relation type in the primary presentation
  - Related models, such as scenarios related to the view
  - Known or anticipated variations (likely very important here)
  - Rationale, assumptions, or other background for the decisions depicted in the view

A.5.1. Viewpoints

IEEE 1471-2000 describes a viewpoint on a system as – “a form of abstraction achieved using a selected set of architectural constructs and structuring rules, in order to focus on particular concerns within a system. The relationship between viewpoint and view is analogous to that of a template and an instance of that template.” Therefore, a viewpoint may contain:

- Specifications of each viewpoint that has been selected to organize the representation of the architecture and the rationale for those selections
- One or more architectural views

- A record of all known inconsistencies among the architectural description's required constituents
- A rationale for selection of the architecture

Each viewpoint shall be specified by:

1. A viewpoint name,
2. The stakeholders to be addressed by the viewpoint,
3. The concerns to be addressed by the viewpoint,
4. The language, modeling techniques, or analytical methods to be used in constructing a view based upon the viewpoint,
5. The source, for a library viewpoint (the source could include author, date, or reference to other documents, as determined by the using organization).

A viewpoint specification may include additional information on architectural practices associated with using the viewpoint, as follows:

- Formal or informal consistency and completeness tests to be applied to the models making up an associated view
- Evaluation or analysis techniques to be applied to the models
- Heuristics, patterns, or other guidelines to assist in synthesis of an associated view

Viewpoint specifications may be incorporated by reference (such as to a suitable recommended practice or previously defined practice). An architectural description shall include a rationale for the selection of each viewpoint. The rationale shall address the extent to which the stakeholders and concerns are covered by the viewpoints selected.

A.5.2. Views

An architectural description is organized into one or more constituents called (architectural) views. Each view addresses one or more of the concerns of the system stakeholders. The term view is used to refer to the expression of a system's architecture with respect to a particular viewpoint.

The relationship between viewpoint and view is analogous to that of a template and an instance of that template. The *viewpoint* is the template and the *view* is the instance of the template.

A.6 Contextual View

The primary goal of this view is to identify the external points of interaction (physical and logical/data) between AMI and anything outside of AMI. Once these points of interaction are defined, security architecture is developed to address the concerns of the stakeholders involved. Use cases are used to model customer, third party and utility interactions with AMI in sections 2.1.2, 2.1.3 and 2.1.4.
Elaborations of the interactions in this view are unlikely to be complete; they should however provide representative examples of –

- Use cases of the outside world interacting with (stimulating) AMI
- Use cases of AMI interacting with (stimulating) the outside world
- Misuse or abuse cases in either direction; that is, specific uses that should be prevented
- Any actor sub-categories where the actor uses the system in a fashion that implies security needs that differ from major actors (e.g., leading to identification of access domains/privilege levels)
- Physical interactions (e.g., installing a meter or physical access to assets like collectors)
- Logical interactions (e.g., user monitors or modifies settings with the utility via web browser or utility initiates a demand-response interaction with a residence)

Elements of the view are the AMI system (as a black box), human actors, and connected systems. Relations of the view are vague - "interacts with", with elaboration in the prose.

A.7 Top Level Model

The top level model represents a high level view of the external stakeholders that interact with the AMI system. This model is used to provide an understanding of security concerns of interaction with AMI for these stakeholders.

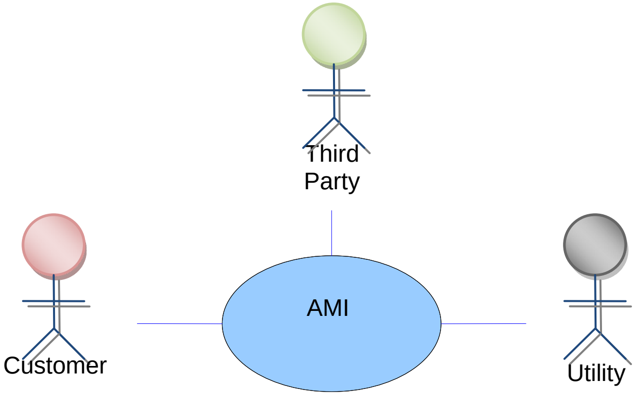

Figure 4 – AMI Top Level Model

General security interaction needs:

- Customers are the consumers of AMI services and have a primary desire of availability and privacy from AMI and service value.
- Third Parties manage AMI resources with delegated authority from the Customer or Utility through an established trust relationship.
- Utilities provide AMI services and primary desire reliably gather information from the Customer to support the availability, resiliency and survivability of the electric grid.

Constraints:

- Bandwidth – current technologies have limited bandwidth for providing security services (examples: encryption, network management services).

- Latency – the time between when data is requested or generated and the time it is received. In many cases, data is only useful if received within a specific window of time.
- Storage – devices that store information either persistently or stage data temporarily are limited in the amount of data they are capable of storing at any given time.
- Processing – the rate at which a device can process information. It is important to keep in mind cryptographic functions require additional processing horsepower above normal processor usage.

A.7.1. Customer Model

The customer model focuses on the interactions between a customer and the AMI system. Customers may include sub-actors such as:

- Residential Customer (Private home owners)
- Commercial Customer (Office buildings, Apartment Complexes)
- Industrial Customer (Manufacturing plants)
- Municipalities Customer (Street lights, traffic lights, subways)

Sub-actors may be considered in the instance that there is different security treatment applied based on the role a sub-actor plays. If the security treatment of all sub-actors is the same or similar then the group is treated as a whole. The differentiating properties are identified in the cases where sub-actors only differ slightly in the treatment of security. The following diagram represents the relationship between the customer and AMI system where the customer may perform a stimulus on the AMI system or vice versa.

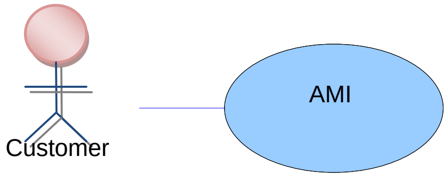

Figure 5 - Customer Model

The following use cases are used to define the relationship between the customer and AMI:

Customer reduces their usage in response to pricing or voluntary load reduction event:

- The utility can notify customers through the AMI system that demand reduction is requested for the purposes of either improving grid reliability, performing economic dispatch (energy trading), or deferring buying energy.

  There are two levels of advanced warning which are envisioned for AMI demand response systems as outlined in Distribution Use Case 2. The first being predicted energy shortages—a few hours notice in advanced—and the emergency shortages—minute to sub-minute notices.

  Security Objective:

  - Prevent false warnings from reaching the customer.

    - Ensure that only people and/or systems that are authorized by the utility can send warnings to the customer
    - Ensure that the system is resilient to periods of over-subscribed network utilization, especially in the case of emergency shortages.

- **Customer has access to recent energy usage and cost at their site:**
- Customers can view a variety of information being gathered by their meter, permitting them to make energy-efficient choices and to shift demand to off-peak periods. Customers may access this information through a variety methods.

  Security Objective:

    - Protect the variety of methods of access from unauthorized access by unauthorized persons outside of the site.
    - Protect the confidentiality of the usage and data associated with a particular customer or site.
    - Protect the devices that communicate the usage and cost data from tampering.
    - Validate that the communication of the usage and cost data is in a manner that is consistent with the utilities intent. For example, display only "need to know" data; ensure that all displayed data is consistent with respect to reality.

Customer prepays for electric services:

- Customers of the AMI system can prepay their accounts and read their current balance. Pre-pay may be done through the internet, phone, or other method.

  Security Objective:

    - Compliance with PCI or other applicable standard is required by utilities or financial entities
    - Ensure that the AMI system and/or payment devices are resistant to payment fraud of many types
    - Ensure that payment data confidentiality is maintained

External clients use the AMI system to interact with devices at customer site:

- The Advanced Meter Infrastructure (AMI) will enable third parties, such as energy management companies, to use the communication infrastructure as a gateway to monitor and control customer equipment located at the customer's premise. The AMI will be required to enable on-demand requests and support a secure environment for the transmission of customer confidential information.

  Security Objective:

    - Ensure that all third-parties agree to some standard of data confidentiality agreement.
    - Ensure that all third-parties agree to some standard of granting access to systems which allow access to monitor and control customer equipment at the premise.

- Ensure that all communications that result in an action with equipment at a customer premise is authorized, authenticated, non-repudiated, logged.
- Ensure that the communication path to a customer premise that allows control of equipment is secured and tamper proof.
- Ensure that customers are required to agree to specific third-party access to their premise gateway.

A.7.2. Third Party Model

The third party model represents the interaction between third parties and the AMI system. Third parties include utility contracted organizations such as a telecom provider, other utility, etc. Third parties may also include organizations that have established contracts with the customer for managing their premise devices within the home area network, for example an energy management system.

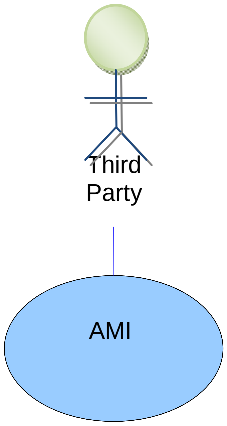

Figure 6 - Third Party Model

The following are use cases describing the relationships between potential third parties and the AMI system.

Multiple Clients Read Demand and Energy Data Automatically from Customer Premises:

- The AMI system can be used to permit gas and water utilities, contract meter readers, aggregators and other third parties to read electrical meters, read gas and water meters, or control third-party equipment on customer premises.

  Security Objective:

  - To protect customer information. Customer grants the right to what information is disseminated and to whom.
  - To maintain integrity of meter data. Meter data should be protected from manipulation or deletion.
  - To establish timely availability of the meter data to the clients for direct scheduled and non-scheduled reads.

A.7.3. Utility Model

The utility model describes interactions between the Utility stakeholder and the AMI system in order to describe the security treatments that need to be applied.

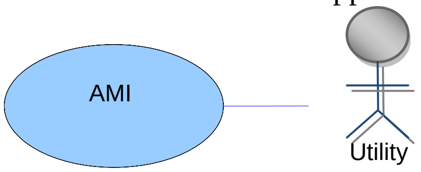

Figure 7 - Utility Model

Utility stakeholder security concerns about AMI:

- Loss of competitive advantage
- Loss of billing integrity
- Service degraded
- Increased cost
- Regulatory compliance

The following are use cases describing the relationships between the Utility and AMI.

Remote Meter Reads

- The AMI system permits the utility to remotely read meter data in intervals so that customers may be billed on their time of use, and demand can therefore be shifted from peak periods to off-peak periods, improving energy efficiency.

  Security Objective:

  - To maintain privacy of customer information in transit and within temporary and permanent memory storage.
  - To protect meter data from manipulation or deletion.
  - To provide timely availability of meter data.

Remote Connect / Disconnect

- The AMI system permits customers' electrical service to be remotely connected or disconnected for a variety of reasons, eliminating the need for utility personnel to visit the customer premises.

  Security Objective:

  - To protect integrity of connect/disconnect control messages; avoiding fake messages, fake senders, unintended receivers, manipulated messages
  - To establish a secure connection in transporting connect/disconnect control messages
  - To establish timely connectivity to connect/disconnect service

- It should also provide an efficient way in which to initiate/terminate a service agreement between customer and utility via remote switching service(on/off)

  Security Objective:

  - To establish timely connectivity to connect/disconnect service

- Posses the ability to remotely limit customer usage as a response to constrained supply as well as the customer's inability to pay the cost for the service

  Security Objective:

  - To protect integrity of connect/disconnect/limit control messages; avoiding fake messages, fake senders, unintended receivers, manipulated messages
  - To establish a secure connection in transporting connect/disconnect/limit control messages

- In addition to the aforementioned the following business transactions should also be made available to the customer and utility:

  - Routine shut-off of service (move out)
  - Routine turn-on of service (move in)
  - Credit & Collections termination of service
  - Local/on site shut-off of service
  - Local/on site turn-on of service
  - Credit and Collection Service Limiting

  Security Objective:

  - To establish timely connectivity to connect/disconnect/limit service
  - To produce historical, non-reputable record of event

Energy Theft

- The AMI system can be used to report when customers are stealing energy or tampering with their meter.

  Security Objective:

  - To produce reliable tamper indication
  - To successfully transmit and receive a tamper signal
  - To securely transmit tamper signal from a non-reputable source

Outage Management

- The AMI system can be used to report outages with greater precision than other sources, or verify outage reports from other sources.

  Security Objective:

Power Quality Analysis

- The AMI system can be used to analyze the quality of electrical power by reporting harmonic data, RMS variations, Voltage and VARs, and can communicate directly with distribution automation networks to improve power quality and fault recovery times.

  Security Objective:

  - To maintain integrity of meter data sent; avoid manipulation and deletion
  - To security meter data being transmitted; avoid customer's private data being released or intercepted
  - To maintain availability of quality analysis information

Distributed Generation Management

- The AMI system can be used to dispatch, measure, regulate and detect distributed generation by customers.

  Security Objective:

  - To maintain integrity of AMI data being transmitted and stored to avoid manipulation and deletion
  - To provide timely availability to system data

- Additional benefits include, but are not limited, to the following:
  - An increase in customer's willingness to participate in a load management program with the utilities
  - Provides a channel of communication from utility to load management devices
  - Reduction in the costs associated with the installation of AMI system components which would enable customer-provided distributed generation (this could increase customer's willingness to participate as well since there wouldn't be any out of pocket costs for the customer)
  - Creates an avenue for the utilities to dispatch and monitor those participants in distributed generation

  Security Objective:

  - To protect confidentiality of customer's data and maintain customer trust

Optimizing Lifetime of Network

- With the advent of new communications, in particular: wireless communication systems, PLC, and BPL, AMI devices would have the ability to interact with the critical physical infrastructure (e.g. IED's such as CBC (Capacitor Bank Controller) systems in order to improve: circuit efficiency, loss reduction, and energy savings). This will help optimize the lifetime of the physical infrastructure. (Ref: Distribution Use Case 2)

  Security Objective:

  - To protect integrity of data stored and in transit between AMI/Smart Grid devices

    - To provide AMI/Smart Grid device information in a timely manner
    - To protect AMI/Smart Grid communications from manipulation, deletion and interception

Management of the End-to-End Lifecycle of the Metering System

- An important requirement of such an AMI system would be the ability of the system to diagnose itself. The system should be able to: collect information about the status/health of certain devices, conduct remote diagnostics, and optimize operating parameters remotely.

  Security Objective:

    - To protect diagnostic data from being manipulated, deleted or masqueraded
    - To validate the authenticity of the diagnostic messages being transmitted
    - To provide timely availability to diagnostic data
    - To secure diagnostic data from eavesdropping or capture

AMI system adaptability

- The system should be able to adapt to anticipated changes that may or may not occur such as:
    - New physical communications methods
    - New features available from equipment vendors
    - New tariffs possibly with certain restrictions (e.g. number of rates or time)
    - Connections to new types of load control equipment
    - New communications protocols
    - Changes to operating parameters
    - New computing applications

Security Objective:

- The aforementioned should be accomplishable with minimal incremental cost in stark contrast to a wholesale system replacement

  Security Objective:

    - Objectives to be determined and prioritized based on technology implemented

Prepay

- Utilities use the AMI system to enforce disconnection when the prepayment balance reaches zero.

  Security Objective:

- To provide confidentiality to customer payment and associated information; avoid eavesdropping, interception or collection of customer data stored (temporary or permanent) or in transit
- To provide integrity of data being transmitted including non-repudiation and validation of customer information transmitted
- To provide the customer availability to their respective account(s) within customer payment services

A.8 Security Domains View

This section describes the internal use cases; cases where activity is stimulated from entirely within AMI itself. Examples are automation and intelligent responses. The following diagram describes the internal services provided by AMI. Assumption is made that measurement, monitoring, and application control encompass all services.

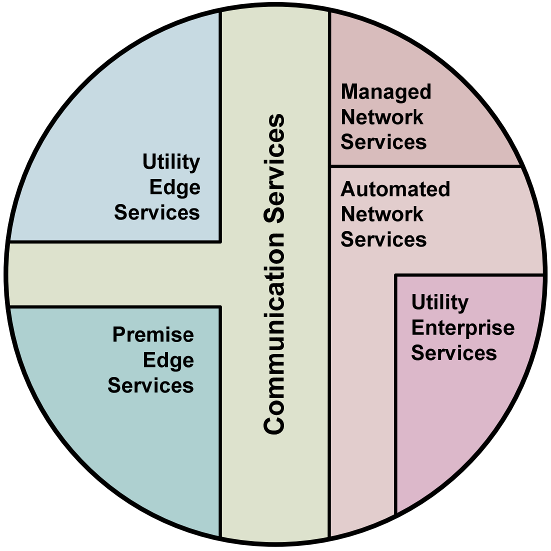

Figure 8 - AMI Service Domains

Legend:

- **Utility Edge Services** – All field services applications including monitoring, measurement and control controlled by the Utility
- **Premise Edge Services –** All field services applications including monitoring, measurement and control controlled by the Customer (Customer has control to delegate to third party)
- **Communications Services** – are applications that relay, route, and field aggregation, field communication aggregation, field communication distribution information.
- **Management Services** – attended support services for automated and communication services (includes device management)
- **Automated Services** – unattended collection, transmission of data and performs the necessary translation, transformation, response, and data staging
- **Business Services –** core business applications (includes asset management)

Stakeholders:

- Customer Users of the system
- Operators of the system
- Responsible Entities of the systems
- Implementers of the system
- Maintainers of the system

Concerns:

How is integrity maintained for processes?
How is integrity maintained for data?
How is confidentiality of customer data maintained (e.g. customer usage)?
How is availability to utility assets maintained?

Viewpoint language:

Use Cases (Misuse Cases)
Note: Potentially move down from business functions.

Analytic Methods:

Penetration Testing
Auditing

Rationale:

This viewpoint was selected because it shows the relationship between AMI services requiring security measures. Drivers for this viewpoint include control, ownership, environmental, and functionality (capability) concerns.

A.8.1. Utility Edge Services Domain

Summary

The Utility Edge Services Domain allows the utility to interact with non-customer-owned edge assets, such a meter (electric, gas, or water) or other end-point device.

Assumptions

The Utility Edge Services Domain assumes a singular service endpoint (point of service).

Ownership and Control Concerns

The utility owns at least some of the assets within the Utility Edge Services Domain. Any asset not owned by the utility in question is owned by a peer entity, such as another utility.

The utility controls all assets within the Utility Edge Services Domain. Assets owned by another entity are controlled by the utility as a proxy for the owner.

A.8.2 Premise Edge Services Domain

Summary

The Premise Edge Services Domain allows the utility to interact with customer-owned edge assets, such as Home Area Network (HAN) devices.

Assumptions

The Premise Edge Services Domain assumes a singular customer.

Ownership and Control Concerns

The utility may own the assets within the Premise Edge Services Domain. Alternatively, assets in the Premise Edge Services Domain may be owned by the Customer or a Third Party Service Provider.

The utility controls all assets within the Premise Edge Services Domain. Control of assets owned by another entity is delegated to the utility as part of admission to the Premise Edge Services Domain.

A.8.3. Communication Services Domain

Summary

The Communication Services Domain facilitates communication between assets in adjacent service domains (Utility Edge, Premise Edge, Managed Network, and Automated Network) and may facilitate communication between assets within the same domain.

Assumptions

The Communication Services Domain assumes interfaces to multiple Utility Edge and Premise Edge Services Domains, and may include interfaces to multiple Managed Network and Automated Network Services Domains.

Ownership and Control Concerns

The utility may own the assets within the Communication Services Domain. Alternatively, assets in the Communication Services Domain may be owned by a Communication Services Provider.

The utility may control assets within the Communication Services Domain. Alternatively, assets in the Communication Services Domain may be controlled by a Communication Services Provider. Assets controlled by a Communication Services Provider may be included in a contractual services agreement with the utility.

A.8.4. Managed Network Services Domain

Summary

The Managed Network Services Domain allows the utility to manage communication configuration, settings, capabilities, and resources in each of the other service domains.

Assumptions

The utility primarily uses assets in the Managed Network Services Domain to manipulate configurations and settings in the Automated Network Services Domain (i.e., human interface).

Ownership and Control Concerns

The utility may own the assets within the Managed Network Services Domain. Alternatively, assets in the Managed Network Services Domain may be owned by a Communication Services Provider.

The utility controls all assets within the Managed Network Services Domain. Control of assets owned by another entity is delegated to the utility as part of admission to the Managed Network Services Domain.

A.8.5. Automated Network Services Domain

Summary

The Automated Network Services Domain allows the utility to implement the communication parameters specified using assets in the Managed Network Services Domain.

Assumptions

The utility primarily uses assets in the Automated Network Services Domain to perform routine and/or repetitive operations at high speed without manual intervention.

Ownership and Control Concerns

The utility may own the assets within the Automated Network Services Domain. Alternatively, assets in the Automated Network Services Domain may be owned by a Communication Services Provider.

The utility controls all assets within the Automated Network Services Domain. Control of assets owned by another entity is delegated to the utility as part of admission to the Automated Network Services Domain.

A.8.6. Utility Enterprise Services Domain

Summary

The Utility Enterprise Services Domain allows the utility to perform the business functions required by enterprise applications.

Assumptions

The assets in the Utility Enterprise Services Domain provide the interface to AMI systems and data for the remainder of the enterprise.

Ownership and Control Concerns

The utility owns all assets within the Utility Enterprise Services Domain.

The utility controls all assets within the Utility Enterprise Services Domain.

Appendix B – Supplemental Material: Business Functions as Stakeholders in AMI Systems

B.1 Introduction

The information provided in this appendix provides supplemental background material for understanding potential business functions within AMI systems. Some of the business functions provide a forward-looking perspective into AMI systems. This information may be used in the development of a utility's specific use cases, but the information in this section is not intended to be regarded as security requirements for AMI.

B.1.2 Scope of AMI Systems

As Smart Grid requirements drive the development new technologies and the deployment of new systems, more and more new and existing Business Functions are becoming stakeholders in these new systems. Advanced Metering Infrastructure (AMI) systems are prime examples of these new technologies: they clearly can provide Smart Grid benefits. However, AMI systems are still a work in process, which can clearly benefit some business functions, but which appear potentially useful for others while not yet obviously beneficial. In addition, there will inevitably be business functions which are not yet foreseen that will suddenly become viable.

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 (see **Error! Reference source not found.**).

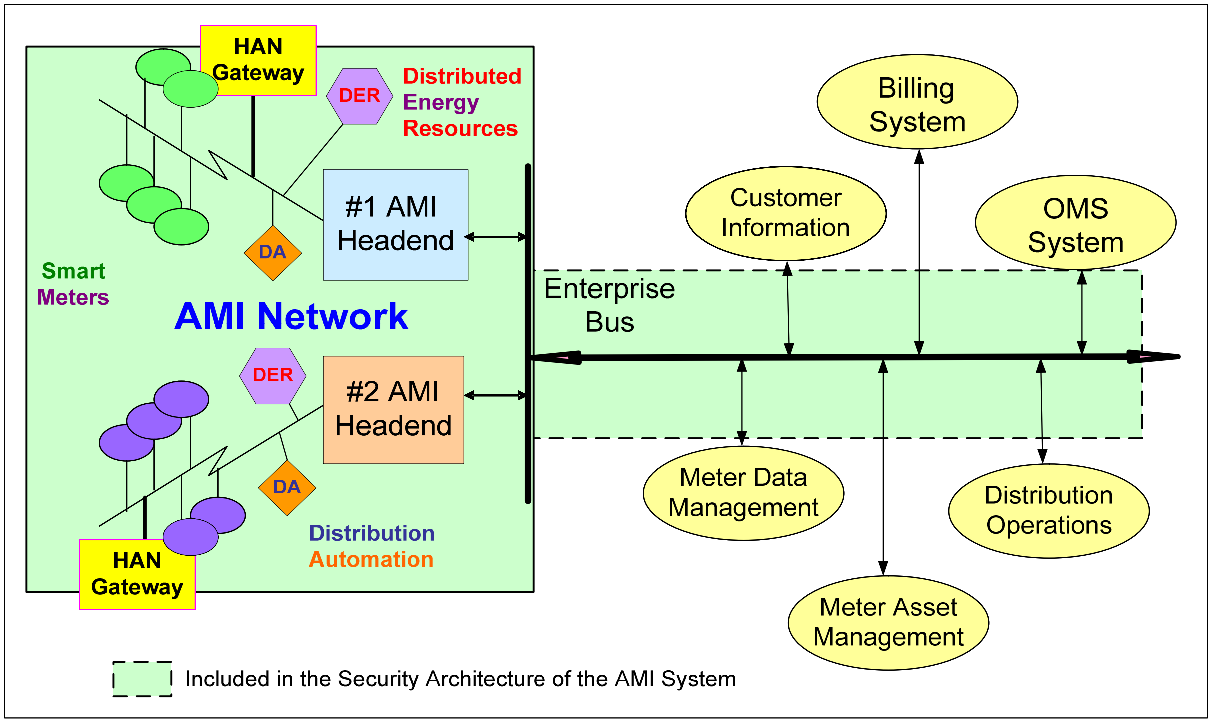

Figure 9 - Scope of AMI Systems

B.2 Overview of Business Functions Utilizing AMI Systems

Identifying and describing Business Functions are the most effective methods for understanding the information exchange requirements. The range of Business Functions utilizing the AMI systems is shown in **Error! Reference source not found.**.

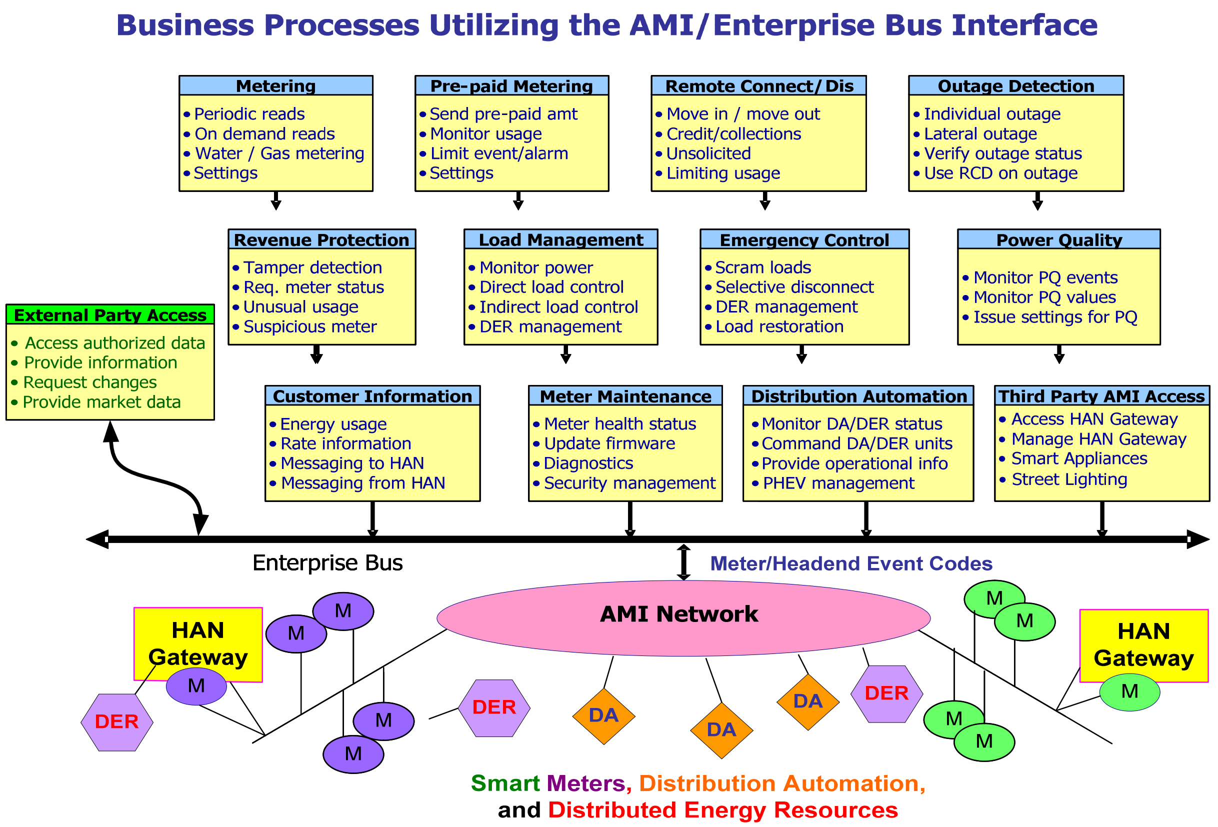

Figure 10 - Business Functions Utilizing the AMI/Enterprise Bus Interface

The following sections expand on these Business Functions.

B.3 AMI Metering Business Functions

B.3.1 Metering Services

Metering 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.

B.3.1.1 Periodic Meter Reading

Traditionally for residential customers and the smaller C&I customers, periodic meter reading services are performed monthly via a meter reader, possibly using handheld or mobile meter reading tools. It takes the current index reading from the meter and records it for billing and other purposes. For Time-of-Use (TOU) data from net metering or other TOU meters, intervals can be established such as “on-peak” and “off-peak”, as defined in the utility’s tariffs. In some utilities or under certain circumstances, actual meter reading is done less frequently, and bills rely on meter reading estimates which are “trued up” later.

In AMI systems, periodic meter reading will retrieve interval data (usually hourly data but possibly 15-minute or 5-minute data). The frequency of retrieving the data from the meter can vary from every 5 minutes, to hourly, to daily, and to monthly.

Among the benefits of AMI for periodic meter readings are the increased accuracy (fewer estimated reads, more exact reading dates/times), and the availability of the to-date meter readings during the billing cycle.

B.3.1.2 On-Demand Meter Reading

Traditionally, on-demand meter reading is performed by sending a meter reader to the meter site around the time requested for the meter reading. Typically reasons for on-demand meter readings include:

- Move in / move out
- Limited usage tariffs
- Billing questions by the customer
- Revenue protection concerns

AMI systems will permit on-demand reads to take place almost immediately or more precisely at the scheduled date and time.

B.3.1.3 Net Metering for DER

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 hybrid electric vehicles (PHEVs) become available, net metering will increasingly be implemented in homes and small businesses, even parking lots.

AMI systems can facilitate the management of net metering, particularly if pricing becomes more dynamic and/or more fine-grained than currently used for TOU rates.

B.3.1.4 Bill - Paycheck Matching

Today, depending on the utility bills arrive monthly, quarterly or yearly and not on a schedule selected by the customer, rather they are based on a schedule that matches the meter reading schedules. Small scale trials have proven that for customers who are living on the margin and miss occasional payments, that matching the date and frequency of the customer’s paycheck reduces the number of late or missing payments significantly, cutting collection costs and reducing the cost to all customers.

AMI systems provide the flexibility to provide customers with bills when the customers prefer to receive them.

B.3.2 Pre-Paid Metering

B.3.2.1 Prepayment Tariffs

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.

B.3.2.2 Limited Energy Usage

Traditionally, customers who use pre-payment tariffs need to go through the utility customer representatives to learn about their current usage or to extend their energy limits. With AMI systems, customers can see their current usage and limits, and may be able to automatically extend their limits electronically (e.g. pay over the Internet with the AMI system then updating their energy limits).

B.3.2.3 Limited Demand

Customers can also have tariffs that limit demand. Some C&I customers have rates that depended on the peak 15-minute demand. Some other customers actually have current limiting equipment to ensure limited demand.

AMI systems can provide the customer with the information necessary to manage their demand limits more precisely and effectively.

B.3.3 Revenue Protection

B.3.3.1 Tamper Detection

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. During the analysis of the data, tampering that is not visually obvious may be detected, such as anomalous low usage.

With AMI systems, smart meters can immediately issue “tampering” alarms that are set off by a number of different sensors and routines in the meter. These tampering actions can include meter removal, tilt, and unauthorized access attempts (smart meters cannot be plugged in upside down).

B.3.3.2 Anomalous Readings

Some anomalous readings in the meter can trigger warning events which can be immediately investigated to determine if they are legitimate (people are on vacation or the factory has shut down an assembly line) or if they are due to tampering, such as wiring around the meter.

B.3.3.3 Meter Status

Some theft of power has occurred by the bypassing of the meter for a few days between scheduled readings by a meter reader. AMI systems will permit the status of meters to be verified at any time during the reading cycle.

B.3.3.4 Suspicious Meter

Some theft of power has occurred by the replacement of a certified meter with a “slow run” meter. AMI systems with smart meters will have each meter “registered” with an identity that cannot be tampered with without showing evidence of that tampering.

B.3.4 Remote Connect / Disconnect

B.3.4.1 Remote Connect for Move-In

The customer initiates a request to move into a location that has electric service but is currently disconnected at the meter. The request can be for immediate action or for a connection at a specific date and time.

Traditionally, utilities send a metering service person to connect the meter. With an AMI system, the connection can be performed remotely by closing the remote connect/disconnect (RCD) switch, using the following steps:

- At the appropriate date and time, read the meter to get the latest reading and to verify that the meter is functional.
- Determine there is no backfeed current detected by the meter
- Issue the connect command to the meter
- Verify that the meter is connected

B.3.4.2 Remote Connect for Reinstatement on Payment

Once a customer pays who was disconnected due to non-payment (or works out some mutually accepted agreements), the meter needs to be reconnected by closing the remote connect/disconnect (RCD) switch. The same process as for a move-in would be used.

B.3.4.3 Remote Disconnect for Move-Out

Traditionally, move-outs are handled by performing a special meter read (“soft” disconnect) around the time of the move-out. Since the power is not actually disconnected, this method can lead to illegal use of power after the move-out and before the next move-in.

With an AMI system, a move-out can have a “hard” disconnect that opens the RCD switch, typically using the following steps:

- Verify that the meter can be disconnected remotely
- Issue the disconnect command at the appropriate date and time
- Verify that the meter is disconnected
- Read the meter for the final billing.

In conjunction with the next meter reading during a move-in connection, any delta between the readings can be detected as a possible tampering or illegal usage of power.

B.3.4.4 Remote Disconnect for Non-Payment

The cost of collections is high, typically higher yet is the cost of disconnecting a customer – not only the lost revenue, but the cost of two special trips to the location, one to turn the power off and eventually another to turn it back on again. While remote disconnects are still pricy today, they offer a much lower cost for turning the power off and once customers understand that a disconnect can be done immediately, collections costs also seem to decline.

B.3.4.5 Remote Disconnect for Emergency Load Control

Some customers could get special rates if they agree to the temporary suspension of electric service in support emergency load shed activities. This is an alternative to wide-scale rolling blackouts and circuit level interruptions. Customers who choose to participate in such a program are eligible to have their power cut during the critical periods.

This type of selective black-out provides the means for reducing power demands on the overall grid while selectively maintaining service to critical customers such as public infrastructure (i.e. traffic lights) and medical facilities.

B.3.4.6 Unsolicited Connect / Disconnect Event

Unsolicited connect/disconnect events can be caused by a number of activities, covered in the following Business Functions:

- Meter manually switched off by utility employee, including both valid and invalid switching
- Meter manually switched off by unknown party, including both valid and invalid switching
- Software/hardware failure switches meter off/on (also includes unauthorized command causing switch)
- Miscellaneous event causes meter to switch off/on
- Meter manually switched on by utility employee, including both valid and invalid switching
- Meter manually switched on by unknown party, including both valid and invalid switching

B.3.5 Meter Maintenance

B.3.5.1 Connectivity Validation

Determination that the customer is connected to the grid and even with the right signally which phase and circuit they are on. In several reviews of customer connectivity today for utilities the phase information is missing from many single phase connections and in some cases the circuit information is missing or wrong. Validation helps with making sure the data analysis is correct for engineering studies and other purposes.

B.3.5.2 Geo-Location

In asset data bases today many meters are literally miles (kilometers) from their physical location in the real world. During the installation of the meters GPS or other geo-location techniques can be used to provide accurate information on the meter's location. If the location of the meter accidently is changed in the database it is possible to flag the problem. This is possible since the location of the circuit is known, helping to eliminate problems that creep in over the long life of electric (gas and water) networks.

B.3.5.3 Battery Management

If there were no smart meters, there would be no need to do battery management, so the benefit only works for smart meter equipped networks. In an operational world the meters communicate more, running the battery down faster. It is important to have good battery management or the cost of maintaining the system will skyrocket. Remote battery monitoring (as part of the regular communications) can help deal with battery replacement planning and battery life extension.

B.4 Distribution Operations Business Functions

B.4.1 Distribution Automation (DA)

B.4.1.1 DA Equipment Monitoring and Control

Some utilities are planning to use the AMI system for distribution automation, as a minimum for direct monitoring and more sophisticated control of capacitor banks and voltage regulators on feeders, rather than relying on local actions triggered by time, current, or voltage levels. Others also would like to monitor and control automated switches and fault indicators if the AMI network were able to stay alive during grid power outages, presumably via battery backup for critical nodes.

B.4.1.2 Use of Smart Meters for Power System Information

If more sensors were available in the distribution network, it would be possible to do distribution SCADA, with the deployment of smart meters and a near real-time communications network, it is possible to pick a sub-set of the smart meters and use them as bell weather devices in the grid to provide a distribution SCADA like capability. In addition some utilities are installing smart meters in place of RTUs for extending their current SCADA system further into the grid.

B.4.1.3 Power System Security/Reliability

As interference with the operation of the distribution grid becomes more common, it becomes more and more important to monitor the integrity of the grid at all times. Smart meters offer a way to get a “heart beat” from the whole of the distribution system on a regular basis thus providing assurance that the grid is intact. That it has not been attacked by a mad man in a backhoe or a copper thief with a chainsaw.

B.4.1.4 Power System Protection

Overloads on the system once were not a big issue devices could operate at two or even three times their rated capacity for several hours on a peak day. Today devices have been engineered to run at loads much closer to their ratings, and overloads of several hours can cause degradation in the devices. By being able to monitor the load on the device and with the deployment of direct load control or disconnect switches, the load on the device can be managed until it can be replaced or upgraded, the same goes for other physical assets that may be de-rated, allowing at least some of the lights to stay on.

B.4.1.5 Site/Line Status

Tag out procedures are supposed to render a segment of the network dead and safe to work on, unfortunately with the addition of true distributed generation, it is possible to have an islanding failure and to have a line that the crew expects to be ready for work, to actually still be live. With the correct smart metering system and the right connectivity mapping, it is possible to use the smart meters to determine if any power is still flowing through the lines. With the potential for the sales of plug-in hybrids to ramp up quickly in the next decade and the lack of protection schemes currently this may become an even larger issue.

B.4.1.6 Automation of Emergency Response

Today in a fire, the fire department normally handles the disconnection of the power and other utilities from the involved structures. Often with a fire axe! With the advent of remote disconnects in the meters it will be possible to cut the power to the structure, as well as gas and other utilities. This makes it easier to restore service after small problems and to more rapidly remove a possible source of problems from the structure.

B.4.1.7 Dynamic Rating of Feeders

Operators can dynamically rate feeders based on the more accurate power system information retrieved via the AMI system from strategic locations. This permits the operators to decide when they can run feeders beyond their ostensible ratings or when to perform multi-level feeder reconfigurations to balance the loads and avoid overloads.

B.4.2 Outage Detection and Restoration

B.4.2.1 Outage Detection

Today the majority of real time information about a customer, comes from the customer, they pick up the phone and call about issues they have, such as an outage, and provide information to the utility. In the future, the smart meter will be able to provide up to date information about the customer and the status of their service.

B.4.2.2 Scheduled Outage Notification

For either scheduled outages for maintenance or for notification of a customer that the power is out in their home when they are at work or away from home, smart metering provides a needed piece. For scheduled outages, if there are in home displays deployed the metering system can provide the outage times and durations to the customers directly impacted and no others. This minimizes possible security issues of the information getting into the wrong hands as security systems that require power stop functioning, etc. It also helps with the number of phone calls that have to be placed to customers to let them know that maintenance is happening. With the connectivity verification, it is possible to really know who is on a specific path and to accurately manage the outage. For unscheduled outages, it possible to use the information coming from the meters to let customers know that they will be returning to a location with no power (water, gas) and that will let them make alternate plans, rather than walking into a surprise.

B.4.2.3 Street Lighting Outage Detection

Street lighting can be critical to safety and crime-prevention, and yet monitoring which street lights are out is currently performed haphazardly by civil servants and concerned citizens. AMI systems could be used to monitor these lights.

B.4.2.4 Outage Restoration Verification

Restoration verification has the metering system report in as the power it returned to the meters. This alert function is built into many meters that are being deployed as smart meters today and includes a timestamp for the restoration time. For some utilities this is improving their IEEE indices, since their crews may take several minutes to complete other actions before reporting the power back on. It can also be used to help isolate nested outages and help the field crews get to the root cause of those nested outages before they leave the scene.

B.4.2.5 Planned Outage Scheduling

Ideally, planned outages should be done at a time when they have the least impact on the customers. Today we use rules of thumb about when to take a planned outage, in the future with a complete data set it is possible to adjust the time of the outage to correspond with the lowest number of customers demanding power. This minimizes the impact to the customers.

B.4.2.6 Planned Outage Restoration Verification

In completing work orders, it is useful to know that all of the customers that were affected by the work order have power and that there are no outstanding issues that need to be corrected, prior to the crew leaving the area. The ability to “ping” every meter in the area that was affected by the work order and determine if there are any customers who are not communicating that they have power is useful to minimize return trips to the work area to restore single customers.

B.4.2.7 Calculation of IEEE Outage Indices

Today the IEEE indices are manually calculated in most utilities and they are not up to date, since the information needed to track them comes from field reports and other documents that do not feed into a central location. Additionally since not every single point is tracked in any system for outages, it is impossible to accurately determine the indices. Most utilities have gotten very good at the development of indices that are very close to the reality that their customers are seeing and to the limits of the information available.

B.4.2.8 Call Center Unloading

Today we rely on customers to call in when there is an outage; this normally is one of the factors in sizing call centers and staffing them. When smart metering is deployed in the right way, it is possible for the system to determine where the outages are and to let the utility call the customer with an outage message and an estimated time to repair. In the long run this will reduce the loading on the call center during periods of high outage levels.

B.4.3 Load Management

B.4.3.1 Direct Load Control

Direct Load Control provides active 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 is thus a callable and schedulable resource, and can be used in place of operational reserves in generation scheduling. Customer like it (if it is invisible), because they do not have to think about it, they sign up, allow the installation and forget it.

AMI systems will enhance the ability of utilities to include more customers in (appropriate) programs of direct load control, since it will increase the number of appliances accessible for participation in load control, and will improve the "near-real-time" monitoring of the results of the load control actions.

B.4.3.2 Demand Side Management

Management of the use of energy is important in a number of ways. Demand Side Management is a step beyond just tariff based load reduction. It assumes that customer will setup or allow to be set up equipment to reduce load when signals are sent to the customer's location. The customer is in charge of making demand side management decisions.

B.4.3.3 Load Shift Scheduling

Given the ability to get customers to shift load when requested, and to do bottom up simulation it becomes possible to work with customers who have the ability to shift load to different times of the day or week. This ability to do load scheduling could have an impact on transmission and other capital expenses.

B.4.3.4 Curtailment Planning

To do proper load reduction, for either de-rated equipment or for planned outage or even to deal with load growth that has gotten ahead of system upgrades takes having data on what the loads are and what can be curtailed. In California, load curtailment has been called rolling blackouts, the best that can be done without an ability to control the demand on the system in a more granular fashion. By using curtailment planning, notice can be given in advance to the impacted customers and they have enough time to respond if they have an option in their contract to keep the power on.

B.4.3.5 Selective Load Management through Home Area Networks

With the deployment of home area networks the utility can choose to manage the load on the grid, to manage peak, to manage customer bills, to allow for a generation or transmission issue to be corrected or other reasons. This can permit, with the right equipment the reduction in the need for reserve margin in generation and for rolling reserve, the selective load management becoming a virtual power plant that is a callable and schedulable asset.

B.4.4 Power Quality Management

B.4.4.1 Power Quality Monitoring

Today for some larger customers and at select locations on the grid we are able to monitor harmonics, wave form, phase angles and other power quality indicators. The need continues to grow as large screen televisions and other consumer electronics devices are increasingly adding harmonics to the system. With the newest metering technology some power quality monitoring is built into the meter and more is on the way. While not every house needs to monitor power quality, a percentage of the meters deployed should probably have this advanced capability.

B.4.4.2 Asset Load Monitoring

With Connectivity Verification and Geo-Location information it is possible to group the devices in a tree structure that correctly shows connection points in the grid. With the ability to read intervals from the meters it is then possible to build a picture of the load that each asset (e.g. transformers, conductors, etc.) are subjected to. This allows an operator to monitor heavily loaded assets and look for ways to off load some of the demand from that asset. It also allows a maintenance planner to prioritize what maintenance should be done to maximize the reliability of the grid, as part of a reliability centered maintenance program.

B.4.4.3 Phase Balancing

One of the least talked about issues with losses in the distribution grid today is single phase load and the imbalance it can cause between the phases. These losses have seldom been measured in the grid and little study has been done of the amount of phase imbalance on the grid today. In early studies the chronic phase imbalance in several circuits that were monitored averaged over 10 percent. While correction is hard when the circuit is run as single phase laterals, in many cases there is enough load on the feeder portion of the circuit to allow rebalancing of the circuit to eliminate more than half of the chronic phase imbalance.

B.4.4.4 Load Balancing

Where there is an option to move a portion of the load from one circuit to another, the instrumentation is not always available to make good choices or to be able to forecast the load in a way that makes the movement pro-active instead of reactive. Automated feeder switches, and segmentation devices are becoming more and more common in the grid. The ability to use metering data to support the operation of these devices will only increase their value to the grid operator. Today with information only at the substation end of the circuit, it is tough to determine where on the circuit the load really is and where to position segmentation and when to activate a segmentation device when more than one is available. Operators today typically learn the right way by trial and error on the system.

B.4.5 Distributed Energy Resource (DER) Management

In the future, more and more of the resources on the grid will be connected to the distribution network and will complicate the operation of the grid for the future. Failure to integrate these resources into the grid and understand their impact will only degrade the operation of the grid and its reliability. It is no longer an option to deal with distributed resources, the time for refusing to allow them has passed. The only choice is to either embrace them and manage their impact or ignore them and suffer the consequences.

B.4.5.1 Direct Monitoring and Control of DER

Some DER units at customer sites could be monitored in “near-real-time” and possibly directly controlled by the utility or a third party (e.g. an aggregator) via the AMI system, in an equivalent manner to load control.

B.4.5.2 Shut-Down or Islanding Verification for DER

Each time an outage occurs that affect the power grid with DER, the DER should either shut down or island itself from the rest of the grid, only feeding the “microgrid” that is directly attached to. In many cases the shut-down or islanding equipment in smaller installations is poorly installed or poorly maintained. This leads to leakage of the power into the rest of the grid and potential problems for the field crews.

Each time an outage occurs, meters that are designed to monitor net power can tell if the islanding occurred correctly, if they are installed at the right point in the system. This reporting can minimize crew safety and allow the utility to let the customer know that maintenance is required on their DER system. In most cases when the islanding fails, other problems also exist that reduce the efficiency of the DER system, costing the customer the power that they expected to get from the system.

B.4.5.3 Plug-in Hybrid Vehicle (PHEV) Management

Depending on how plug-in hybrids are sold and how the consumers take to them, they may either become one of the largest new uses of power or they may not have an impact. A major problem is that planners are now assuming that they will be mobile generation plants, that the drivers will burn fuel and store power in the battery to be drawn during the peak times while parked in the company garage. Others have assumed that the cars will become the largest new consumer of power in the downtown grid, an overstressed part of the grid already.

How plug-ins are managed and how consumers will use them is a social experiment. What is not is that they will draw a large amount of power from somewhere and have the potential to store a lot of power for later use. How the power company measures which car provides or takes how many megawatt hours and proves it and bills for it, will be an interesting change. Smart meters can help with this if the right standards are place to deal with communication from the car to the meter.

B.4.5.4 Net and Gross DER Monitoring

There are two different generation results from distributed generation, the gross output of the device and the net input into the grid, after the owner takes their needed energy. The two can be very different at times when the DER is creating most power the owner may also be drawing so heavily that the net result to the grid is still negative. At other times, the demand from the owner may be less than the output, even though the output may be well under the design output of the device.

Some utilities have decided to reward renewable generation owners on the gross output, while other utilities have decided to reward them on the net output, possibly with TOU rates. But to manage a utility and the reliability of the grid it is important to know both the net and the gross output of the device for simulation, load forecasting and for engineering design.

B.4.5.5 Storage Fill/Draw Management

If someone has installed distributed storage, when should it be topped off, and when should the storage discharge? Today's answer is to use a timer in most cases or a phone based trigger. For one utility the use of electric thermal storage for winter heat and time of use tariffs that encouraged topping up at a specific time of the day resulted in the destruction of a number of pieces of equipment on the grid as demand exceeded the local ability to supply that demand. The attempt to improve the load factor on the grid with this storage system resulted instead with demand that exceeded all expectations.

Smart metering with a home area network capability can trigger each storage device based on the total load in the area, leveling out the peaks in the system and providing better use of generation resources that may be variable in nature.

B.4.5.6 Supply Following Tariffs

DER has a strong probability of having a large percentage of renewable generation which has a strong variable component. Since the supply will be variable and highly variable on short notice, it may be that to avoid either a large component of rolling reserve that uses fossil fuels, it may be that a supply following tariff could be possible. It would require a very high speed forecasting system, excellent weather information and near real time communications to devices in the homes and in businesses with almost instant response. This is a tall order in today's world, but the cable companies have proven that millions of devices are possible to broadcast to in near real-time, so it is possible.

Smart meters on the right communications network and with the right in home gateway could provide a piece of this supply following tariff system.

B.4.5.7 Small Fossil Source Management

There is a large amount of diesel generation that is installed on customer sites to deal with outages on the grid. Some companies are now forming to manage these resources, not for outage, but for peak power production, bidding into the market a few megawatts at a time. While the use of these resources is a good thing, the penetration of private companies will never be as complete as if the utility were to work with their customers to equip most of this generation with controls and monitoring equipment.

Whether the utility operates and maintains these resources or allows third parties to take responsibility is not important. What is important is that smart metering can reduce the cost and complexity of making these resources available. In California more than 2,000 Megawatts of generation are already installed, more than enough to end most rolling blackouts (if the resources are in the right areas).

B.4.6 Distribution Planning

B.4.6.1 Vegetation Management

Momentary outages normally increase as vegetation grows back in an area and starts to become potential issue for overhead lines. Smart metering allows the return of momentary outage information and allows the outage counts to be overlaid on a GIS system. This allows the planners to better target vegetation management people to the right locations. In the underground world, cable failures and splice failures can be found early, prior to a complete failure.

B.4.6.2 Regional and Local Load Forecasting

Given the ability to draw a full data set from the field, it is now possible to forecast regional and local loads and generation that can be used to prepare for and to set prices for both demand and supply.

B.4.6.3 Simulations of Responses to Pricing and Direct Control Actions

As more detailed information is available through AMI systems on regional and local loads and generation, it will be possible to assess the responses of both customers and the power system to price-related actions as well as direct control actions. This ability to simulate the market a day or more in advance should allow for better planning and for the system to run with smaller amounts of rolling reserve and ancillary services.

B.4.6.4 Asset Load Analysis

With the ability to have a real load history on a specific asset and to be able to do bottom up forecasting, the same can be done for assets in the connection tree. This should allow planners and others to see potential problem areas before they really exist.

B.4.6.5 Design Standards

Many of today’s standards assume that complete data is not available so there are factors of safety built into the calculations at each step of the design process for the transmission and distribution grid to make sure that the design is useful for its full design life. The improvement in load and demand data from the smart meters will make it possible to remove many of the rules of thumb and design to the real needs of the customers.

B.4.6.6 Maintenance Standards

Maintenance is done with incomplete information. So the maintenance standards allow for this, in some cases too much maintenance is done and sometimes too little is done, standards call for the best possible maintenance planning that incomplete information can provide. The good news is that the reliability of the system is very high, better than any other service (including telecommunications and cable TV) that is available to a customer. The bad news is with all the retirements in the industry, the experienced technicians that are required to make the judgment calls in the field will all be replaced in a few years. Improving the standards for maintenance with better information will mean that the new field workers will be routed to the highest priority work almost every time.

B.4.6.7 Rebuild Cycle

When is the right time to rebuild a circuit and how much of it really needs to be upgraded? Today with the information we have, we hang some recorders and use a few weeks or months of data from a few locations to determine what to rebuild, with the improved data set and the improved standards it is possible to actually determine the sections of the grid to rebuild and how much to reinforce them.

B.4.6.8 Replacement Planning

Equipment replacement is based on the estimated load or a load study that is normally conducted with less than perfect information. This has resulted in the engineering team being conservative and over sizing many of the replacement equipment. Smart metering offers better information to make better sizing decisions.

B.4.7 Work Management

B.4.7.1 Work Dispatch Improvement

Today we use manufacturers' recommendations, models, estimates, and visual inspection to determine when a lot of maintenance work should be done. While it works, in some utilities it means more maintenance than others think is required and in others it means less. In almost every case, some maintenance is performed that is not really required for reliability centered maintenance strategies. When smart metering information is available and used to do asset loading analysis and other data analysis, work can be more accurately dispatched to the crews in the field improving reliability in the system for the same number of jobs completed.

B.4.7.2 Order Completion Automation

Some utilities have the field crew log the completion of their job prior to packing up; others want the crew ready to roll prior to completion of the order. Some want the crews to look around before leaving, some want the crew to leave and let the customers call if there is still an issue in the area. With smart metering, as restoration alerts come in, it is possible to automate the time the job was completed and some of the closing paperwork, allowing the crew to stay in the field longer each day and to do less paperwork overall.

B.4.7.3 Field Worker Data Access

Today if a line worker wants to know the status of an area of the grid, she can measure power flow, she can look at meters or he can call dispatch. Access to near real time information on the status of the customers close to the worker's location is limited today. With the deployment of smart metering, depending on how the software is configured and the security setup, it may be possible for a field worker to get access to the a near real-time map of the status of the customers in their working area, minimizing the need for dispatch to tell the worker where to go next and what to do.

With experience, field workers have proven to be very good at determining where in their work area a likely root cause is, based on outage information, reducing the time it takes to find the cause and start the repair work.

B.4.7.4 Reliability Centered Maintenance (RCM) Planning

Today we guess at the loading on devices using models, and use that information to develop a reliability centered maintenance plan. Based on that information we do our best to perform the maintenance that the system requires to make sure that people have power. With the ability to do load monitoring and load forecasting more accurately, preseason maintenance can be scheduled based on the facts that the system generates. While it will never prevent all failures in the system, use of this information and a well designed RCM plan can result in significantly less outage for non-natural disaster causes.

B.5 Customer Interactions Business Functions

B.5.1 Customer Services

B.5.1.1 Remote Issue Validation

When a customer calls today with a problem, other than twenty questions on the phone or rolling a truck to the location, there is no way to understand if the customer really knows what the problem is or if they do not understand the problem. Use of near real time information from smart meters can allow the customer service representative (CSR) to provide better information to the customer and to provide better advice on what to do with the current situation. It can also reduce the dispatch of trucks for customer complaints. In general it reduces both call volume and call handling times.

B.5.1.2 Customer Dispute Management

The most frequent customer dispute is a high bill. They complain about the meter reading being wrong. In truth there are enough meter reading errors that high bills are a fact of life. But the ability to check the current meter reading directly from the meter while the customer is on the phone and re-calculate the bill if the bill was high, and to end the post call investigation, by being able to directly validate the customer dispute reduces the time to clear a complaint that is non-phone time and it reduces the call handling time of the life of the dispute. It is not unusual that the initial call time goes up, since the CSR has to explain how they are getting the information and may have to have the customer walk to the meter while on the phone and verify the numbers that show on the meter. This has reduced monthly disputes with chronic callers over a period of 3 to 6 months in most utilities that have this ability.

B.5.1.3 Outbound Customer Issue Notification

Not only can customers be called at work for problems with outage, but other problems can be determined and customers notified, in one case, a meter looked like it had been tampered with, but the customer had a complaint about low voltage on file. A review of the situation determined that one of the wires was probably loose in the customer’s breaker panel. That call resulted in the customer hiring an electrician and fixing a number of electrical problems in their home that the electrician uncovered while fixing the loose wire in the panel. This is one example of a number of proactive actions that can be taken with the customer to help them be safe and know what is going on with their energy consumption. Similar work was undertaken on behalf of a water company and a number of beyond the meter leaks were identified with night time readings on homes with high water bill complaints.

B.5.1.4 Customer Energy Advisory

Some utilities have undertaken to provide a customer energy consumption advisory that allowed customers to indicate what they have for energy consuming devices and information about their home. In return, the utilities rank their consumption against similar homes and provide feedback on the equipment and appliances that were consuming significant energy.

This advisory can even suggest what should be replaced and the payback period on the replacement, based on energy usage. The comparison allows customers to see how they did against similar customers and where they ranked in energy consumption. This has been very useful in getting customers to pay more attention to their consumption.

B.5.1.5 Customer Price Display

To make a realistic decision about using or not using energy and water, customers need to know how much it will cost. As we have seen with Gasoline the global consumption decreased very little (in reality only the projection of growth in consumption declined, not the actual usage) when the price tripled at the pump in many countries. Electricity, gas and water today are in the noise of running a household for most families and for many businesses the cost does not enter the top five costs for the business. To this end, making a decision to consume energy and water is easy.

For a few businesses and a small percentage of residential customers this is not true and they have strong motivation to conserve power. With critical peak pricing or time of use pricing and rising prices for energy and water, the percentage of the average family income consumed by these utilities will no longer be noise and having information about pricing, will drive some conservation. Expect that customers will need to know the price to wash a load of clothes, not the price of a kilowatt hour.

B.5.2 Tariffs and Pricing Schemes

B.5.2.1 Tariff Design

Today a sample of the customers is used to determine what the customer profile should be and how that profile should be priced. In many cases the classification of the customers is very broad and does not really take into account the different ways that customers actually consume power. For example, a young educated single male living in an apartment may have a lower usage than the young family across the hallway and they may both pay the same per kilowatt-hour of power.

However, the young male many actually cost the utility more to serve, since the load factor for that single male may be much lower than the load factor for the young family. By being able to provide accurate data, better tariffs can be designed and better segmentation done to support a fair power price.

B.5.2.2 Rate Case Support

Today to get almost any change in what can be charged to the customers or what is placed in the rate base, it requires a rate case. In some rate cases the documents filed fill rooms and rooms in a building, mostly because the issues can be handled in a black and white manner. Experts are required to testify on many aspects of the rate case using data from other locations, since the complete data set to answer the question does not exist at the utility. While experts will not go away, and there will still be a lot of estimating, it is important to realize that smart meters provide a large data set to assist with the rate cases.

B.5.2.3 Tariff Assessments

Do critical peak tariffs create the response expected, does it do it for all segments of customers, and does it impact some customer segments more harshly than others. Use of smart meter data allows a better review of how the customers are responding to the tariffs and how to re-work them to better fit the needs of the society.

B.5.2.4 Cross Subsidization

An issue that is raised over and over again is cross subsidization of customers, one group of customers paying part of the cost of another group of customers. With our example in Tariff Design, more than likely the young family is subsidizing the young male. Regulators want to know what the cross subsidization is, they do not always want to eliminate it (e.g. the long distance rates for the telephone companies for decades financed the ability of everyone to have a phone). By having complete data on each and every customer, subsidization arguments no longer fall on “I think” arguments, but fall into the “I know” allowing the regulator to only have intended subsidies.

B.5.2.5 Customer Segmentation

Customer segmentation has traditionally been done by industry or by business segment or by customer type, not by the actual needs or profile of the customers. Regulators have never had enough data to make segmentation decisions that really classify customers together by the way they consume power and their needs for power quality or their creation of power quality issues that the utility needs to fix. Smart metering can provide the data to make meaningful segmentation decisions.

B.5.3 Demand Response

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. As noted below, 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.

Sub functions for demand response, which may or may not involve the AMI system directly, could include:

- Enroll Customer
- Enroll in Program
- Enroll Device

- Update Firmware in HAN Device
- Send Pricing to device
- Initiate Load Shedding event
- Charge/Discharge PHEV – storage device
- Commission HAN device
- HAN Network attachment verification (e.g. which device belongs to which HAN)
- Third Party enroll customer in program (similar to, but not the same as the customer enrolling directly)
- Customer self-enrollment
- Manage in home DG (e.g. MicroCHP)
- Enroll building network (C&I – e.g. Modbus)
- Decommission device
- Update security keys
- Validate device
- Test operational status of device

B.5.3.1 Real Time Pricing (RTP)

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, one aluminum company cut the cost of power by more than 70% with real time pricing and flexible scheduling. The extension of real time pricing to smaller customers and even residential customers is possible with smart metering and in home displays. Most residential customers will probably decline to participate individually because of the complexity of managing power consumption, but may be quite willing to participate if they are part of a community whose power usage is managed by an aggregator or energy service provider.

B.5.3.2 Time of Use (TOU) Pricing

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.

B.5.3.3 Critical Peak Pricing

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.

California is the largest proponent of this tariff program at this time. Most of the California utilities would prefer an incentive program instead to encourage the same behavior. There is some question as to whether retailers in unregulated markets would have to pass thru the Critical Peak Pricing to customers or if they could offer a flat price and hedge the risk of the critical peak pricing.

B.6 External Parties Business Functions

B.6.1 Gas and Water Metering

B.6.1.1 Leak Detection

In the world of gas and water, non-revenue water and leaking gas pipes are important to track down. In the water industry, use of pressure transducers on smart meters has proven useful when doing minimum night flows to find unexpected pressure drops in the system. Normally the need is one pressure transducer meter per 500 to 1000 customers in an urban environment.

B.6.1.2 Water Meter Flood Prevention

With a disconnect in the water meter, it is possible if there is a sudden increase in flow and a drop in pressure that is sustained and unusual, that the disconnect can be activated and prevent flooding. Much work will have to be done in the control software algorithms to make this a useful benefit and not one the shuts off the water when the sprinkler system and the shower are both running.

B.6.1.3 Gas Leak Isolation

Similar to flood prevention, again the software needs to get much better or their needs to be a gas leak sensor in the structure that communicates with the meter.

B.6.1.4 Pressure Management

If there is a home area network, then shut off devices or throttling devices can be attached to specific water taps and the gas meter can communicate to thermostats and water heater controls to manage the rate of consumption in the location and help with pressure management on critical days.

B.6.2 Third Party Access

B.6.2.1 Third Party Access for Outsourced Utility Functions

For some utilities, many of the business functions listed in the previous sections may be provided by third parties, rather than by the utility. In these situations, messaging will come through the "external party access" avenue, rather than an internally-driven messaging. The business processes will be fundamentally the same, but the security requirements could be significantly different and probably requiring stronger authentication at each system handoff.

Some of the business functions provided by third parties could include:

- Prepaid metering
- Remote connect/disconnect
- Load management
- Emergency control
- Distribution automation
- Customer usage information
- HAN management

B.6.2.2 Third Party Security Management of HAN Applications

Customers will need access to HAN application accounts through a secure web portal where they can upload device and software security keys. Those keys will need to be sent through the AMI network to the meter to allow the HAN devices to provision and join with the meter.

Future functionality may include extraction of security keys out of the meter for storage in the utility’s database. This will allow the keys to be downloaded back to a meter if it ever has to be replaced. This functionality will be required to eliminate the need to re-provision all the HAN devices in the house in the event of a meter replacement.

B.6.2.3 Appliance Monitoring

Appliances seldom last as long in the home as they do in the lab, part of this is that home owners do not do maintenance when they should, and part of it is that when small problems occur that are not handled, so they become big and expensive problems. Smart meters are a key part of an appliance monitoring solution, even for appliances that were installed long ago.

B.6.2.4 Home Security Monitoring

Today’s security monitoring industry uses phone lines and other communications methods to monitor homes. The ability to hook security monitoring devices into a home area network and provide alerts and alarms over the smart metering network could lower the cost of home security monitoring making it more affordable to the people who live in areas most likely to need it.

B.6.2.5 Home Control Gateway

Home owners may want to control their home devices themselves or they may want a third party to do so, in either case, the smart metering system can be a method of providing that home area network gateway and allowing that control to be done.

B.6.2.6 Medical Equipment Monitoring

More and more medical equipment is being installed in homes as nursing homes and hospitals are getting too expensive to live in and more life support equipment is required for people who still can live at home unassisted most of the time. Today that equipment is only monitored by specialized companies and this seldom happens. It is a growing need especially for the elderly customers of the utility. While utilities may not wish to step into this role, the smart metering infrastructure can provide a way for authorized third parties to do so.

B.6.3 External Party Information

B.6.3.1 Regulatory Issues

There are a number of issues that regulators need to judge the performance of a utility and the fairness of a utility to its customers. Smart metering has a role to play in providing facts to the regulator to help them manage these issues.

B.6.3.2 Investment Decision Support

When a utility goes to the regulator for a major capital expense there is a need for proof that the expense is required. Today like other regulator interactions, the data is typically made up of sampled data and expert opinions. With smart metering the complete data set is available to support the decisions.

B.6.4 Education

B.6.4.1 Customer Education

Customers today call the call center and receive bills. They have little interaction with their utilities, less than 40% of the customer base interacts with the utility annually. The majority of the call volume is related to outage or other power quality issues. The second highest interaction reason is billing issues. If the industry is to be successful in changing people's habits and helping to reduce consumption, then there will need to be more interaction with customers, some on billing issues, some on power quality, but more on the way they consume power and what they have for appliances.

AMI systems will provide a means of interacting more with the customer, but only if the customer understands the capabilities – as well as being assured that AMI systems are not "Big Brother" watching over them.

B.6.4.2 Utility Worker Education

Utility workers will need significant education to learn not only their own roles in a utility with AMI, but also the issues of security and privacy that will become far more critical with the widespread scope of AMI systems.

B.6.5 Third Party Access for Certain Utility Functions

For some utilities, many of the business functions listed in the previous sections may be provided by third parties, rather than by the utility. In these situations, messaging will come through the "external party access" avenue, rather than an internally-driven messaging. The business processes will be fundamentally the same, but the security requirements could be significantly different and probably requiring stronger authentication at each system handoff.