Interoperability and Cyber Security Plan

NRECA CRN Smart Grid Regional Demonstration

Grant DE-OE-0000222

National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203

Contract:

Craig Miller, Project Manager
Craig.miller@nreca.coop
703-626-9683

20 May 2010

Prepared by:

Cigital, Inc.
21351 Ridgetop Circle
Suite 400
Dulles, VA 20166

Cornice Engineering, Inc.
P.O. Box 2542
Durango, CO 81302

Power Systems Engineering
1532 W. Broadway, Suite 100
Madison, WI 53713

Table of Contents

List of Figures

List of Tables

Preface

PURPOSE

This Interoperability and Cyber Security Plan is a Phase I deliverable and provides the NRECA demonstration team's approach to the interoperability of enterprise applications and certain field devices, along with its approach to identifying and managing certain risks in the smart grid demonstration project awarded as part of the DOE Funding Opportunity Number DE-FOA-0000036. We will focus primarily on needs and risks associated with the interoperability and cyber security of components the team will be acquiring and deploying during the defined smart grid demonstration activities.

CONTACTS

The following are the primary individuals to contact with questions regarding this plan.

Contact	Title	Contact	Email Address
Craig Miller	Project Manager	703-626-9683	craig.miller@nreca.coop
Sammy Migues	Principal	703-404-5830	smigues@cigital.com
Gary McNaughton	Vice President	928-638-4062	gmcnaughton@corniceengineering.com
Rick Schmidt	VP, System Design & Comm.	608-268-3502	schmidtr@powersystem.org

EXECUTIVE SUMMARY

In its June 2009 funding opportunity announcement, the Department of Energy (DOE) highlighted interoperability as one of the key smart grid priorities. Using smart components to interconnect and manage ever-increasing parts of the nation's electric grid will increase reliability and result in a variety of efficiencies. It will also increase the exposure of the electric grid to new threats and attacks that can seriously undermine safety and security. Therefore, increasing interoperability while safely managing risk is a key DOE program goal.

This document has been written in response to a specific DOE requirement associated with the DOE's contract award to the National Rural Electric Cooperative Association (NRECA) for a Smart Grid Demonstration Project. The NRECA demonstration comprises a short Phase I that establishes project plans and approaches, and a multiyear Phase II that acquires, develops, integrates, deploys, and monitors smart grid technology.

A key Phase I deliverable is this Interoperability and Cyber Security Plan (ICSP). The primary purpose of the ICSP is to demonstrate the breadth and depth of the NRECA approach to ensuring functional success of smart grid deployments that also exhibit appropriate cyber security functions and properties. Of course, there remain many unknowns at this point. Standards are still being defined and developed, statutory and regulatory guidance is evolving, vendors are responding to changing market forces, hackers and researchers are finding issues in current technologies, and all stakeholders are getting smarter as they focus resources on the issues at hand. Consequently, it is not currently possible to create a comprehensive and detailed "cookbook" of step-by-step interoperability and cyber security (ICS) activities that will be performed over the coming years.

This Phase I document focuses on enumerating and describing tasks that will be performed in Phase II. These tasks are meant to ensure that important facets of interoperability and cyber security are analyzed and appropriately addressed in the context of the demonstration requirements and the prevailing standards, laws, regulations, technologies, and demonstration participant needs. As needed, this document will also be revised during Phase II to ensure that all groups making up the NRECA demonstration team are applying current and necessary ICS analysis and lessons learned.

The NRECA demonstration team's approach will incorporate a broad spectrum of guiding principles designed to ensure short-term progress and the lasting usefulness of all activities conducted. Our approach to ICS is designed to contain costs, even while working with participants nationwide, working with a diverse group of vendors, and managing risk in light of a rapidly evolving set of requirements and guidance. These principles include the following:

- **Cyber security of smart grid deployments is a large and complex issue.** The NRECA team will ensure that our approach highlights the risks being addressed and the decisions involved in long-term success. We will apply our strategic cyber security framework to ensure we are efficiently raising the bar for ICS, not just meeting the current requirements. We will ensure that ICS goals are organically linked to our demonstration activity types, not to ideas that are outside the process and addressed at the end of the project.

- **Demonstrate innovation and leadership.** We will design, code, and test extensions to the MultiSpeak® protocol that are needed to achieve some of the DOE's interoperability goals. Cyber security, and software security in particular, will figure prominently in our approach and goals. By collaborating with commercial vendors we will extend, use, and increase the security of MultiSpeak® and as a result provide some tools necessary to realize a secure smart grid. By submitting our work to standards bodies, we can accelerate their efforts to harmonize requirements nationally and globally. By instituting strong functionality and security testing procedures in our group, we can create a test harness capability that is useful to the entire industry.
- **Have a strategy of continuous improvement to manage change while achieving interoperability and security goals.** We will maximize use of the necessary cyber security and risk management concepts from the evolving North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection standards (CIPs), National Institute of Standards and Technology (NIST) publications, statutory and regulatory directives, and industry guidance not only to ensure the completeness of our approach but also to justify the usefulness of each included step based on actual risk reduced. We will not attempt to apply every "best practice" to every situation, especially in cases of small participants that are not required to comply with NERC CIPs. Instead, our risk management approach will be iterative and strive for continuous improvement in a way that is commensurate with the associated risk and compliance needs.
- **Build on the existing MultiSpeak® specification.** We will leverage the resources, experience, and methodologies developed by the MultiSpeak® Initiative over the past decade to optimize the approach to be used to extend interoperability standards to the full range of smart grid requirements.
- **Incorporate, as appropriate, relevant developments as they occur in other standards, protocols, and interfaces under development.** The rapid evolution and significant efforts being applied in all aspects of smart grid development can, when combined with the strong basis represented in the MultiSpeak® specification, lead to superior demonstration results.
- **Understand the importance of vendors.** A key strength of enterprise application interoperability is the existing core of over 50 software vendors supplying utility clients. Their expertise and contributions to developing a comprehensive set of standards will be critical.
- **Realize that the practical application of interoperability and security is key.** It will not be sufficient for the interoperability and security teams to propose standards and activities for demonstration sites. Those proposals must be tested, applied in the field, and refined as needed throughout the demonstration portion of the project.
- **Use existing knowledge to make new efforts more efficient.** We will leverage any cyber security assessments already performed by or on behalf of any of our demonstration participants or vendors. Such results will be used to streamline the risk assessments done in concert with installation, modification, or updating of smart grid components as part of our demonstrations. We will also make available, as appropriate, risk assessment

materials we may produce to assist in future risk management activities by demonstration participants.

- **Do detailed work when necessary and apply lessons learned broadly.** For detailed and time-consuming risk assessment and interoperability activities, we will target demonstration activity types and participant environments that present new or unique challenges. We will do as much analysis as possible using "standard configurations" of common components before installation begins in participant environments. We will take advantage of the knowledge and lessons learned to streamline future assessments and activities, as well as installation efforts.
- **Manage impact and costs closely.** We will pay special attention to the immediate impact and ongoing costs associated with recommended cyber security controls. Since nearly all of our demonstration participants are very small compared with investor-owned utilities, they may find it difficult or impossible to achieve economies of scale with vendors or in performing operational security activities. We will remain cognizant of this as we make cyber security controls recommendations.
- **Motivate vendors as a key to long-term success.** We will actively advise smart grid component vendors to help drive functional cyber security requirements, nonfunctional software security requirements, and interoperability into their product development processes. If possible and appropriate, we will also work with vendors on training regarding secure software development, threat and attack modeling, and detailed security testing in a suitable environment that does not disrupt participant operations. From the other side of the security equation, we will educate our demonstration participants to ask for evidence of cyber security, software security maturity, and interoperability as part of procurements. We will also provide advice on topics such as supply chain security and acquiring products that clearly facilitate meeting statutory and regulatory compliance requirements.

The primary purposes of the American Recovery and Reinvestment Act of 2009 are stimulating the economy and creating and retaining jobs. The NRECA and its team are firmly committed to assisting the DOE in these national goals by providing information to vendors to stimulate development and sales, facilitating product purchases and installation at cooperative utilities, and providing guidance and advice where possible to the thousands of individuals and firms that must become "smart grid aware" in very short order. We collectively thank the DOE for this opportunity.

INTRODUCTION

The National Rural Electric Cooperative Association (NRECA[1]) won an award to support the Department of Energy's (DOE's) Smart Grid Regional Demonstration Program (SGRDP) and the Smart Grid Clearinghouse. The NRECA, through its research arm, the Cooperative Research Network (CRN[2]), supports 930 co-ops in the adoption of new technology and technology applications meant to control costs and improve reliability and service levels. The demonstration project described here strongly supports the DOE as it faces the complexity of developing national use cases for speedy, cost-effective deployment of the smart grid.

The NRECA's project demonstrates diverse smart grid technologies, spanning multiple utilities, geographies, climates, and applications. The project significantly advances interoperability and security across a range of technologies. This diversity is evidenced by the scale and range of technologies included in the planned demonstrations, including a substantial number of smart meter modules, demand response (DR) switches, in-home displays/smart thermostats, ZigBee gateways, voltage sensors, and fault detectors.

This ICSP provides the NRECA demonstration team's approach to identifying and managing certain risks in the smart grid demonstration project awarded as part of the DOE Funding Opportunity Number DE-FOA-0000036. This ICSP provides the high-level plans for achieving interoperability while managing cyber security risk within the NRECA project team demonstrations. In the following sections, this document describes the planned demonstration architectures and the approach for achieving interoperability among the various technologies within the participant environments. It also describes the risk management approach we will take in mitigating the cyber security risks identified before and during the demonstrations.

- Section 2 describes the demonstration architecture.
- Section 3 discusses the interoperability plan.
- Section 4 discusses the cyber security approach.
- Section 5 provides initial cyber security advice for cooperatives.
- Section 6 provides initial cyber security advice for vendors.
- Appendix A includes details on the planned demonstrations.
- Appendix B includes a cross-reference of program objectives and document sections.

DEMONSTRATION ARCHITECTURE

Discussion of the demonstration architecture is divided into two sections: the first deals with enterprise applications, and the second addresses field devices and systems. It is important that a clear focus and perspective be established for the work to be undertaken during this project. One

[1] See http://www.nreca.org/.

[2] See http://www.nreca.org/resources/crn.htm.

way in which that can be accomplished is by placing the project work within a logical conceptual framework and then by introducing increasingly more detailed development plans.

In that regard, we begin the discussion of the demonstration architecture by placing it within the context of the Smart Grid Conceptual Reference Model developed by the NIST. The conceptual reference model is a tool for describing, discussing, and developing the architecture of the smart grid. As envisioned by NIST in its Framework and Roadmap for Smart Grid Interoperability[3]: "The model is a tool for indentifying the standards and protocols needed to ensure interoperability and cyber security, and defining and developing architectures for systems and subsystems with the Smart Grid."

Figure 1 shows the highest level of the conceptual reference model. It provides an overview of seven defined domains relevant to the smart grid and the communication and electrical flows among those domains. We use it here as a descriptive reference to ensure we have a touchstone with ongoing NIST activities.

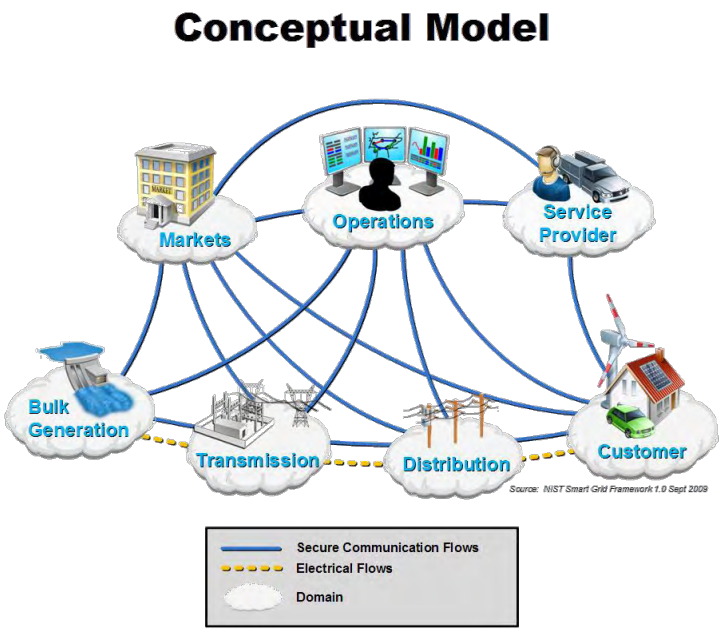


Figure 1. NIST Smart Grid Conceptual Model.

This model comprises seven domains and a variety of "actors." Actors include devices, systems, or programs that make decisions and exchange information necessary for performing applications: smart meters, solar generators, and control systems are examples of devices and systems. Applications are tasks performed by one or more actors within a domain. For example, corresponding applications may be home automation, solar energy generation and energy

[3] National Institute of Standards and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, NIST Special Publication 1108, January 2010.

storage, and energy management. The domains and primary actors constituting this conceptual model are listed in Table 1.

Domain	Actors in the Domain
Consumers	The end users of electricity. May also generate, store, and manage the use of energy. Traditionally, three consumer types are discussed, each with its own domain: residential, commercial, and industrial.
Markets	The operators and participants in electricity markets.
Service Providers	The organizations providing services to electrical consumers and utilities.
Operations	The managers of the movement of electricity.
Bulk Generation	The generators of electricity in bulk quantities. May also store energy for later distribution.
Transmission	The carriers of bulk electricity over long distances. May also store and generate electricity.
Distribution	The distributors of electricity to and from consumers. May also store and generate electricity.

Table 1. Domains and Actors in the NIST Conceptual Model.

Figure 2 provides a more detailed view of the NIST conceptual model.[4] Of course, underlying this model is a legal and regulatory framework that includes policies and requirements that apply to various actors and applications, and to their interactions. Federal, state, and local laws and regulatory guidance drive many aspects of the smart grid.

[4] National Institute of Standards and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, NIST Special Publication 1108, January 2010.

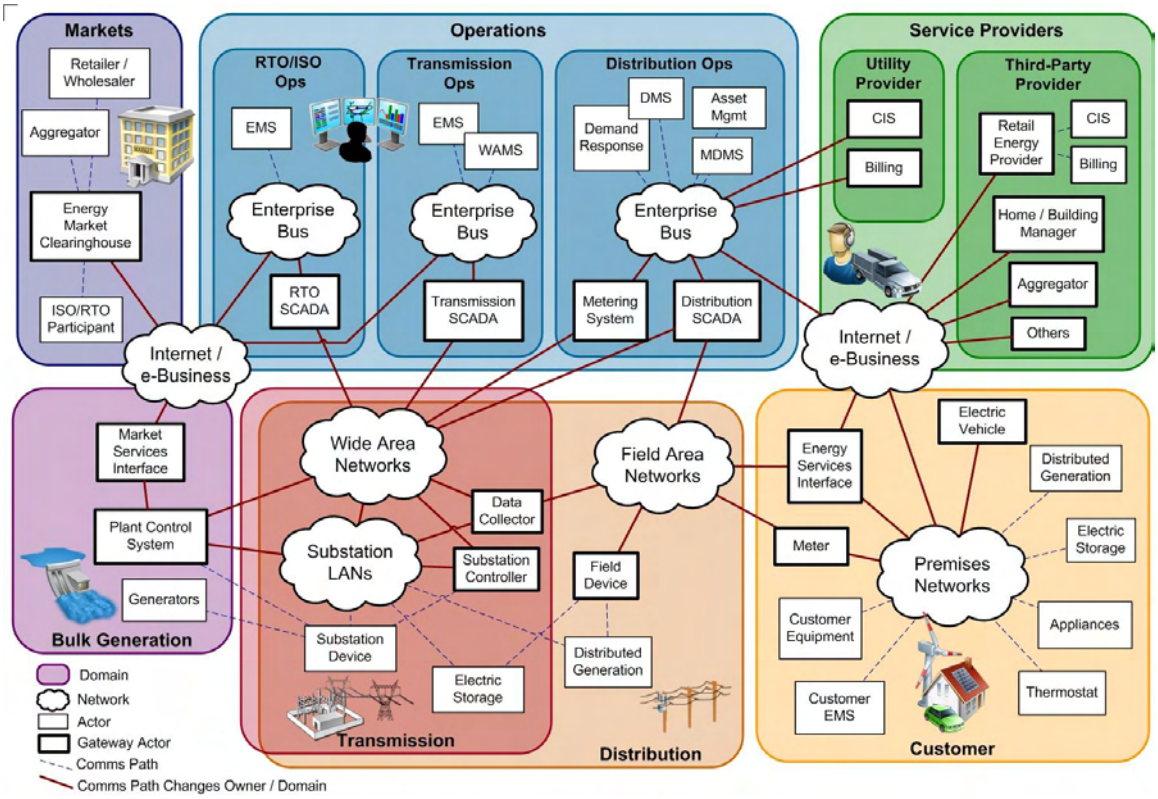


Figure 2. NIST Smart Grid Conceptual Model—Detailed View.

Given these conceptual diagrams as a common backdrop, the following describes the NRECA demonstration architecture.

PHYSICAL AND LOGICAL ARCHITECTURE FOR ENTERPRISE APPLICATION INTEGRATION

LOGICAL ARCHITECTURE FOR ENTERPRISE APPLICATION INTEGRATION

Figure 3 provides significant detail about the specific constituents of four of the NIST domains central to our demonstrations. This figure will be discussed throughout this document, particularly in the detailed discussion of interoperability provided in Section 3. However, we introduce it here to (1) develop an appreciation for the constituent parts of key domains and their interactions, (2) establish an overview of how the project supports compatibility with NIST's emerging smart grid framework for standards and protocols, and (3) provide an organizing methodology and reference numbering system for key actors. As shown in Figure 3, the enterprise application interoperability portion of this demonstration will extensively involve four of the domains as defined in the NIST conceptual model—Markets, Operations, Service Providers/Aggregators, and the distributed storage (DS) and distributed generation (DG) portions of the Distribution domain. Also in Figure 3, numbers A1 through A22 provide reference numbers used throughout this document to refer to specific actors (for example, software applications).

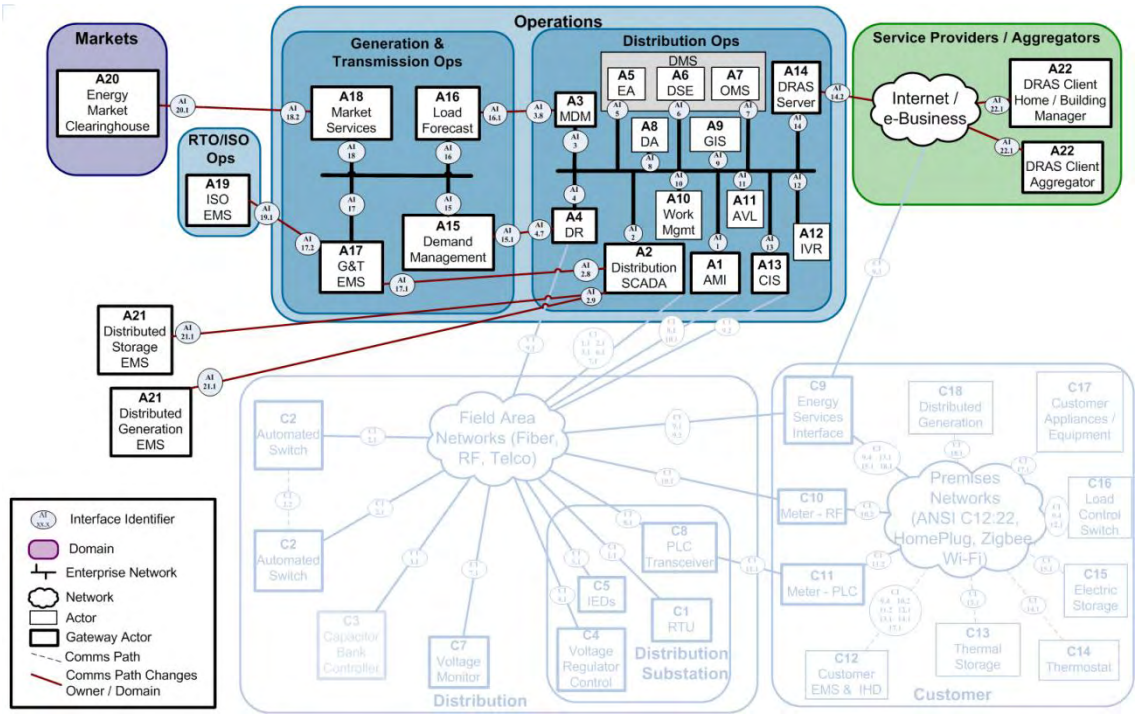


Figure 3. Project Logical Architecture—Enterprise Applications.

In Figure 3, the colored oblongs are the domains corresponding to those in NIST's Smart Grid Conceptual Reference Model. The Operations domain is further divided into three subdomains: Distribution Operations, Generation and Transmission (G&T) Operations, and Regional Transmission Operator/ Independent System Operator (RTO/ISO) Operations. For the purposes of the NRECA project, this further division reflects the fact that it is customary in the electric cooperative market segment to have a division of ownership between the distribution utility operator and the G&T utility operator. However, the same actors and subdomains will be found in vertically integrated utilities as well. In that case, the connections (interfaces) among those actors would be intracompany rather than intercompany relationships. Thus, Figure 3 applies to markets, operations, and service providers for all utilities.

Each box in Figure 3 is an actor. Boxes with lightweight bounding lines are actors that are contained within one domain or subdomain. Boxes with heavyweight lines are gateway actors—those that bridge two domains or subdomains. As far as the discussion of logical architecture is concerned, actors are software applications. For the balance of the discussion in Section 2 and Section 3, the term *application* generally is used rather than *actor*.

Software applications that potentially exchange data within an enterprise network are shown as being connected with heavyweight black lines. Such an exchange of data occurs across interfaces. Enterprise networks may be local area networks (LANs) or wide area networks (WANs) or any combination of the two. When software applications are connected together such that the data flows span the NIST conceptual model domains (or subdomains), then the communications path between the linked gateway actors is shown as a lightweight red line. Table 2 describes each enterprise software application.

Application	Description
(A1) AMI	The advanced metering infrastructure (AMI) system manages communications with meters, typically at consumer locations. The AMI system also often acts to manage consumer loads or to connect, disconnect, or reconnect consumer services.
(A2) Distribution SCADA	Distribution domain supervisory control and data acquisition (SCADA) systems control and obtain data about (typically) distribution substation equipment.
(A3) MDM	Meter data management (MDM) systems typically act as a centralized data management system to store meter readings and meter-related event data, such as consumer outages, meter change-outs, or meter demand resets. MDM systems often are used to validate meter data, including estimating missing data. MDM systems may also include supplemental modules to filter, accumulate, or analyze meter data before it is sent to other systems. In the context of this project, the MDM system may be either (1) a shared system located on the G&T operator network or (2) a system on the network of a single distribution operator.
(A4) DR	Demand response (DR) systems accept demand targets or market price signals from other systems, such as the demand management system (see A15, below), and send control or price signals to other systems, such as the AMI (see A1, above) or the demand response automation server (see A14, below) so that those systems can pass such control or price signals to other systems or to end devices.
(A5) EA	Engineering analysis (EA) accepts facility data and/or power system models from a geographic information system (see A9, below) and operational data such as metered data from AMI (A1, above) or system operations data from distribution SCADA or distribution automation systems (A2, above or A8, below) and performs offline analyses of the data. EA systems are often used for system-planning purposes. EA systems are sometimes deployed as a module of a distribution management system (DMS).
(A6) DSE	Distribution state estimation (DSE) systems are an emerging variety of engineering analysis system that are designed to perform real-time or near-real time analyses of power system models based on actual metered data and system operations data. DSE systems are often deployed as a module of a DMS.
(A7) OMS	The outage management system (OMS) accepts detected outage information from consumer telephone calls, as well as from automated outage detection systems such as the AMI system (A1, above) or the interactive voice response system (A12, below). The OMS system then analyzes the pattern of detected outages based on a power system model and assists a dispatcher in managing crews to restore the affected facilities.

(A8) DA	Distribution automation (DA) systems are similar to distribution SCADA systems (see A2, above) except that DA systems typically control or obtain data from devices down line of the distribution substation.
(A9) GIS	The geographic information system (GIS) stores and displays information about consumers, facilities, and work in a geographic context. The GIS is often used as the central repository for the power system model that is subsequently provided to the EA (A5, above), DSE (A6, above), or OMS (A7, above).
(A10) WM	The work management (WM) system generates and tracks work-related activities. The WM system is often integrated with (1) the AMI (A1, above) or MDM (A3, above) for managing work related to setting, replacing, and retiring meters; (2) the customer information system (A13, below) for managing service or construction work; and (3) the OMS (A7, above) for managing outage restoration.
(A11) AVL	The automatic vehicle location (AVL) system uses global positioning system (GPS) technology to locate utility-owned vehicles and display them in geographic context. AVL system output is often used in the GIS (A9, above), the OMS (A7, above), and the WM (A10, above).
(A12) IVR	The interactive voice response (IVR) system automatically answers consumer calls and routes them to the appropriate department or system for further action. In this context, the IVR is integrated with the OMS (A7, above) to manage consumer outages.
(A13) CIS	The customer information system (CIS) typically consists of several software modules that include a customer database, a bill calculation mechanism, plant inventory, and accounting systems. The CIS must be integrated with many of the systems listed here to provide consumer information and to accept meter readings from the AMI (A1, above) or MDM (A3, above).
(A14) DRAS Server	The demand response automation server (DRAS) is a system that accepts DR targets or market price signals from the DR (A4, above) and implements the open automated demand response (OpenADR) protocol. OpenADR is used to coordinate DR actions with DRAS client systems (A22, below) at consumer facilities or third-party service aggregators.
(A15) DM	The demand management (DM) system accepts DR targets or market price signals from the load forecast system (A16, below) and manages appropriate DR actions with the DR system (A4, above) at each of the distribution utilities.
(A16) Load	The load forecast (LF) system accepts market signals from the market services application (A18, below), calculates the relative value of the output of generation assets and DR

Forecast	resources, and sends DR management targets to the DM system (A15, above).
(A17) G&T EMS	The generation and transmission (G&T) energy management system (EMS) is a system that collects data from and controls G&T assets, acting in a manner similar to a SCADA system.
(A18) MS	The market services (MS) system coordinates market signals with the energy market clearinghouse (A20, below) and sends market information to the LF application (A16, above).
(A19) RTO/ISO EMS	The regional transmission operator (RTO)/independent system operator (ISO) EMS collects information on regional transmission assets and operational conditions and acts to control those transmission assets.
(A20) EMC	The energy market clearinghouse (EMC) is the market system that coordinates with market participants to exchange either price signals or bid and offer information. The EMC system in the market domain communicates with the market services application(s) (A18, above) in the G&T system operator domain.
(A21) DER EMS	The distributed energy resources (DER) energy management system (EMS). This system acts to collect information about the operation of and to control the assets of a DER facility. In the context of this demonstration project, the DER may be either a DG or DS facility. In the context of this demonstration project, it is assumed that the DER EMS will coordinate with the distribution SCADA application (A2, above) in operation at the distribution operator.
(A22) DRAS Client	The DRAS client implements the client portion of the OpenADR protocol, which is used to coordinate DR actions with the DRAS system (A14, above).

Table 2. Description of Enterprise Software Applications.

Note that, like the NIST conceptual model, Figure 3 presents comprehensive logical architecture requirements. In order to be able to carry out the ultimate objectives of the smart grid as currently visualized by the industry, all of the applications will eventually need to be developed and integrated at a particular utility. Although some of the applications and interfaces currently exist, primarily in NRECA's MultiSpeak® specification and within the work of other standards development organizations, many parts of the whole need development. As a result, it is likely that no single cooperative included in this project will—at the end of Phase II—incorporate all of the aspects of the smart grid. A primary goal by the end of Phase II is to have provided at least a first generation tool for use for each of the applications and interfaces.

Thus, by identifying key required actors and communication paths in these four domains, Figure 3 plays a key role in establishing what parts of these systems are currently in place and what parts need to be developed during the project. We explore these subjects in greater detail in Section 3. Topics discussed there include:

- The current state of each interface among actors and the interface capabilities that will require development as part of this demonstration project
- The standards that currently (or will someday) affect each interface
- How we will accommodate those standards during project development
- The process we will use during interface development
- How we will manage interface definition changes during the project

PHYSICAL ARCHITECTURE FOR ENTERPRISE APPLICATION INTEGRATION

Figure 3 shows the logical architecture for enterprise integration that will be required to accomplish the goals of the project. It will be necessary to implement physical networking connectivity among the application endpoints in order to achieve this level of logical integration. Typical LAN, WAN, and Internet networking practices will be followed here. If any of the demonstration sites need assistance to achieve the required physical connectivity, the project participants, in coordination with the vendors of the software applications being installed as part of the project will provide that help.

LOGICAL ARCHITECTURE FOR FIELD DEVICE INTEGRATION

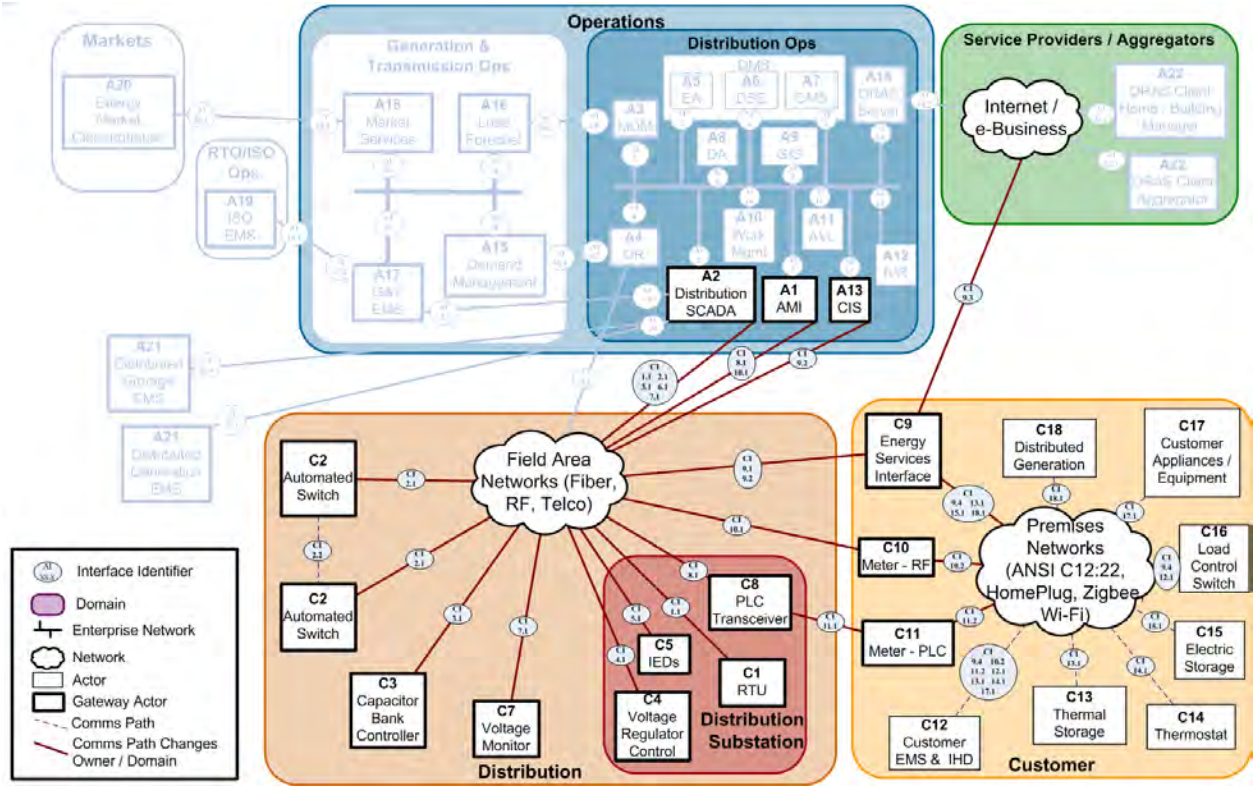


Figure 4 provides an overview of the domains, physical component (device) actors, and component interfaces that comprise our smart grid demonstration activity types. Application actors were defined in the previous section and only those to which a direct physical component interface exists are illustrated. Note that component vendors offer varying levels of integration,

also affecting component interfaces, so the physical and logical architecture will be specific to each implementation.

For the scope of this document, the physical and logical components of the infrastructure networks (wireless field network and LAN) were not illustrated or documented in detail. Rather, the communications networks were treated as "clouds" through which activity type communications are routed to the appropriate component or application. For some activities, such as a wireless mesh AMI network, the communications network is integral to the physical component (meter). The consumer premises communications network, on the other hand, can vary from wireless ZigBee and Wi-Fi to HomePlug and other emerging home area networks (HANs).

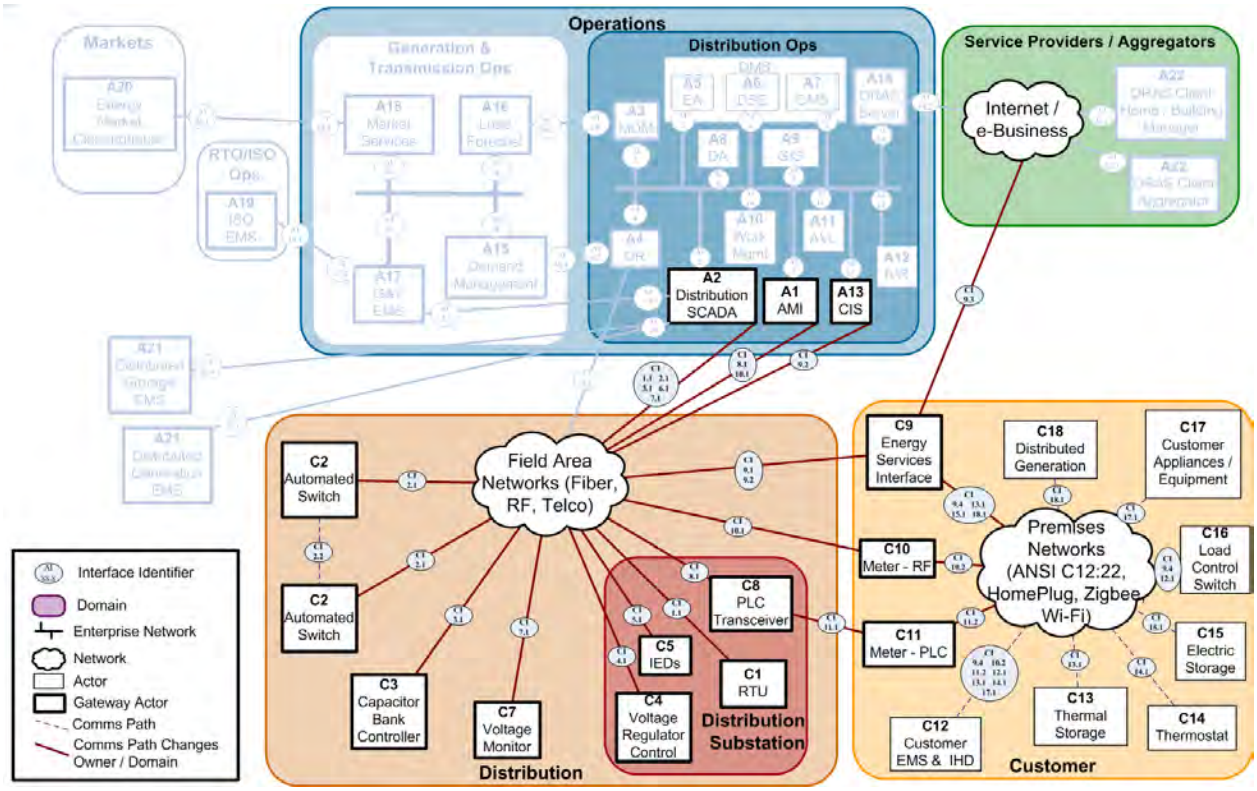


Figure 4. Smart Grid Demonstration Grant Automation Components and Interfaces.

Table 3 provides the definition of the components and interfaces illustrated in

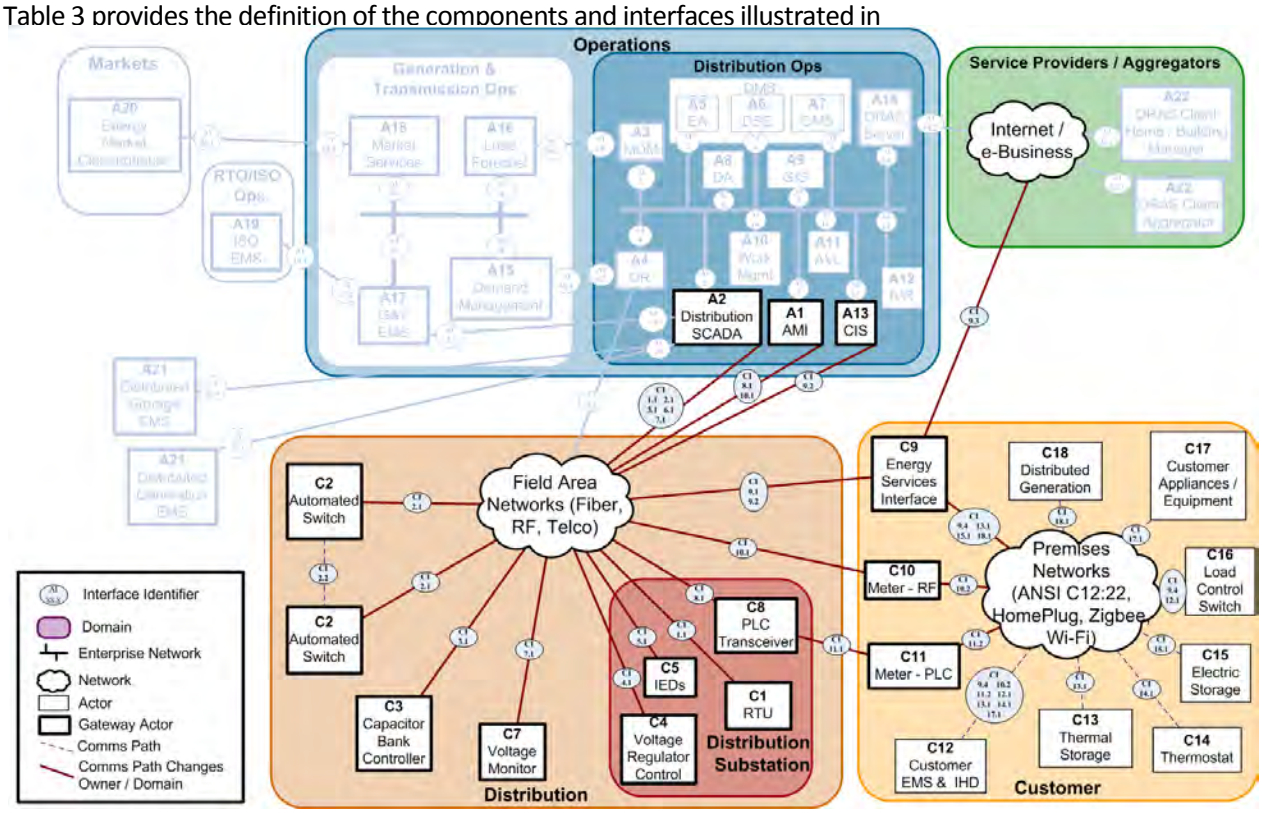


Figure 4, including:

- Components (physical devices) numbers and descriptions
- Components and applications to which each component interfaces within the scope of the activity types
- Interface numbers and high-level descriptions of data exchanged
- Example external standards or an indication of whether communications are proprietary to the vendor

Automation Component #	Automation Component	Component Description	Interfaces With	Interface Number	Data Exchanged	External Standards Used
C1	Remote terminal unit (RTU)	Receives data from sensors and power equipment, and can issue control commands, such as tripping circuit breakers if it senses voltage, current or frequency anomalies, or can raise/lower voltage levels in order to maintain the desired level.	A2) Distribution SCADA module of DMS	CI_1.1	1. Transmit data periodically or upon event 2. Receive control commands	DNP3 IEC 61850
C2	Switch gear	Curcuit opening electrical disconnects, fuses and / or circuit breakers used to deenergize equipment and clear faults downstream.	A2) Distribution SCADA module of DMS	CI_2.1	1. Transmit data periodically or upon event 2. Receive control commands	DNP3 IEC 61850
			C2) Switch gear	CI_2.2	1. Transmit data and commands upon event for local switch control to isolate fault	DNP3 IEC 61850
C3	Capacitor bank controller	Device to control capacitor bank.	A2) Distribution SCADA module of DMS	CI_3.1	1. Transmit data periodically or upon event 2. Receive control commands	DNP3 IEC 61850
C4	Voltage regulator	Responds to set point commands and reports status information and power system measurements.	A2) Distribution SCADA module of DMS	CI_4.1	1. Transmit sensor data periodically or upon event 2. Receive control settings	DNP3 IEC 61850

Automation	Automation	Component Description	Interfaces	Interface	Data Exchanged	External
C5	Intelligent electronic device (IED)	Receives data from sensors and power equipment, and can issue control commands, such as tripping circuit breakers if it senses voltage, current or frequency anomalies, or can raise/lower voltage levels in order to maintain the desired level.	A2) Distribution SCADA module of DMS	CI_5.1	1. Transmit voltage, current or frequency data periodically or upon event 2. Transmit commands, for example for protection such as auto reclose	DNP3 IEC 61850
C7	Voltage monitor	Used to monitor voltage, detect interruption, and monitor power quality.	A2) Distribution SCADA module of DMS	CI_7.1	1. Transmit voltage level data periodically or upon event	DNP3 IEC 61850
C8	PLC transceiver	Device used to inject and extract low-frequency communications on power lines to support bidirectional communication (for AMI supported DR and load control, for example) to downstream devices such as meters.	A1) AMI headend	CI_8.1	1. Commands from AMI head-end (for example, disconnect) 2. Meter data (voltage, kWh)	Ethernet, proprietary vendor data structure
			C11) Meter—PLC	CI_11.1	1. Commands from AMI head-end 2. Meter data (voltage, kWh)	Vendor proprietary PLC protocol
C9	Energy services interface (ESI)/HAN gateway	An interface between the distribution, operations, and consumer domains and the devices within the consumer domain.	C12) Consumer EMS and in-home display (IHD)	CI_9.4	1. Pricing signals (CPP), TOU data, load management commands and/or status	CPP standards in development, load management proprietary, ZigBee smart energy profile (SEP)
			C15) Electric storage	CI_15.1	1. Energy storage status data 2. Energy storage	

Automation	Automation	Component Description	Interfaces	Interface	Data Exchanged	External
					commands	
			C18) Distributed generation —consumer premises	CI_18.1	1. Generation and storage status	
			Internet/e-Business—Web portal	CL_9.3	1. Meter data, energy usage, pricing signals, and so on.	HTTPS
C10	Meter—RF	Utility-owned point-of-sale device used for the transfer of product and measuring usage from one domain/system to another. Communications back to head-end are wireless, either mesh or point-multipoint.	A1) AMI Head-end	CI_10.1	1. Commands from AMI head-end (for example, disconnect) 2. Meter data (voltage, kWh)	Vendor proprietary, American National Standards Institute (ANSI) C12.19
			C12) Consumer EMS and IHD	CI_10.2	1. Meter data (voltage, kWh)	ZigBee, ANSI C12.22, and so on
C11	Meter —PLC	Utility-owned point of sale device used for the transfer of product and measuring usage from one domain/system to another. Communications back to head-end are over the powerline to the substation and then via fiber, microwave, or Telco to operations.	C8) PLC transceiver	CI_11.1	1. Commands from AMI head-end (for example, disconnect) 2. Meter data (voltage, kWh)	Vendor proprietary, ANSI C12.19
			C12) Consumer EMS and IHD	CI_11.2	1. Meter data (voltage, KWH)	ZigBee, ANSI C12.22, and so on.
C12	Consumer EMS with IHD	An application service that communicates with devices in the home. The application service may have interfaces to the meter to report usage	C9) ESI	CL_9.4	1. Pricing signals (CPP), TOU data, load management commands	ZigBee, ANSI C12.22, and so on

Automation	Automation	Component Description	Interfaces	Interface	Data Exchanged	External
		or to the operations domain to get pricing or other information to make automated or manual decisions to control energy consumption more efficiently. The EMS may be a utility subscription service, a consumer-written application, or a manual control by the utility or consumer.			and/or status	
			C10) Meter—RF	CL_10.2	1. Meter data	ZigBee, ANSI C12.22, and so on
			C11) Meter—PLC	CL_11.2	1. Meter data	ZigBee, ANSI C12.22, and so on
			C13) Thermal Storage	CL_13.1	1. Thermal storage status 2. Thermal storage commands	ZigBee, ANSI C12.22, and so on
C13	Thermal storage	Consumer appliance that will respond to load control signals to store or shed electric load as an up-and-down regulation tool. For the demo grant, an interactive water heater control is used.	C12) Consumer EMS and IHD	CL_13.1	1. Thermal storage status 2. Thermal storage commands	Proprietary PLC protocol
C14	Thermostat	A device for regulating the temperature of a system near the desired setpoint by switching heating or cooling devices on or off or regulating the flow of heat transfer fluid.	C12) Consumer EMS and IHD	CL_14.1	1. Thermostat set point 2. Thermostat temperature reading	ZigBee, ANSI C12.22, and so on
C15	Electric storage	Energy storage resources, such as solar or wind, used to store generated energy (located at a consumer site) to interface to the controller (HAN/BAN) to perform any energy-related activity.	C9) ESI	CL_15.1	1. Energy storage status data 2. Energy storage commands	ZigBee, ANSI C12.22, and so on
C16	Load control switch	A remote-controlled relay placed on home appliances, such as water heaters and	C9) ESI	CL_9.4	1. Pricing signals (CPP), TOU data, load	ZigBee, ANSI C12.22, and so on

Automation	Automation	Component Description	Interfaces	Interface	Data Exchanged	External
		air conditioners, that receives a signal from the electric utility to turn power off to the appliance during times of peak electric demand.			management commands and/or status	
			C12) Consumer EMS & IHD	CL_12.1	1. Load control status	ZigBee, ANSI C12.22, and so on
C17	Consumer appliance and equipment	A device or instrument designed to perform a specific function, especially an electrical device, such as a toaster, for household use. An electric appliance or machinery that may have the ability to be monitored, controlled, and/or displayed.	C12) Consumer EMS and IHD	CL_17.1	1. Appliance status and energy usage	ZigBee, ANSI C12.22, and so on
C18	Distributed generation at consumer premises (solar, wind)	Energy generation resources, such as solar or wind, used to generate energy (located at a consumer site) to interface to the controller (HAN/BAN) to perform any energy related activity.	C9) ESI	CL_18.1	1. Generation and storage status	

Table 3. Smart Grid Demonstration Grant Components and Interface Descriptions.

CONSOLIDATED DEMONSTRATION ARCHITECTURE

Figure 5 integrates the combined logical and physical device architectures, illustrating the overall demonstration architecture. The demonstration architecture adds detail to the NIST Smart Grid Conceptual Reference Model to represent the demonstration activity types, which are defined in the next section. Note the breadth of the demonstration encompasses five of the seven domains identified in the NIST conceptual model, with numerous cross-domain interfaces providing significant ICS challenges. While each participant's smart grid demonstration architecture is defined by existing applications, vendor-specific components and technologies, and demonstration activities, the consolidated architecture provides an overall framework for the demonstration project.

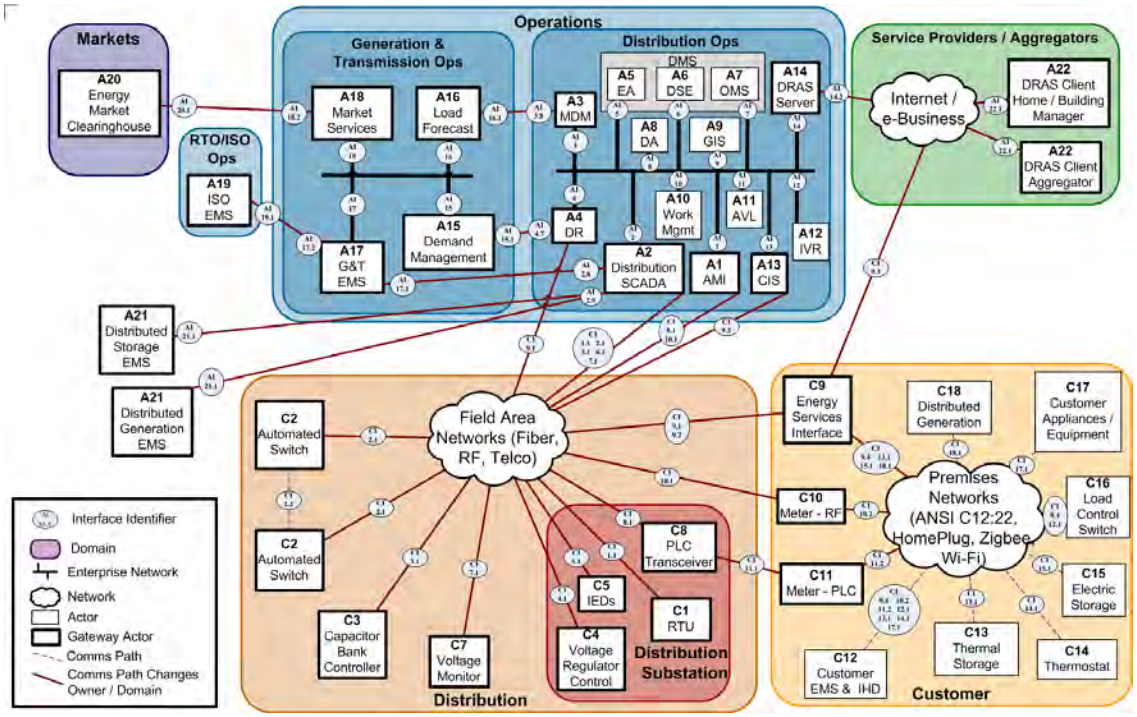


Figure 5. Consolidated Demonstration Architecture.

SMART GRID DEMONSTRATION ACTIVITY TYPES

The NRECA smart grid demonstration includes 10 activity types, comprising 3 general categories (DR, DA, and enabling technologies) and 2 general activity types. We categorize the activity types into DR and DA and describe each category below. Following the descriptions are diagrams of physical and logical interfaces of the two representative activity types. Diagrams and descriptions of all 10 NRECA demonstration activity types are given in Appendix A.

Types	Participants	Demand Response			Distribution Automation			Enabling Technologies			
		IHD/Web Portal Pilots	DR over AMI	Interac-tive Thermal Storage	Smart Feeder Switching	Advanced Volt/Var Control	CVR*	AMI	MDM	Comm	SCADA
Activities	Adams Electric Co-op, IL	X	X		X	X	X	X		X	X
	Adams-Columbia Electric Co-op, WI				X	X	X				X
	Clarke Electric Co-op, Inc., IA	X	X		X		X	X		X	X
	Consumers Energy, IA	X	X					X		X	
	Corn Belt Power Co-op, IA									X	
	Calhoun Co. ECA		X					X			
	Humboldt Co. REC		X					X			
	Iowa Lakes EC		X								
	Midland Power Co-op		X								
	Prairie Energy Co-op		X					X			
	Delaware County Electric Co-op, NY	X	X					X		X	
	Flint EMC, GA	X						X			
	Kaua'i Island Utility Co-op, HI	X	X					X	X	X	
	Menard Electric Co-op, IL	X				X					X
	New Hampshire Electric Co-op, NH	X	X	X				X		X	
	Nolin RECC, KY	X	X		X	X	X	X		X	X
	Owen Electric Co-op, Inc., KY	X	X		X	X	X	X		X	X
	Prairie Power, Inc., IL					X					X
	Salt River Electric Co-op Corp., KY				X						
	Snapping Shoals EMC, GA	X	X		X			X		X	X
	United REMC, IN	X	X		X	X	X		X	X	
	Washington-St. Tammany EC, LA				X					X	X

Table 4. Demonstration Grant Activity Types by Participant.

Note: CVR = conservation voltage reduction.

DEMAND RESPONSE (DR)

- **IHD/Web portal pilots.** This program will study the consumer behavior modifications resulting from varying the energy price signals of residential electricity consumers. Critical peak pricing (CPP), time-of-use pricing (TOU), and a combination of these two rate signals will be studied. We will conduct additional study on the interaction between these dynamic pricing signals and the existence of in-home energy use displays and Internet-based energy use Web portals (WPs). This program will also study the consumer behavior modifications resulting from the availability to consumers of data detailing their electricity use.
- **DR over AMI (water heater and air conditioner direct load control)**. This program will study the load impacts resulting from cooperative direct control of consumer water heaters and air conditioners (ACs). During high cost periods, cooperatives will be able to remotely shut off end-use water heaters and ACs.

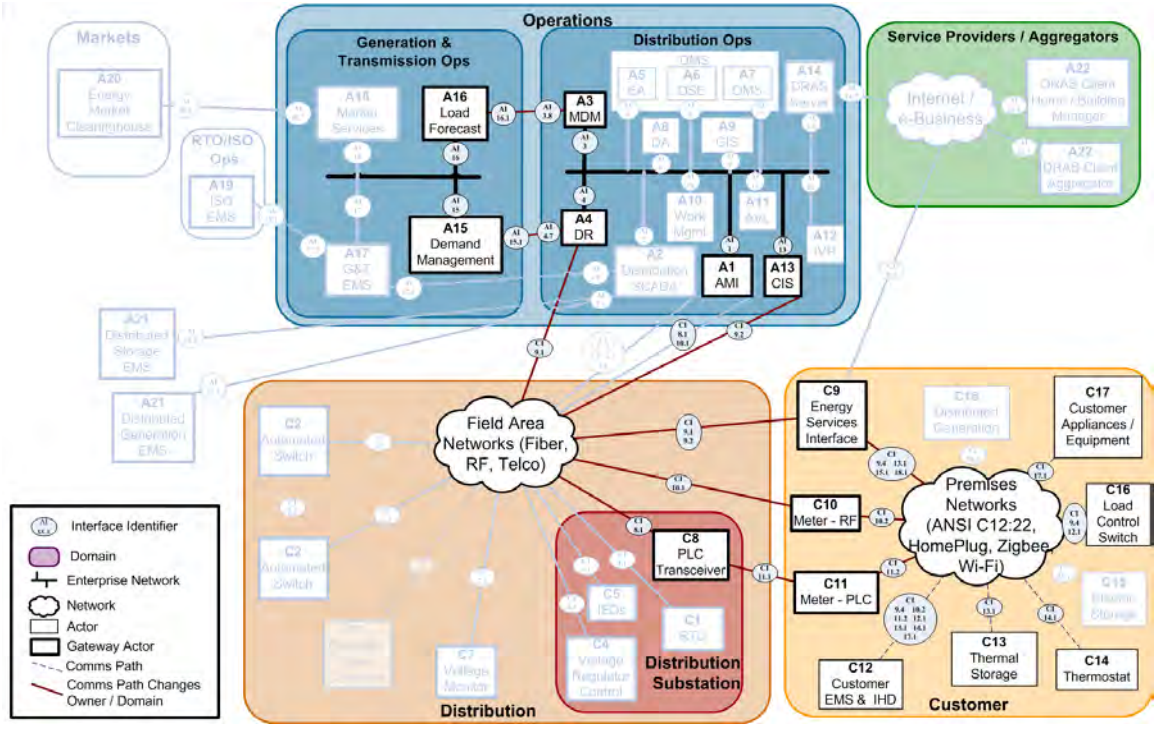


Figure 6. Smart Grid Demonstration Grant Activity Type—Demand Response over AMI.

- **Interactive thermal storage.** This program will study the load impacts resulting from an energy storage device produced by Steffes Corporation, which allows for storage of low-cost energy to heat water heaters during higher-cost times.

DISTRIBUTION AUTOMATION (DA)

- **Smart feeder switching**. Smart feeder switching entails automated network reconfiguration of electrical distribution networks to minimize interruptions and improve system reliability.

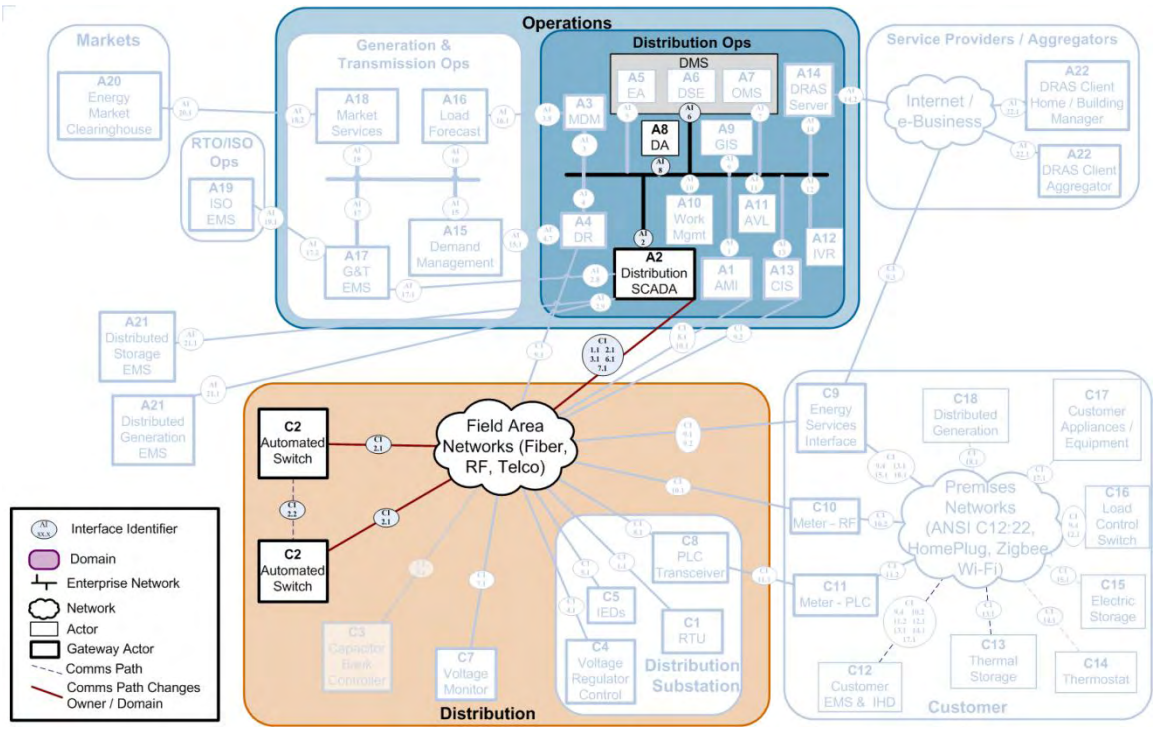


Figure 7. Smart Grid Demonstration Grant Activity Type—Smart Feeder Switching Components and Interfaces.

- **Advanced volt/VAr control.** Volt/VAr control of distribution feeders will result in improved voltage support on long distribution feeders while also minimizing distribution line energy losses.
- **Conservation voltage reduction.** CVR is typically employed to accomplish reduction of peak demand during certain times of the day. Peak demand reduction during co-incident peaks results in substantial wholesale power demand cost savings for utilities.

ENABLING TECHNOLOGIES

We consider the following to be technologies that enable the DR and DA activity types. We include these to facilitate integration with some of our smart grid demonstration participants who already have related technologies.

- **AMI for DR activities.** AMI systems comprise state-of-the-art electronic and digital hardware and software, which combine interval data measurement with continuously available remote communications. These systems enable measurement of detailed, time-based information as well as frequent collection and transmittal of such information to various parties.

  AMI typically refers to a full measurement and collection system that includes meters at the consumer site, communication networks between the consumer and a service provider (such as an electric, gas, or water utility), and data reception and management systems that make the information available to the utility (Source: FERC). AMI is the enabling technology for DR activities.

- **MDM for DR activities.** An MDM system performs long-term data storage and management for the data that are now being delivered by smart metering systems. These data consist

primarily of usage data and events that are imported from AMI systems. A MDM system will typically import the meter data then validate, edit, and evaluate (VEE) to cleanse the data before making it available to end users.

- **Communications (DR and DA activities).** Communication is the means of getting information from one piece of equipment to another. This communication could use microwave, unlicensed spread spectrum, licensed UHF, or any of a number of methods.
- **SCADA (front-end master system).** SCADA provides the basic infrastructure to deploy basic and advanced substation and distribution system automation. It has the potential to vastly improve operational efficiencies, and provides the tools required by operators and engineers to become more productive in their jobs. It is a key component in the process of evolving the smart grid.

INTEROPERABILITY PLAN FOR DEMONSTRATIONS

This section documents the plan for achieving interoperability among enterprise applications and field devices. It lays out how the project, beginning with the firm base provided by the existing MultiSpeak® standard for interoperability, will support compatibility with NIST's emerging smart grid framework for standards and protocols. It provides an extensive model of the applications and devices needed for complete smart grid coverage. It also notes which of those parts currently exist and which need development. Finally, it lays out a schedule for developing the parts required to make available complete smart grid solutions for the utility of the future.

OVERVIEW OF STANDARDS AFFECTING ENTERPRISE APPLICATIONS

A foundational principle of the demonstration project is to base the interoperability features for both enterprise applications and field devices on industry consensus standards. We will pursue this goal where it is practical to do so, where there is sufficient consensus on the appropriate choice among optional standards, and where such standards are mature or are expected to be available in a stable form during the development portion of the project. The critical standard on which we will base enterprise application interoperability is the MultiSpeak® specification (MultiSpeak®), a consensus standard that has been developed, is currently maintained, and is continually refined by the MultiSpeak® Initiative. The MultiSpeak® Initiative is a collaboration of over 50 leading software vendors and service providers along with Cooperative Energy Services (CES), a wholly-owned subsidiary of the NRECA.

INTRODUCTION TO MULTISPEAK®

MultiSpeak® is a standard that defines enterprise application interfaces and has offered guidance to distribution utilities on enterprise application integration since 2000. It consists of (1) a data model documented in unified modeling language (UML) and extensible markup language (XML) schema formats and (2) service definitions defined in Web services description language (WSDL) contracts.

MultiSpeak® is stable and mature in its support of 30 enterprise application integration profiles. It is in operation at over 500 utilities in at least 11 different countries. However, the completion of this demonstration project will entail significant extensions to the existing interfaces and the addition of many new interfaces. The details of these planned developments are outlined in Section 3.2.

The MultiSpeak® Initiative has a strong commitment to the use of well-understood and widely adopted standards and protocols. This is evidenced by the fact that MultiSpeak® Web services make use of:

- XML schema
- Simple object access protocol V1.1 (SOAP)[5]

[5] Simple Object Access Protocol (SOAP) 1.1 – W3C Note 08, May 2000 (http://www.w3.org/TR/2000/NOTE-SOAP-20000508/).

- Web services description language (WSDL) V1.1[6]
- Hypertext transfer protocol (HTTP) V1.1[7]
- Extensible markup language (XML)[8]

Within the standard itself, MultiSpeak® already incorporates such standards as:

- ANSI C12.19/MC19 for revenue metering end-device tables[9]
- Open geospatial consortium GML for exchange of location-based information addressing geographic data requirements[10]

The MultiSpeak® reference architecture is based on the Basic Profile 1.1 (Profile), which was developed by the Web Services Interoperability Organization (WS-I).[11] The Profile is a set of nonproprietary Web service specifications along with clarifications, refinements, interpretations, and amplifications of those specifications, which is designed to promote interoperable Web implementations. Table 5 lists the specifications that are included in the Profile. MultiSpeak® uses all of the standards and protocols that are included in the Profile, except for Universal Description, Discovery, and Integration (UDDI). UDDI is a standard of the Organization for the Advancement of Structured Information Standards (OASIS), which is designed to facilitate the discovery of Web services across distributed, unrelated networks, such as the Internet. The use of UDDI is optional in MultiSpeak®. More information about WS-I and the Profile are available at www.ws-i.org.

Function	Protocol
Schema Definition	XML Schema 1.0
XML Messaging	SOAP 1.1

[6] Web Services Description Language (WSDL) 1.1 – W3C Note 15, March 2001 (http://www.w3.org/TR/wsdl.html).

[7] RFC2616: Hypertext Transfer Protocol (HTTP) 1.1 – Internet Engineering Task Force, June 1999 (http://www.ietf.org/rfc/rfc2616).

[8] Extensible Markup Language (XML) 1.0 – W3C Recommendation 04, Third Edition, February 2004 (http://www.w3.org/TR/REC-xml).

[9] ANSI C12.19, American National Standard For Utility Industry End Device Data Tables, American National Standards Institute (http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+C12.19-2008).

[10] OpenGIS® Geography Markup Language (GML) Implementation Specification, Version 2.1.2., 2002. Open GIS Consortium, Inc.

[11] Basic Profile Version 1.1 – Web Services Interoperability Organization, Final, August 24, 2004 (http://www.ws-i.org/Profiles/BasicProfile-1.1-2004-08-24.html).

Service Description	WSDL 1.1
Service Publication and Discovery	UDDI 2.0
Transport	HTTP 1.0 or 1.1 (HTTP 1.1 is preferred)

Table 5. WS-I Basic Web Services Profile 1.1.

Additional discussion of the MultiSpeak® specification follows in Section 3.1.3. At this point, the discussion will turn to other electric utility industry standards and how they might affect the interoperability features of the demonstration project.

STANDARDS OTHER THAN MULTISPEAK®

NIST SP 1108[12] identifies 75 existing standards that are applicable or likely to be applicable to the ongoing development of the smart grid. A significant subset of those will directly affect work on this project. A considerable completed effort during Phase I of this project has been to investigate existing standards and interfaces that might play a role during the development of the project interface designs. Sources of information have included: (1) discussions with representatives of other standards development organizations (SDOs), (2) participation in various priority action plan (PAP) committees, (3) participation in the Transmission and Distribution Domain Expert Working Group (DEWG), (4) attendance at technical meetings such as the NIST Smart Grid Interoperability Panel, and (5) discussion with affected vendors. Because of those efforts, it has been possible to identify the key standards, protocols, and interfaces we must incorporate into the enterprise application interoperability portion of this project. The standards critical to this project and currently identified by NIST adoption are shown in Table 6. Key standards that NIST has identified for potential future adoption are listed in Table 7.

NIST Identifier #	Standard Designation	Standard Released?	Coverage	How Project Will Incorporate This Standard (See Note)
NIST Table 4-1 Standards				
#2	ANSI C12.19/MC19	Yes	Revenue metering.	Already included in MultiSpeak®.

[12] National Institute of Standards and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, NIST Special Publication 1108, January 2010.

#4	DNP	Yes	Substation and feeder device automation; communications between control centers and substations.	Harmonization between DNP and IEC 61850 (Standard #6) in process; MultiSpeak® will incorporate the resulting standard beginning with V4.3 in calendar year 2011 if it is available.
#5	IEC 60870-6/ TASE.2	Yes	Control center messages.	The project will incorporate TASE.2 directly where appropriate rather than attempting to harmonize MultiSpeak® and TASE.2.
#6	IEC 61850	Yes	Communications T&D substations; being extended to cover communications between distributed resources and substations.	Harmonization between DNP (Standard #4) and IEC 61850 in process; MultiSpeak® will incorporate the resulting standard beginning with V4.3 in calendar year 2011 if it is available.
#7	IEC 61968/ 61970	Yes	Common information model among control centers; EMS interfaces; distribution grid management.	Not part of demonstration; harmonization efforts between IEC61968 and MultiSpeak® are underway in other projects
#13	OpenADR	Yes	Messages between utilities and commercial/industrial consumers.	The project will incorporate OpenADR in the appropriate interface and will develop MultiSpeak® functionality necessary to support the deployment of OpenADR.
#15	Open Geospatial Consortium GML	Yes	Exchange of location-based information addressing geographic data requirements.	Features of GML are already included in MultiSpeak®. Support for GML will be updated and extended as appropriate.
#16	ZigBee HomePlug SEP	V1.0 Yes V2.0 Pending	HAN device communications and information model.	SEP is a home networking standard. MultiSpeak® is a standard for server-to-server communications in the enterprise domain, thus SEP and MultiSpeak® do not directly interface. However, the project will develop MultiSpeak® functionality in such a way that it supports the deployment of ZigBee SEP in the home, beginning with support for SEP 1.0 in MultiSpeak®

				V4.1 in midyear 2010 and SEP 2.0, if available, in MultiSpeak® V4.2 at year-end 2010.
#17	OpenHAN	Early work has been released.	HAN to utility advanced metering systems.	OpenHAN describes system requirements for the home area network. MultiSpeak® is a standard for server-to-server communications in the enterprise domain, thus OpenHAN and MultiSpeak® do not directly interface. However, the project will develop MultiSpeak® functionality in such a way that it will support OpenHAN requirements as they evolve.

Table 6. Standards Critical to this Project.

Note: For details, see Section 3.3.1, which describes the general methodology that will be used to incorporate existing and developing standards as they become available. In addition, see Section 3.3.2, which shows the proposed schedules for future MultiSpeak® releases incorporating or harmonizing with these standards.

NIST Identifier #	Standard Designation	Standard Released?	Coverage	How Project Will Incorporate This Standard (See Note)
NIST Table 4-2 Standards				
#19	IEEE P2030	No	Draft guide for interoperability between the electrical system and end-use applications.	Will monitor developments and incorporate as warranted.
#24	IEEE C37.111-1999	Yes	Transient system data from power system monitoring.	Will monitor developments and incorporate as warranted.
#31	NAESB OASIS	No	Utility business practices for transmission service.	Will be incorporated as appropriate when available.
#32	NAESB WEQ 015	No	Utility business practices for DR.	Will be incorporated as appropriate when available.
#34	OASIS EMIX	No	Exchange of market information	Will be incorporated as appropriate when

			such as price, characteristics, time, and related information.	available.
#36	OASIS oBIX	No	General Web service specification for communication with control systems.	Will be incorporated as appropriate when available.
#37	OASIS	No	Communication specification for schedule and interval.	Will be incorporated as appropriate when available.

Table 7. Potential Future NIST Standards Important to the Project.

Note: For details, see Section 3.3.1, which describes the general methodology that will be used to incorporate existing and developing standards as they become available. In addition, see Section 3.3.2, which shows the proposed schedules for future MultiSpeak® releases incorporating or harmonizing with these standards.

For clarity, Tables 6 and 7 use the NIST standard number from either Table 4-1 ("Standards Identified by NIST") or Table 4-2 ("Additional Standards, Specifications, Profiles, Requirements, Guidelines, and Reports for Further Review ") of NIST SP1108.

MULTISPEAK® STANDARD

As noted above, the existing MultiSpeak® standard contains a significant number of interfaces that will be required to implement the smart grid functionality. This existing core of the MultiSpeak® standard will be critical to the work on this project. Because of the existence of these capabilities, the project can focus primarily on new developments. A key strength of this project is that it has an existing team of over 50 vendors in the form of the MultiSpeak® Initiative Technical Committee, along with existing development procedures, methodologies, and structures for adding to the MultiSpeak® standard. Since many of the vendors have already implemented interoperable products based on MultiSpeak®, it will be easier to add support for the new developments than if the same vendors had to build support for other potential standards from the ground up.

The existing MultiSpeak® standard can be best understood in the form of an enterprise bus representation, as shown in Figure 8.

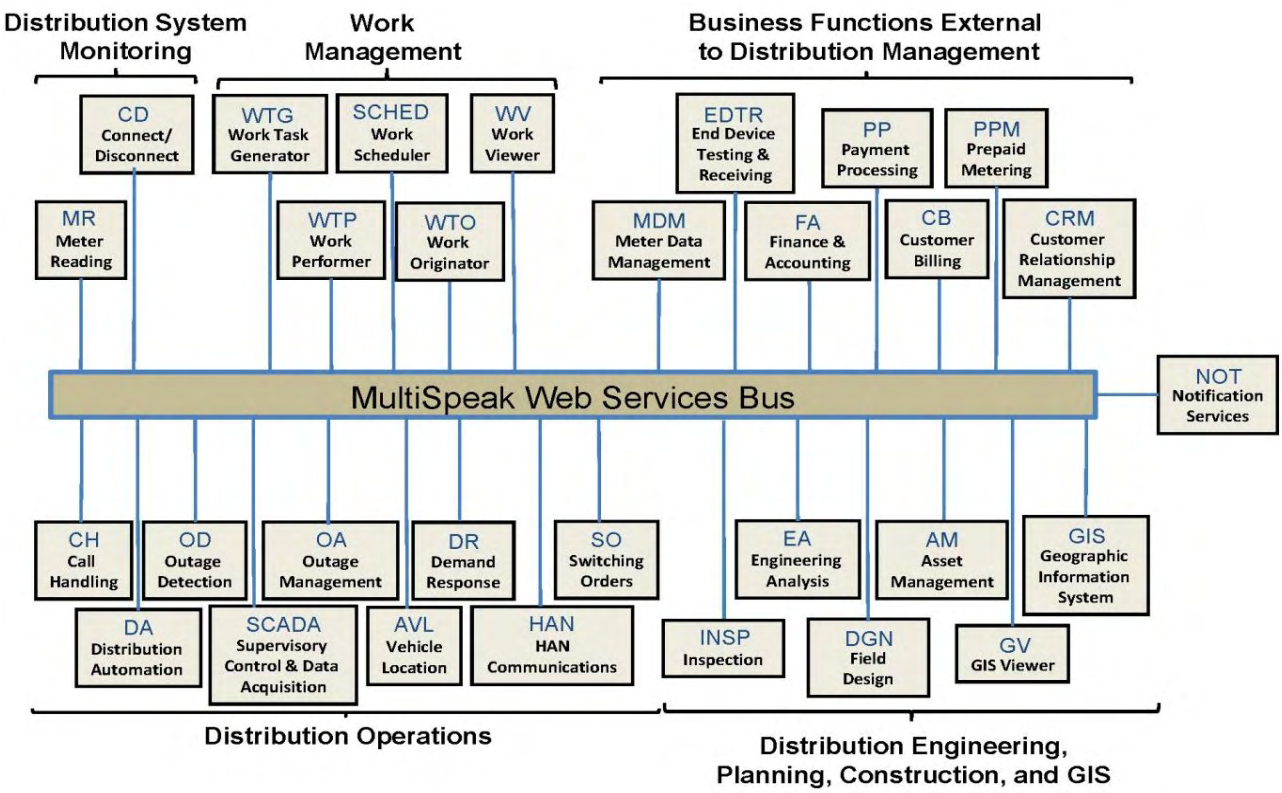


Figure 8. MultiSpeak® as an Enterprise Service Bus.

Each of the boxes in Figure 8 represents a single abstract software function that is currently supported in MultiSpeak®. Any given piece of application software can implement one or more abstract functions as appropriate. In some cases, such as for a GIS, the application likely would implement only a single function, the GIS server. In other cases, an enterprise application might implement many abstract functional capabilities. For instance, an AMI system would implement a meter reading (MR) server and might also implement connect/disconnect (CD), outage detection (OD), DR, HAN communications, DA, and/or prepaid metering (PPM) servers.

Note that each physical software application (for instance, AMI) would be a single actor, despite the fact that it might implement one or more abstract MultiSpeak® software functions when represented in the MultiSpeak® enterprise service bus representation.

Each of the software functions of an application is physically implemented using a Web server endpoint that uses the MultiSpeak®-defined data objects and service definitions along with the Web standards and protocols discussed in Section 3.1.1. Thus, a single application might implement one or more distinct Web service endpoints. This approach facilitates modular development. In addition, since each version of MultiSpeak® is deployed in its own namespace, it is possible for a single application to implement interfaces that support a number of different versions of MultiSpeak® merely by deploying Web services endpoints that support different versions, each in their distinct namespace. This makes it possible for a single application to interface with a number of other applications that support several different versions of MultiSpeak®, each using the version of the defined services that would be appropriate for that

application. This capability will be used extensively during the project to facilitate versioning and support the dynamic updates that will be necessary during the rapid development cycle of new capabilities and implementation at numerous sites with different versions of different applications installed. See further discussion on the topics of versioning and backward capability in Section 3.7.

Figure 8 shows the abstract representation of application interconnectivity that is labeled "MultiSpeak® Web Services Bus." Physical implementations at a utility could be simply point-to-point interconnections between Web server endpoints, or could be a more complex middleware implementation such as an enterprise service bus, depending on the needs of each utility.

REQUIREMENTS FOR ENTERPRISE APPLICATION INTEGRATION DEVELOPMENT

REQUIRED INTERFACES AND INTEGRATION REQUIREMENTS

Interoperability implies the exchange of data among software applications; such exchange will occur across interfaces between applications. New interfaces must be developed—and existing MultiSpeak® interfaces will need to be enhanced—in order to achieve the goals of the project. This section looks at the required interfaces and integration requirements.

Figure 9 shows the anticipated enterprise interfaces. The application interface (AI) numbers shown in small circles indicate the required AIs among applications (As). We provide more detail on each in Table 9.

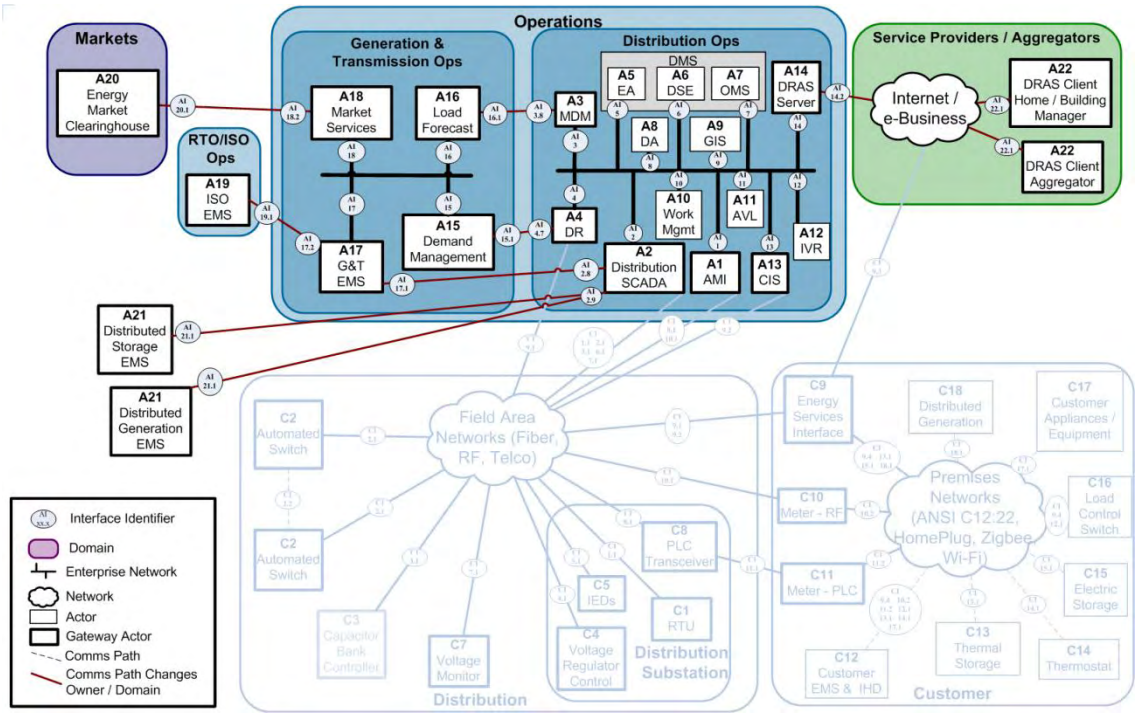


Figure 9. Project Integration Development Requirements—Enterprise Applications.

For applications that integrate only with other applications in the same domain (or subdomain), thereby enabling communication between the applications over an enterprise network, the interface is shown with a solid black line and is labeled using an application interface identifier (AI-#), as detailed in Table 9. For instance, for the AMI application, the application interface is labeled AI 1. As there are multiple interfaces to support all of the information flows within the Distribution Operations domain between the AMI application and other applications, each of these constituent interfaces is further refined as AI 1.1 (AMI to MDM), AI 1.2 (AMI to DR), AI 1.3 (AMI to EA), and so on. For clarity, these finer divisions are not specifically drawn.

In contrast, for interfaces between gateway actors, that is to say those interfaces that span domains or subdomains, the required communications links are shown as a red line and the interface is labeled with the detailed interface numbers (AI X.X format). For instance, between the EMC application (A20) in the Markets domain and the MS application (A18) in the G&T Operations domain, the interface is labeled as AI 20.1 on the EMC application (A20) end and AI 18.2 on the MS application (A18) end.

Table 9 provides detailed information on all of the interfaces anticipated during the project. Note that some of the numbers in Column 3 are shaded and others are unshaded. Shaded boxes are those for which existing MultiSpeak® standards currently exist. Those that are unshaded show interfaces that will be developed as part of the project. All interfaces, existing or to be developed, will be iteratively updated during the project period to reflect needed refinements or to harmonize with complementary standards.

The table lists standards that will be considered for harmonization with the identified interface during the project development. Note that several outside standards could affect many of these interfaces. In many cases, a single interface might be affected by standards that are being developed by as many as five different SDOs. All of these SDOs will be acting on their own schedules and all also will be trying to take into account the work being delivered independently by outside SDOs. It may be difficult to adapt to the schedules of all of these interrelated SDOs during the period of project development. In Section 3.3 we lay out a process for maximizing the chances of successful harmonization with the output of other SDOs.

Table 9 also categorizes the level of cyber security risk inherent in each planned interface, based on the type of data currently anticipated to be exchanged over that interface. In each case, we define the classes of risk associated with each interface (as shown in Table 8).

Cyber Security Risk Level	Class of Cyber Security Risk	Abbreviation for Class of Cyber Security Risk
1	**Safety** (risk to life and limb)	S
2	**Outage** (leading to improper operation of a power system device, possibly resulting in a consumer outage)	O
3	**Privacy** (potentially disclosing private data, such as consumer social security or credit card numbers)	P

4	**Monetary** (potentially leading to increased tangible costs to the utility)	M

Table 8. Cyber Security Risk Levels.

In each case, the highest class of risk that is associated with an interface determines the "cyber security risk level" rating for that interface.

Application	Interfaces With	Interface Number	External Standards	Cyber security Risk Level
A1) AMI	A3) Meter Data Management	AI 1.1	ZigBee SEP (1.0, 2.0), IEC 61968, Part 9, C12.19	2 (O, P, M)
	A4) Demand Response	AI 1.2	ZigBee SEP (1.0, 2.0), IEC 61968, Part 9, C12.19	2 (O, P, M)
	A5) Engineering Analysis	AI 1.3	IEC 61968, Part 9, C12.19	4 (M)
	A6) Distribution State Estimation	AI 1.4	IEC 61968, Part 9, C12.19	2 (O, P, M)
	A7) Outage Management System	AI 1.5	IEC 61968, Part 9, C12.19	2 (O, P, M)
	A13) Customer Information System	AI 1.6	ZigBee SEP (1.0, 2.0), IEC 61968, Part 9, C12.19	2 (O, P, M)
A2) Distribution SCADA	A3) Meter Data Management	AI2.1		2 (O, M)
	A4) Demand Response	AI 2.2		2 (O, P, M)
	A5) Engineering Analysis	AI 2.3		2 (O, M)
	A6) Distribution State Estimation	AI 2.4		2 (O, M)
	A7) Outage Management System	AI 2.5		2 (O, P, M)
	A8) Distribution Automation	AI 2.6	ICCP (TASE.2)	1 (S, O, P, M)
	A9) Geographic Information System	AI 2.7		2 (O, M))

	A17) G & T EMS	AI 2.8	ICCP (TASE.2)	1 (S, O, P, M)
	A21) DER EMS	AI 2.9	ICCP (TASE.2), DNP3	1 (S, O, P, M)
A3) MDM	A1) Advanced Metering Infrastructure	AI 3.1	ZigBee SEP (1.0, 2.0), IEC 61968, Part 9, C12.19	2 (O, P, M)
	A2) Distribution SCADA	AI 3.2		2 (O, M)
	A4) Demand Response	AI 3.3	ZigBee SEP (1.0, 2.0), IEC 61968, Part 9, C12.19	2 (O, P, M)
	A5) Engineering Analysis	AI 3.4	IEC 61968, Part 9, C12.19	4 (M)
	A6) Distribution State Estimation	AI 3.5	IEC 61968, Part 9, C12.19	2 (O, P, M)
	A7) Outage Management System	AI 3.6	IEC 61968, Part 9, C12.19	2 (O, P, M)
	A13) Customer Information System	AI 3.7	ZigBee SEP (1.0, 2.0), IEC 61968, Part 9, C12.19	2 (O, P, M))
	A16) Load Forecast	AI 3.8	NAESB and OASIS (Price and Schedule)	3 (P, M)
A4) Demand Response	A1) Advanced Metering Infrastructure	AI 4.1	ZigBee SEP (1.0, 2.0), IEC 61968, Part 9, C12.19	2 (O, P, M)
	A2) Distribution SCADA	AI 4.2		2 (O, P, M)
	A3) Meter Data Management	AI 4.3	ZigBee SEP (1.0, 2.0), IEC 61968, Part 9, C12.19	2 (O, P, M)
	A9) Geographic Information System	AI 4.4		2 (O, P, M)
	A13) Customer Information System	AI 4.5	ZigBee SEP (1.0, 2.0), IEC 61968, Part 9, C12.19, NAESB and OASIS (Price and Schedule)	2 (O, P, M)
	A14) Demand Response Automation Server (DRAS)	AI 4.6	NAESB and OASIS (Price and Schedule), OpenADR	2 (O, P, M)
	A15) Demand Management	AI 4.7	NAESB and OASIS (Price and Schedule)	3 (P, M)

A5) Engineering Analysis	A1) Advanced Metering Infrastructure	AI 5.1	IEC 61968, Part 9, C12.19	4 (M)
	A2) Distribution SCADA	AI 5.2		2 (O, M)
	A3) Meter Data Management	AI 5.3	IEC 61968, Part 9, C12.19	4 (M)
	A7) Outage Management System	AI 5.4		2 (O, P, M)
	A9) Geographic Information System	AI 5.5		4 (M)
	A13) Customer Information System	AI 5.6		4 (M)
A6) DSE	A1) Advanced Metering Infrastructure	AI 6.1	IEC 61968, Part 9, C12.19	2 (O, P, M)
	A2) Distribution SCADA	AI 6.2	ICCP, TASE.2	2 (O, M)
	A3) Meter Data Management	AI 6.3	IEC 61968, Part 9, C12.19	2 (O, P, M)
	A7) Outage Management System	AI 6.4		2 (O, P, M)
	A8) Distribution Automation	AI 6.5		2 (O, M)
A7) OMS	A1) Advanced Metering Infrastructure	AI 7.1	IEC 61968, Part 9, C12.19	2 (O, P, M)
	A2) Distribution SCADA	AI 7.2		2 (O, P, M)
	A3) Meter Data Management	AI 7.3	IEC 61968, Part 9, C12.19	2 (O, P, M)
	A5) Engineering Analysis	AI 7.4		2 (O, P, M)
	A6) Distribution State Estimation	AI 7.5		2 (O, P, M)
	A8) Distribution Automation	AI 7.6		1 (S, O, P, M)
	A9) Geographic Information	AI 7.7		2 (O, P, M)

	System			
	A10) Work Management	AI 7.8		1 (S, O, P, M)
	A11) Automatic Vehicle Location	AI 7.9		4 (M)
	A12) Interactive Voice Response	AI 7.10		2 (O, P, M)
	A13) Customer Information System	AI 7.11		2 (O, P, M)
A8) Distribution Automation	A2) Distribution SCADA	AI 8.1	ICCP (TASE.2)	1 (S, O, P, M)
	A6) Distribution State Estimation	AI 8.2		2 (O, M)
	A7) Outage Management System	AI 8.3		1 (S, O, P, M)
A9) GIS	A2) Distribution SCADA	AI 9.1		2 (O, M)
	A4) Demand Response	AI 9.2		2 (O, P, M)
	A5) Engineering Analysis	AI 9.3		4 (M)
	A7) Outage Management System	AI 9.4		2 (O, P, M)
	A13) Customer Information System	AI 9.5		2 (O, P, M)
A10) Work Management	A7) Outage Management System	AI 10.1		1 (S, O, P, M)
	A11) Automatic Vehicle Location	AI 10.2		4 (M)
	A13) Customer Information System	AI 10.3		2 (O, P, M)
A11) AVL	A7) Outage Management System	AI 11.1		4 (M)

	A10) Work Management	AI11.2		4 (M)
A12) IVR	A7) Outage Management System	AI 12.1		2 (O, P, M)
	A13) Customer Information System	AI 12.2		2 (O, P, M)
A13) CIS	A1) Advanced Metering Infrastructure	AI 13.1	ZigBee SEP (1.0, 2.0), IEC 61968, Part 9, C12.19	2 (O, P, M)
	A3) Meter Data Management	AI 13.2	ZigBee SEP (1.0, 2.0), IEC 61968, Part 9, C12.19	2 (O, P, M)
	A4) Demand Response	AI 13.3	ZigBee SEP (1.0, 2.0), IEC 61968, Part 9, C12.19, NAESB and OASIS (Price and Schedule)	2 (O, P, M)
	A5) Engineering Analysis	AI 13.4		4 (M)
	A7) Outage Management System	AI 13.5		2 (O, P, M)
	A9) Geographic Information System	AI 13.6		2 (O, P, M)
	A10) Work Management	AI 13.7		2 (O, P, M)
	A12) Interactive Voice Response	AI 13.8		2 (O, P, M)
A14) DRAS Server	A4) Demand Response	AI 14.1	NAESB and OASIS (Price and Schedule), OpenADR	2 (O, P, M)
	A22) DRAS Client	AI 14.2	OpenADR	2 (O, P, M)
A15) Demand Management	A4) Demand Response	AI 15.1	NAESB and OASIS (Price and Schedule)	3 (P, M)
	A16) Load Forecast	AI 15.2	NAESB and OASIS (Price and Schedule)	4 (M)
A16) Load Forecast	A3) Meter Data Management	AI 16.1	NAESB and OASIS (Price and Schedule)	3 (P, M)
	A15) Demand Management	AI 16.2	NAESB and OASIS (Price and Schedule)	4 (M)

	A18) Market Services	AI 16.3	NAESB and OASIS (Price and Schedule)	4 (M)
A17) G&T EMS	A2) Distribution SCADA	AI 17.1	ICCP (TASE.2)	1 (S, O, P, M)
	A19) ISO EMS	AI 17.2	ICCP (TASE.2)	1 (S, O, P, M)
A18) Market Services	A16) Load Forecast	AI 18.1	NAESB and OASIS (Price and Schedule)	4 (M)
	A20) EMC	AI 18.2	NAESB and OASIS (Price and Schedule)	4 (M)
A19) ISO EMS	A17) G&T EMS	AI 19.1	ICCP (TASE.2)	1 (S, O, P, M)
A20) Energy Market Clearinghouse	A18) Market Services	AI 20.1	NAESB and OASIS (Price and Schedule)	4 (M)
A21) Distributed Energy Resources EMS	A2) Distribution SCADA	AI 21.1	ICCP (TASE.2), DNP3	1 (S, O, P, M)
A22) DRAS Client	A14) DRAS Server	AI 22.1	OpenADR	2 (O, P, M)

Table 9. Enterprise Application Interfaces.

Note: The shaded boxes in Column 3, "Interface Number," indicate those interfaces that currently exist in MultiSpeak®. Thus, unshaded boxes show which interfaces will need to be developed during the project. See Table 9 *and Table 10 for further information. All interfaces, existing or new, will be iteratively updated as needed to reflect needed refinements or to harmonize with complementary standards.*

Cyber security risk levels, provided in the last column, show the level of security concern with the exchange of data over this particular interface. The values are 1 (Safety concern), 2 (Outage concern), 3 (Privacy concern), and 4 (Monetary concern).

Many of the interfaces that will be required to accomplish the goals of the project already exist in MultiSpeak®; however, some existing interfaces will require enhancements. Some new interfaces will also be required. Table 10 details the interface developments that will be required in order to accomplish the goals of the DR portion of the demonstration project. Table 11 details interface development required for the DA demonstration.

Interface	Domains Affected	Applications	Business Requirements	Development Required

Interface	Domains Affected	Applications	Business Requirements	Development Required
AI 20.1 – AI 18.2	Markets, G&T	EMC MS	This interface is between the market and the G&T consisting of either capacity price signals or a bid and offer system, depending on the ISO market-clearing protocol.	New interface.
AI 19.1 – AI 17.2	ISO/RTO, G&T	G&T EMS, ISO/RTO EMS	This interface exchanges EMS information as necessary between the G&T and the ISO/RTO.	New interface.
AI 18.1 – AI 16.3	G&T	MS, LF	This interface coordinates the resources available (whether generation or DR) and the price of those resources with the ISO market-clearing mechanism.	New interface.
AI 16.1 – AI 3.8	G&T, Distribution Operator	LF, MDM	This interface enables the load forecast system to obtain historical metered load information from the MDM system.	Modifications to existing MultiSpeak® MDM interface.
AI 16.2 – AI 15.2	G&T	LF, DM	Once the load forecast application determines the level of DR resources necessary, the DM application coordinates with the distribution operator(s) the DR actions necessary.	New interface.
AI 15.1 – AI 4.7	G&T, Distribution Operator	DM, DR	The DM application issues direct load control, DR signals, and/or price signals to accomplish the required DR actions. The DR system accomplishes the required actions and reports back to the load management system on the amount of DR actually achieved.	Modifications to existing MultiSpeak® DR interface.
AI 2.9 – AI 21.1	Distribution Operator, DG, Storage	SCADA, DG EMS, Storage EMS	These interfaces enable the SCADA system to communicate with the EMS at the DG and/or storage resources. The SCADA system must be able to (1) obtain status and analog data from the distributed energy resources (DER), (2) pass along control signals or price signals from the DR system at the distribution operator to the DG/storage resources, and (3) take control actions to bring the	Modifications to existing MultiSpeak® SCADA interface.

Interface	Domains Affected	Applications	Business Requirements	Development Required
			DER into play where necessary to optimally manage the distribution grid.	
AI 4, AI 13, AI 1, AI 3	Distribution Operator	DR, CIS, AMI, MDM	These interfaces permit the AMI, CIS, and DR systems to interact so that pricing signals or DR actions can be transmitted to the consumer premise via the AMI headend, and feedback on demand actions taken by consumers can be returned to the DR and eventually the load management system at the G&T. Furthermore, metered load and meter events must be passed back to the MDM system for subsequent delivery to the load forecast application.	Modifications to numerous existing MultiSpeak® interfaces.
AI 4.6 – AI 14.1	Distribution Operator	DR, DRAS	The DR application must be able to pass demand control and/or price signals to the DRAS so that it can coordinate DR actions with third-party service providers and/or industrial consumers.	New interface.
AI 14.2 – AI 22.1	Distribution Operator, Service Provider	DRAS, DRAS Client	The DRAS at the distribution operator must be able to send DR actions or pricing signals to the third-party service provider and get in return receive demand bids or feedback on consumer DR actions that were aggregated by the service provider.	New interface.

Table 10. Required Interface Development for the Demand Response Activities.

Interface	Domains Affected	Applications	Business Requirements	Development Required
AI 17.1 – AI 2.8	G&T, Distribution Operator	G&T EMS, SCADA	The EMS at the G&T must be able to exchange status and analog measurements with the SCADA system at the distribution operator so that each system is aware of the state of the grid operated by	New interface.

Interface	Domains Affected	Applications	Business Requirements	Development Required
			the other party. Furthermore, each control system must be able to request the other to take control actions on its behalf in order to relieve power system bottlenecks or to optimize volt/VAr flow.	
AI 5, 6, 7 AI 2 AI 8, AI 1, 3	Distribution Operator	DMS, SCADA, DA, AMI/MDM	The DSE module of the DMS gathers information on the state of the system using the SCADA, down line distribution automation systems, and the AMI (and/or MDM) system. The DSE then calculates the optimal configuration of the distribution system based on current conditions and send control actions to the SCADA and DA systems for implementation.	Modifications to numerous existing MultiSpeak® interfaces.

Table 11. Required Interface Development for the Distribution Automation Activities.

REQUIRED MULTISPEAK® SERVERS

Section 3.2.1 identified the domains, applications (actors), and interfaces that will require development during the project. It should be noted that the discussion in Section 3.2.1 focused on software applications (actors), but the MultiSpeak® specification is developed in terms of abstract software functions. This section translates the needs developed in Section 3.2.1, as expressed from the application perspective, into requirements for additions, modifications, and enhancements to the abstract software functions used in the MultiSpeak® specification.

The existing MultiSpeak® standard coverage will need to be augmented with work on a number of additional abstract software functions (servers) to be developed, as shown in Tables 12 and 13, to meet the requirements discussed in Section 3.2.1. Since the MultiSpeak® servers implement abstract software functionality, it is possible that different software vendors will package the functionalities provided in these new MultiSpeak® servers in different manners. Thus, it is possible that different applications (actors) will actually implement the new capabilities when they are deployed as part of the project. This flexibility is one of the strengths of the abstract formulation inherent in the MultiSpeak® design pattern; it permits different vendors to mix and match capabilities in innovative approaches that were not anticipated at the time of the original development of the specification.

Server Designation	Server Name	Description	Application (Actor) That Will Likely Implement This Server

CP	Commissioning and Provisioning	This server coordinates utility commissioning and provisioning of new HANs and new HAN devices.	AMI
DER EMS	Energy Management System at Distributed Energy Resources	The EMS at a DG or DS facility (jointly referred to as distributed energy resources, DER).	DER EMS
DM	Demand Management	The DM function communicates the actions necessary to the DR server at the distribution operator. Actions may include price signals, direct load control signals, and peak alerts.	
DRAS System/Client	Demand Response Automation Server System/Client	The system that coordinates DR signals using the OpenADR standard protocol to third-party service providers/aggregators or commercial and industrial facilities.	DRAS System/Client
EMC	Energy Market Clearinghouse	This is the function that manages the energy and ancillary services market.	EMC
G&T EMS	Energy Management System at Generation and Transmission Operator	EMS at the G&T operator.	G&T EMS
LF	Load Forecast	This function forecasts next-day and next-hour energy and demand requirements based on historical trends and weather data.	LF
MM	Message Management	This server generates new messages to be displayed on HAN devices, such as in-home displays. The MM would issue new messages to the HAN communications server to facilitate display on end devices.	CIS and/or DR

MS	Market Services	This is the function that bids energy, capacity, and ancillary services into the market.	MS
PM	Price Management	This server would interface with the market, the DR server, and the G&T DM server.	CIS and/or DR

Table 12. New MultiSpeak® Servers—Demand Response Support.

Server Designation	Server Name	Description	Application (Actor) That Will Likely Implement this Server
DER EMS	Energy Management System at Distributed Energy Resources	The EMS at a DG or DS (jointly referred to as distributed energy resources, DER).	DER EMS
DSE	Distribution State Estimator	The function of a DMS that performs real-time state estimation on the distribution system.	DSE
G&T EMS	Energy Management System at Generation and Transmission Operator	EMS at the G&T operator.	G&T EMS

Table 13. New MultiSpeak® Servers—Distribution Automation Support.

ENTERPRISE APPLICATION INTEROPERABILITY: PROCESS STEPS AND SCHEDULE

DEMONSTRATION PROJECT PROCESS: STEPS DELINEATED TO ACHIEVE THE APPLICATION INTEROPERABILITY OBJECTIVES

This section describes the flowchart of steps that will be followed for each new interface and for enhancing existing MultiSpeak® interfaces. Figure 10 shows the key project Phase II steps for developing, refining, releasing, supporting, and testing the enterprise application interoperability portion of this project. As indicated in the figure, it will not be sufficient to merely develop new standards; those standards must be incorporated into commercial products, rigorously tested for

interoperability, and used in daily operations at utilities in order for the objectives of the project to be achieved. The steps shown in Figure 10 are derived from those used successfully to date in developing the MultiSpeak® standard.

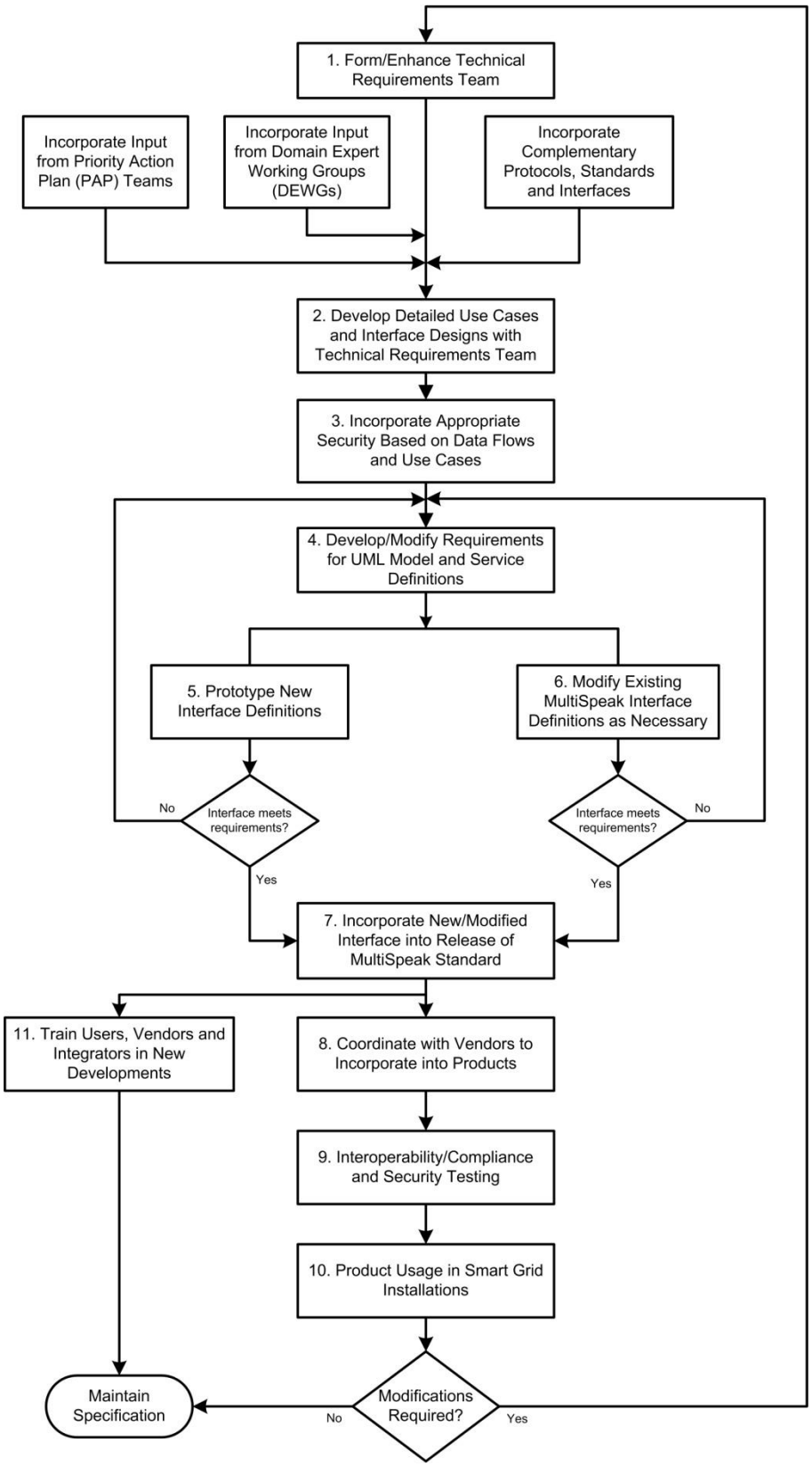


Figure 10. Software Application Interoperability Task Flowchart.

Step 1: Form and enhance the technical requirements team. Stakeholders from the vendor, utility, and standards community will be sought out to help establish the technical requirements for the required interapplication interfaces. The MultiSpeak® Initiative has an established, cohesive Technical Committee that will form the backbone of this team. It will be augmented by other technical representatives with specific expertise, depending upon the requirements of the particular interface under development. The emphasis has been, and is anticipated to continue to be, on team members that are providers of the software along with the eventual users of the software affected by the standard under development.

Step 2: Develop detailed use cases and interface design parameters. Once the technical interface requirements teams are assembled, targeted discussions will be facilitated to develop detailed use cases and interface designs that support those use cases. The requirements will include, where appropriate, the input from the NIST Priority Action Plan (PAP) teams, DEWGs, and public releases of complementary standards and protocols, such as those identified in Tables 6 and 7. The results of these deliberations will be documented in standard use case format and unified modeling language (UML) sequence diagrams.

Table 14 outlines the PAPs that likely will result in requirements that need to be addressed during development of MultiSpeak® interfaces. The PAPs are segregated into subject areas rather than being presented in numerical order.

NIST PAP #	Coverage	How Output of PAP Could Affect MultiSpeak® Interface Technical Requirements
	DR-Related PAPs	
#3	Common Pricing Model	Affects expression of price in market signals. This PAP could affect pricing model from the Markets domain through the utility to the Customer and Service Provider domains.
#4	Common Scheduling Model	Affects expression of when events occur in calendar time. This PAP could affect pricing and event signals from the Markets domain through the utility to the Customer and Service Provider domains.
#9	Standard DR and DER Signals	This PAP makes use of the outputs of PAPs #3 and #4 to communicate signal from the Market to the Customer or DER facility, including all potential domains in the end-to-end DR demonstrations.
#10	Standard Energy Usage Information	This PAP studies the communication of consumer energy usage data with third parties. This could affect the modeling and expression of metered data.

	DER-Related PAPs	
#7	Electric Storage Interconnection Guidelines	This PAP describes the modeling and interactions of DER facilities with the utility. Affects both the end-to-end DR and distribution grid management demonstrations in so far as distributed storage facilities are included.
#9	Standard DR and DER Signals	This PAP makes use of the outputs of PAPs #3 and #4 to communicate signal from the Market to the Customer or DER facility, including all potential domains in the end-to-end DR demonstrations.
	Metering-Related PAPs	
#6	Common Semantic Model for Meter Data Tables	This PAP addresses the choice and expression of data, primarily from consumer revenue meters. The output of this PAP may require modifications of the metering and measurement models in MultiSpeak®.
	Modeling PAPs	
#8	Common Information Model (CIM) for Distribution Grid Management	This PAP addresses the harmonization of MultiSpeak® with the IEC CIM standard (IEC 61970 and IEC 61968). Harmonization activities between MultiSpeak® and these IEC standards are ongoing with funding sources other than those that support this project; significant output from those harmonization efforts will be incorporated into the interface development anticipated here.
#12	IEC61850 Objects/DNP3 Modeling	This PAP addresses the harmonization of the DNP3 and IEC 61850, both master-to-remote protocols. MultiSpeak® is a master-to-master protocol, so this effort will not directly affect the project, but the results of PAP #12 might have ramifications for master-to-master communications interfaces, if they will be incorporated into the interface development anticipated here.

#14	T&D Power Systems Model Mapping	This PAP addresses the harmonization of MultiSpeak® with the IEC CIM standard (IEC 61970 and IEC 61968) for the purpose of expressing power system models. Harmonization activities between MultiSpeak® and these IEC standards are ongoing with funding sources other than those that support this project; significant output from those harmonization efforts will be incorporated into the interface development anticipated here.

Table 14. Existing NIST Priority Action Plans That May Impact Enterprise Application Interoperability.

Table 15 outlines the DEWGs whose efforts will likely result in requirements that need to be addressed during development of MultiSpeak® interfaces.

NIST DEWG	Coverage	How Output of DEWG Could Affect MultiSpeak® Interface Technical Requirements
TnD	Transmission and Distribution	This DEWG deals with distribution grid management. Its primary role is to develop use cases that should be addressed in smart grid implementations. T&D DEWG use cases will be considered for adoption in the MultiSpeak® interfaces deployed in the distribution grid management portion of the demonstration as appropriate.
H2g	Home–to-Grid	This DEWG deals with the interaction of the residential consumer with the utility. Output of this DEWG will be addressed primarily in the end-to-end DR portion of the project.
B2g	Building-to-Grid	This DEWG deals with the interaction of a commercial building EMS with the utility. Output of this DEWG will be addressed primarily in the end-to-end DR portion of the project.
I2g	Industry-to-Grid	This DEWG deals with the interaction of industrial facilities with the utility. Output of this DEWG will be addressed in both the end-to-end DR and distribution grid management portions of the project as appropriate.
PEVtg	Electric Vehicle-to-Grid	This DEWG deals with the interaction of electric vehicles with the utility. Output of this DEWG will be addressed primarily in the end-to-end DR portion of the project as appropriate.

Table 15. Existing NIST Domain Expert Working Groups That May Impact Enterprise Application Interoperability.

Step 3: Incorporate appropriate security features. As described in detail in Section 4, security will be required (1) from the interoperability standards themselves, (2) from the vendors supplying software applications, (3) from the cooperatives, and (4) from end users. Security cannot be "bolted on" to the interoperability standard, but must be incorporated during the design of new parts of the MultiSpeak® standard and as part of the refinement of existing parts of the MultiSpeak® standard. This step in the project plan will endeavor to provide the needed requirements. Security requirements will be based on the data flows anticipated for each use case.

Step 4: Develop or modify requirements for UML model and service definitions. Once the use cases have been identified and documented in Step 2 and security requirements have been identified in Step 3, then it will be possible for the Technical Requirements Team to outline the detailed changes in the UML data model and service definitions that are necessary to implement the modified use cases.

Step 5: Prototype new interface definitions.

Step 6: Modify existing MultiSpeak® interface definitions. At this stage, prototype interface designs (release candidates) for new and enhanced interfaces will be developed. Funding for upgrading existing interfaces, where they do not directly affect the project, will be provided by sources outside of the project funding. During Steps 5 and 6 interface definitions will be implemented based on the use cases and UML sequence diagrams generated during team deliberations. The data model will be developed in UML class diagrams and the resulting UML classes will be cast into XML schemas. Next, interface services will be generated as Web services, based on this data model. Web service contracts will be documented in WSDL files. Steps 5 and 6 will be executed iteratively until the needs of the Technical Requirements Team are met. Since the Technical Requirements Team includes vendors that will eventually offer products featuring MultiSpeak® interfaces, those vendors can begin initial development and testing of product interfaces at this point, even before formal incorporation of the modifications into the MultiSpeak® standard (Step 7) are complete.

Step 7: Incorporate new or modified interfaces into the MultiSpeak® standard. During this task, the team will work with the MultiSpeak® Technical Requirements Team to formalize and adopt the final interfaces. Specification documentation will be added or modified as necessary to describe the interfaces added as part of the demonstration project. It is anticipated that the MultiSpeak® Initiative will release the results of these deliberations to the industry on an annual basis. Section 3.3.2 discusses the anticipated release schedule for the MultiSpeak® Specification.

Step 8: Vendors incorporate modified specifications during product development. During this step, vendors will complete product development incorporating the updated interface definitions. As a result of the inclusion of vendors in the project Technical Requirements Team, project developments can be incorporated into products on an ongoing basis in a more streamlined manner. This procedure has been successfully used for the past decade to move MultiSpeak® standards work as efficiently as possible into the commercial market.

Step 9: Interoperability, compliance, and security testing. The MultiSpeak® Initiative provides an interoperability and compliance testing laboratory as a resource to vendors interested in investigating and certifying MultiSpeak® compatibility. As part of the project, the testing suite will

be enhanced to include a deeper level of interoperability and compliance testing as well as security certification.

Step 10: Product usage in smart grid installations. Once interface developments have been incorporated into products (Step 8) and tested (Step 9), vendors will install products featuring MultiSpeak® interfaces at utility smart grid installations. Vendors will assist those cooperatives that act as demonstration sites to install and configure the MultiSpeak® interfaces that are necessary to achieve the required level of integration. Due to the rapid application development lifecycle required for achieving the goals of the demonstration, vendors likely will need to provide several Web services endpoints to be able to support multiple versions of the MultiSpeak® interfaces.

Step 11: Training of users, integrators, and vendors in new developments. A key strength of the MultiSpeak® specification is the availability of a pool of individuals at utilities, vendors, consultancies, and system integrators who have received training in the use of the MultiSpeak® standard to provide support for end users. The MultiSpeak® Initiative offers training on the application of the specification on a periodic basis (typically three to four times each year). Funding for this activity will be provided by sources other than the demonstration grant, but its execution will provide a key role in assuring widespread understanding of the application interface development results of the project.

Note that during development, testing, installation, and early operation, the software applications interoperability team will work with the vendor and utility developers and the Technical Requirements Team to address concerns and iteratively improve the interface designs. When gaps or shortcomings are identified, those issues will be documented and tracked. Subsequently, issues will be fed back into the requirements process so that they might be addressed in an expedited manner. Again, this process has been refined during the past work on MultiSpeak®, and the project will use that experience base to proceed.

SCHEDULE

The precise schedule of events leading to adoption of the technologies standardized will depend on a number of factors outside the control of the project team. Some of these factors include:

- Release dates for complementary standards, protocols, and interfaces
- Development of interoperability testing standards and methodologies
- Speed of incorporation of new standards into commercial products by vendors
- Speed of adoption of new software applications by end users

The project team has somewhat more control over when the various interfaces will be addressed and incorporated into an upgraded MultiSpeak® standard. An April 1, 2010, meeting of the MultiSpeak® Technical Committee approved a draft schedule to meet the goals of the project. This schedule is provided in Table 16.

Version	Target Release Date	Information Cutoff Date	Major Modifications or Additions	Outside Standards and Versions	Demo Interfaces
4.1	6/30/2010	12/31/2009	**Inspection** (R1)		
			PAN Support [CP(R1), HAN (R1), MM (R1), PM(R1)]	ZigBee SEP 1.0, IEC 61968, Part 9 (1st Ed.)—Partial Support	AI 4, AI 13, AI 1, AI 3
4.2	12/31/2010	7/1/2010	**Asset Management** (R1)		
			Inspection (R2)		
			E2E Demand Response [DM (R1),LF (R1)]	ZigBee SEP 2.0, IEC 61968, Part 9 (2nd Ed), NAESB, OASIS (WS-Calendar, Pricing, Energy Information)	AI 16.1-AI 3.8 AI15.1- AI4.7 AI16.2 - AI 15.2
			AMI [DR (R2), MR(R2), MDM (R2), CB (R2)]	ZigBee SEP 2.0, IEC 61968, Part 9 (2nd Ed), NAESB, OASIS (WS-Calendar, Pricing, Energy Information)	AI 4, AI 13, AI 1, AI 3
			PAN Support [CP(R2), HAN (R2), MM (R2), PM(R2)]	ZigBee SEP 2.0, IEC 61968, Part 9 (2nd Ed), NAESB, OASIS (WS-Calendar, Pricing, Energy Information)	AI 4, AI 13, AI 1, AI 3
			DRAS (R1) (Both client and server implementations)	OpenADR	AI 4.6 - AI 14.1 AI 14.2 - AI 22.1

4.3	12/31/2011	7/1/2011	**E2E Demand Response** [EMC (R1), MS (R1)]	NAESB, OASIS (WS-Calendar, Pricing, Energy Information)	AI20.1 - AI 18.2 AI 18.1 - AI 16.3
			ICCP [EMS (R1), SCADA (2)]	TASE.2 (ICCP)	AI 19.1 - AI 17.2 AI 17.1 - AI 2.8
			E2E Demand Response [DM (R2),LF (R2)]		AI 16.1 - AI 3.8 AI15.1 - AI4.7 AI16.2 - AI 15.2
			DER [SCADA (R2), DG (R1), DS (R1)]	DNP3, IEC 61850	AI 2.9 - AI 21.1
			DMS [EA (R2), DSE (R1), OA (R2), DA(R2), SCADA(R2)]	DNP3, IEC 61850	AI 1, AI 2, AI 3, AI 5, AI 6, AI 7, AI 8
4.4	12/31/2012	7/1/2012	Refinement as required.		
4.5	12/31/2013	7/1/2013	Refinement as required.		

Table 16. Proposed Schedule for MultiSpeak® Enhancement Versioning.

Note the following about Table 16:

- In Column 4: CP, DM, DRAS, EMC, EMS, LF, MM, MS, and PM are new MultiSpeak® servers about which more detail can be found in Table 12.
- In Column 4, detail about new MultiSpeak® servers DSE and EMS can be found in Table 13.
    - In Column 4, DG and DS are jointly referred to as being DER. Detail about the new MultiSpeak® DER EMS server can be found in Table 13.

- Existing MultiSpeak® servers in column 4: CB, DA, DR, EA, HAN, MDM, MR, OA, and SCADA are shown in Figure 8.
- R1 and R2 refer to Release 1 and Release 2 of a particular new server.
- The demo interfaces described in the last column can be found described on Figure 9 and Table 9.

Version 4.1 of the MultiSpeak® specification is scheduled to be publically issued by June 30, 2010. Version 4.1 has been identified by NIST as being the target for harmonization with IEC 61968 as part of PAPs 8 and 14. Version 4.2 is expected to follow by year-end 2010. Subsequent releases will be issued annually near year's end. When a new version is issued to the MultiSpeak® Initiative members, the prior version will be released publically. The time lag between the release of new versions for vendor consideration and publically for universal consideration allows time for issues with the new release to be identified by vendors building software written to the new versions and to be fixed.

It is likely there will be a number of prerelease builds and release candidates that will be created in the process of preparing to issue a version release. Vendors participating in the demonstration project will have access to all of the intermediate builds and release candidates so that progress on the demonstration will not slow awaiting a version release.

MultiSpeak® is anticipated to issue version releases at least annually and on a predictable schedule, with a target of a new release every year during the period 2010 through 2013 in December. It is expected that the vendors will work toward support of the new release in generally available products to be displayed at key trade shows such as TechAdvantage and DistribuTECH roughly 14 months later. This should provide adequate time for vendors to develop to the new release and to perform interoperability testing with potential business partners prior to the cycle of trade shows.

In order to incorporate new information (primarily standards, protocols, and interfaces from other organizations), an imposed cutoff date for new information is set for the July preceding each calendar year release (as shown in Table 16). Input from other SDOs will be accepted until approximately July 1 of each year. If the output of another group is significant to the work of MultiSpeak® and is available as a public release prior to July 1, then typically the Technical Requirements Team will determine whether the input should be considered for adoption in the annual release. This would provide the team roughly six months to determine how to support the new public release of another SDO's work. If the output of another SDO were issued in public form after July 1, then typically it would be considered for inclusion in the following year's annual release. At any time, the Technical Requirements Team could decide to take input from another SDO after July 1 if it explicitly decided to do so.

Table 16 also contains the key major modifications or additions currently scheduled to be included in each MultiSpeak® release candidate. These also serve as the major goals for deliverables for the Phase II enterprise application interoperability project work. Again, it should be noted that the specific contents for each year's deliverables will depend on issues not in the control of the project team. However, there is reasonable expectation among those affected (vendors serving on the Technical Committee and project team members) that the milestones shown are achievable. The major modifications identified are keyed to MultiSpeak® abstract software functions.

ORGANIZATIONS AND RESPONSIBILITIES

Activities will be conducted during the project by Cornice Engineering, Inc., Science Applications International Corporation (SAIC), and Cigital, Inc., with regards to the software application interoperability. Power Systems Engineering, Inc. will be responsible, in collaboration with the utilities and vendors, for installation, configuration, and site acceptance of applications. Figure 11 shows which organization is primarily responsible for which activities. Furthermore, those activities that will complement project activities and for which Cornice Engineering has primary responsibility, but where funding is provided outside the demonstration project, are shown in a contrasting color.

Cornice has primary responsibility for:

- Forming and managing the Technical Requirements Team
- Incorporating applicable content developed independently by NIST PAPs, DEWGs, and other SDOs (note that the activity of incorporating the content developed by these groups into MultiSpeak® will be funded by the project, as shown in Figure 11; however, the work associated with coordinating with the PAP and DEWG teams will be funded outside the scope the demonstration)
- Working with the Technical Requirements Team to develop and document use cases
- Developing requirements for the new and modified interfaces based on the output of the Technical Requirements Team
- Incorporating the UML models and service definitions provided by SAIC into the MultiSpeak® Specification
- Working with vendor members of either the MultiSpeak® Technical Committee or the Technical Requirements Team to aid understanding of the MultiSpeak® specification
- Provide training on the application and use of the MultiSpeak® specification (funding provided outside of the scope of the demonstration project)

Cigital has primary responsibility for:

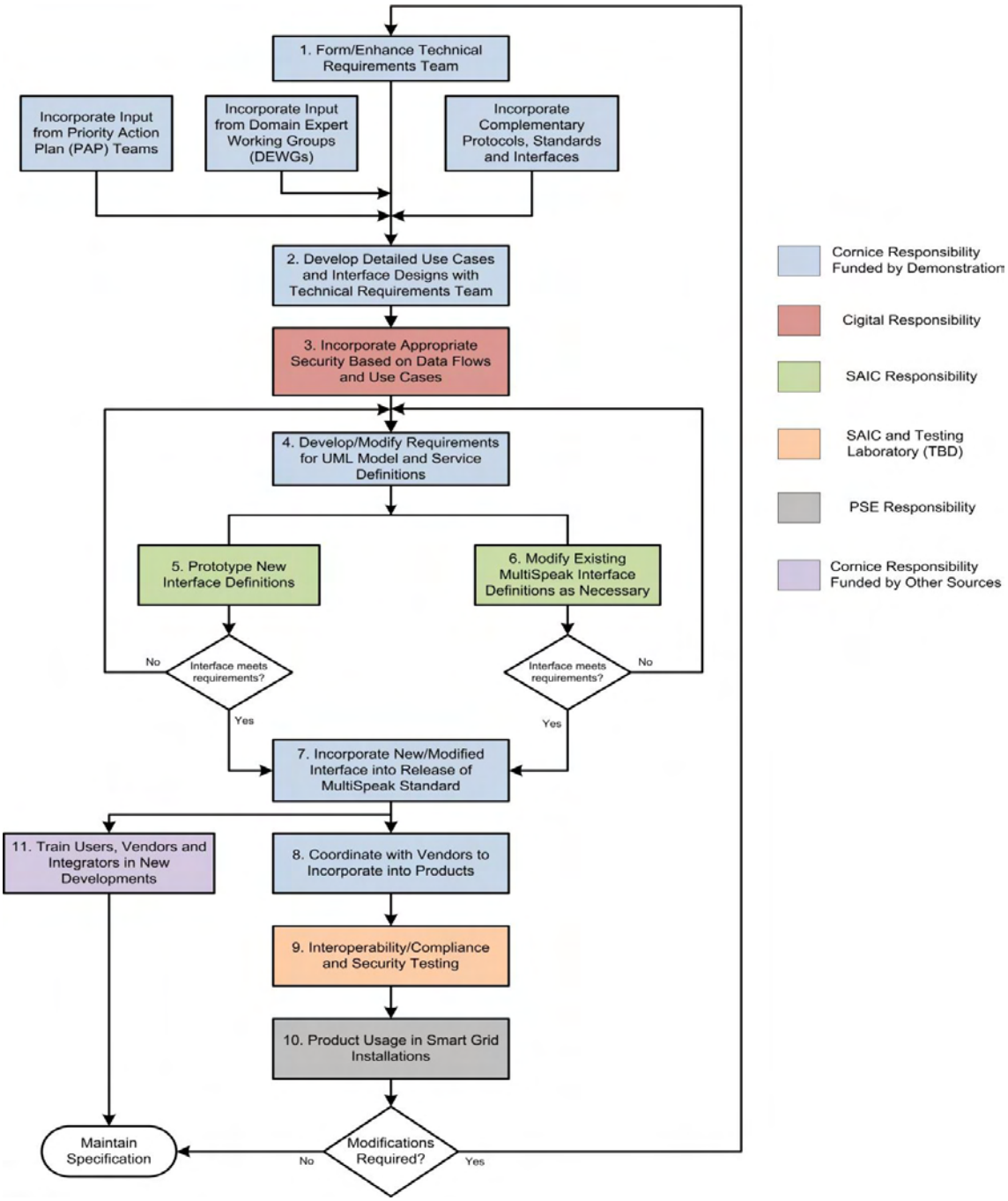
- Ensuring that interfaces developed as part of the project incorporate the required security features

SAIC has primary responsibility for:

- Developing and maintaining MultiSpeak® UML models, XML schemas, and Web service definitions
- Maintaining lists of issues raised during requirements development, early vendor testing, and utility site implementations
- Tracking how each issue is resolved

Power Systems Engineering has primary responsibility for:

- Working with vendors and utilities to coordinate installation, configuration, and site acceptance of software applications



- Providing feedback to the Software Team (Cornice and SAIC) on issues raised during installation and operation at demonstration sites

Figure 11. Delineation of Responsible Parties.

SECURITY

Early in Phase II of this demonstration project, the NRECA demonstration team will begin a series of security-related discussions regarding MultiSpeak®. In particular, we will create the specifications that help ensure that MultiSpeak® provides the security funationality and properties required to meet operational needs and to ensure the necessary confidentiality, integrity, and availability goals.

As necessary and practical, the NRECA team will define the security extensions, create reference models for vendors to follow, provide advice to involved parties, and provide guidance on security testing of vendor code. To perform this work as efficiently as possible, the NRECA team may also create functional and security test harnesses that allow vendors to verify whether their implementation is both complete and secure.

INTEROPERABILITY, COMPLIANCE, AND SECURITY TESTING

PRESENT TESTING PROCEDURES

The MultiSpeak® Initiative has provided compliance testing since 2001 and compliance and interoperability testing since 2006. At present, both compliance and interoperability testing are provided using a testing harness. The testing harness application acts as the universal client that can be used to test any software that implements MultiSpeak® server capabilities, and as the universal server that can be used to test any application that provides MultiSpeak® client capabilities.

Compliance testing for the batch message transport consists of two parts: (1) validation of the received batch message issued by the software under test using the MultiSpeak® XML schema and (2) verification that the software under test can accept a valid MultiSpeak®-formatted batch message and display that it has handled the data appropriately.

Compliance testing for Web service transports consists of showing that the software under test exchanges Web services method calls in a MultiSpeak®-compatible manner using a set of standard test data, when communicating with the test harness. The testing harness verifies each Web service data payload to ensure that it validates using the MultiSpeak® XML schema.

Interoperability testing is performed between two vendor applications. The vendors prepare an assertions document that describes the utility business process that the MultiSpeak® integration supports and how that integration is accomplished using MultiSpeak® Web services method calls. The vendor-prepared assertions are then tested. During the test, the testing harness is used in a "man in the middle" mode. That is to say, Vendor A's application sends a Web service call to the testing harness, which validates the data payload and then sends the repackaged Web service call to Vendor B. When Vendor B responds to the original Web service, that response is sent to the testing harness, validated, and passed on to Vendor A's application. This process is followed for each Web service method that is being tested. The testing agent can at any time ask to be shown that the software under test has accepted the data being sent and has taken the appropriate action based on those data.

PROPOSED TESTING PROCEDURES

It is proposed that the present interoperability and compliance testing regime be enhanced as part of the demonstration process, if practical and appropriate to do so. Applications that implement Version 4.x MultiSpeak® interfaces and that are to be installed as part of the demonstration will undergo enhanced interoperability testing, but should also be tested for security. The following improvements are recommended:

- Perform testing with both valid data and invalid data to make sure that applications deal appropriately with improperly formatted data.
- Perform testing with data sets that intentionally attempt to exploit potential security weaknesses in the software under test.
- Perform testing using data sets that are intentionally designed to be excessive in size so that the software under test can be checked for potential overflow attacks and to ensure that software handles the data appropriately or fails "gracefully."

LEGACY SOFTWARE AND BACKWARD COMPATIBILITY

Most of the capabilities that will be developed during the project period (for example, support for premises area networking, OpenADR, or DER) do not currently exist in utility software installations, so that issues of legacy software and backward compatibility are not as prominent when considering interoperability of software applications as they are for hardware devices.

Traditionally, the MultiSpeak® Technical Committee has chosen to constrain its development of successive builds of MultiSpeak® within Version 3.0 to be backward compatible within that version. Thus, when it was necessary to add data model elements that violated the requirement to maintain backward compatibility, it became necessary to move to a new major release. It became necessary to move to Version 4.0 when the standard added: (1) international addresses, (2) international telephone numbers, (3) support for a wide variety of units of measure (including both English and metric units), (4) features to support future harmonization with the International Electrotechnical Commission Common Information Model (IEC CIM) standards, and (5) XML schema development based on a UML model.

The MultiSpeak® Technical Committee, at its meeting on April 1, 2010, discussed the scope of development that will be required to support the demonstration project as well as to incorporate the work of outside SDOs. Table 16, which outlines the schedule for the next several years' development effort, resulted from those deliberations. However, due to the extensive nature of the anticipated changes, and the speed at which the changes need to be rolled out, the Technical Committee decided to relax its prior constraint that all subsequent pre-release builds and releases be backward compatible. To mitigate this action, the Technical Committee decided to accelerate the number of internal draft builds while reducing the number of final releases scheduled. At the same time, it was decided to make access freely available to final releases on an accelerated schedule. Thus, it would be possible to accelerate internal development while providing a stable release schedule for those attempting to adopt the MultiSpeak® Specification.

In summary, the Technical Committee decided that:

- Major versions (VX, where X = 4.2, 4.3, 4.4, 4.5. . .) will not be constrained to be backward compatible, by design, with previous major releases.

- Releases will be made on a predictable, annual basis.
- Once a new version is released for internal development, the prior release will be made freely available for public download from the MultiSpeak® Web site.
- Where backward compatibility is possible and desirable, vendor software will provide that functionality by deploying multiple Web services end points, each implementing the namespace of the versions of the MultiSpeak® Web services that are to be supported.

The provision of multiple Web services endpoints permits vendor software to communicate appropriately, using multiple prior releases of MultiSpeak®, while also supporting the current version of the services. This approach ensures that a vendor application does not attempt to call on functionality that cannot exist in another application that only supports an older release of MultiSpeak®.

CYBER SECURITY PLAN CONSIDERATIONS

A system security plan documents the systematic and comprehensive approach that will be taken to ensure a fielded system includes all of its required security functions and properties throughout its entire lifecycle. The functional security aspects are usually derived from various sources, such as statutory and regulatory guidance, market forces, consumer demands, and available time and financial resources. Required nonfunctional security aspects are usually derived from the various threats, attacks, and risks associated with the actual system being constructed and the environment in which it will be deployed.

Several current and evolving documents establish cyber security requirements for cooperatives and the systems they deploy, including cyber security requirements specific to adopting smart grid technologies. Most of these references include a discussion of the threat and attack environment applicable to smart grid technologies and provide high-level people, process, and technology requirements for ensuring an appropriate security posture. They do not call out specific technologies, vendors, or versions and typically leave the implementation method up to the organization. These references include the following:

- 128 Federal Energy Regulatory Commission (FERC) 61,060,[13] Smart Grid Policy, July 16, 2009—provides guidance regarding the development of a smart grid
- NERC CIPs[14]—The NERC CIP standards are mandated for all entities responsible for the availability and reliability of the bulk electric system
- NISTIR 7628 (Draft, February 2010)[15]—Smart grid cyber security strategy and requirements
- NIST SP800-53[16]—Recommended security controls for federal information systems and organizations
- NIST SP800-82[17]—Draft guide to industrial control system security
- AMI-SEC System Security Requirements v1.01[18]—Security requirements for the AMI
- Institute of Electrical and Electronics Engineers (IEEE) 1686-2007[19]—Security standard for substation intelligent electronic devices cyber security capabilities

[13] Found at http://www.nerc.com/files/Smart_Grid_7-16-09_Policy_Statement.pdf.

[14] Found at http://www.nerc.com/page.php?cid=2|20.

[15] Found at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/NISTIR7628Feb2010/draft-nistir-7628_2nd-public-draft.pdf.

[16] Found at http://csrc.nist.gov/publications/PubsSPs.html.

[17] Found at http://csrc.nist.gov/publications/PubsSPs.html.

[18] Found at http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/1.%20System%20Security%20Requirements/AMI%20System%20Security%20Requirements%20-%20v1_01%20-%20Final.doc.

To ensure adequate topical coverage in our cyber security plan, we also examined several resources that provided security plan templates.[20]

Smart grid technologies introduce significant new risks into electrical cooperative environments. A rapid influx of IT networking, Internet-accessible systems, large data stores, private data and associated legal issues, complex applications and hardware that require careful configuration, vendor management needs, and a host of other items will significantly change existing risk profiles. That these changes are also occurring very rapidly only exacerbates the problem. A corresponding increase in the maturity of a cooperative's network, data, and software security practices will be required. Similarly, changes will be required in smart grid technologies and this will in turn require changes in vendor hardware, software, development methods, and testing. Comprehensive and forward-looking application of a robust set of security considerations is key to early and ongoing success.

APPLYING CYBER SECURITY ACTIVITIES

The sections below discuss a range of core cyber security activities that are applicable to the deployment of secure smart grid technologies. As part of the NRECA demonstration, we will iteratively apply these activities in three distinct contexts:

- **Demonstrations.** The NRECA team will apply these cyber security activities continuously as we develop, integrate, and deploy the 10 activity types that are part of the NRECA demonstration proposal. We will help ensure that security is not a barrier to meeting the DOE's accelerated timetables for standards development and interoperability. Application of these cyber security activities is the foundational part of ensuring that cyber security breaches cannot cause broad-based systemic or cascade failures.
- **Vendors.** The NRECA team will use these cyber security activities to educate vendors and provide advice for integrating into their product requirements and engineering methodologies the concepts and practices that accomplish at least four objectives:
  - Delivering a product (device, protocol, and so on) that meets then-current interoperability and functional security requirements (be they statutory, regulatory, contractual, or otherwise derived)
  - Delivering a product that includes appropriate nonfunctional security properties (that is, is secure with respect to known threats and attacks using feasible risk mitigation approaches)
  - Delivering a product that allows participants (electrical cooperatives) to achieve their statutory, regulatory, and contractual goals under normal circumstances[21]

[19] Found at http://smartgrid.ieee.org/standards/approved-ieee-smartgrid-standards.

[20] These include NIST SP800-18, *Guide for Developing Security Plans for Federal Information Systems*, and the U.S. Nuclear Regulatory Commission (NRC) Regulatory Guide (RG) 5.71, *Cyber Security Programs for Nuclear Facilities*.

  - Establishing a product engineering life cycle that includes the security activities and gates that are capable of producing the product envisioned in the preceding three objectives

- **Electrical cooperatives.** The NRECA team will use these cyber security activities to advise demonstration participants—the electrical cooperatives—in several areas:
  - The governance and compliance impacts that come with fielding smart grid technologies, specifically in the area of cyber security
  - The security concerns and service-level agreements that cooperatives will likely want to discuss with smart grid vendors, be they providers of hardware, software, or services
  - The efficient and effective address of the operational changes associated with fielding smart grid technology
  - Important steps to take in each phase of smart grid technology deployment, including procurement, installation and commissioning, operations, ongoing maintenance and support, and decommissioning and removal

From a security perspective, the ongoing engineering conducted by the NRECA team, by vendors, and by smart grid demonstration participants comprises the following three high-level elements:

- Security assessment (threat modeling and controls selection)
- Security controls design/implementation
- Security assessment (security test and evaluation)

We will also consider the following security principles as security mechanisms are specified, built, or recommended:

- Holistic (addresses multiple physical, network, software, process, people areas)
- Compartmentalization (plan for failure)
- Defense in depth (security must be multilayered)
- Secure the weakest link
- Protect, detect, respond (controls must be multifaceted)

The ongoing and iterative cyber security interaction conducted as part of the demonstration with vendors and participants will be facilitated by activities such as:

- Documentation and design review
- Interviews
- Observation and inspection

[21] That is, the vendors will not deliver a product that makes it effectively impossible for cooperatives to achieve compliance with their specific mandates.

- Configuration and code analysis
- Vulnerability scanning
- Penetration testing

The results of these activities will inform our understanding of real risks. Armed with that knowledge, we can confidently recommend risk-based and compliance-based controls that help all participants efficiently and economically achieve their respective goals.

Sections 4.2 through 4.12 contain additional detail on the core cyber security activities we will apply during the course of this demonstration, including references to relevant guidance. Each topic includes a brief description of how it will be applied. Note that the references to relevant guidance are subject to change. The state of regulation, directives, and guidance is in flux at this time and will remain so for the foreseeable future. As the time arrives for performing a particular piece of interoperability or cyber security work, the NRECA demonstration team will use the best available guidance at that time. It is also important to understand that there will likely be many instances when only a few of the security ideas below apply to the activity at hand, safely allowing for an abbreviated process.

RISK MANAGEMENT PROGRAM

A risk management program ensures system operations are occurring under acceptable conditions. It encompasses risk assessment, risk mitigation, and ongoing evaluation and assessment. In this particular case, we are concerned with cyber security risks throughout the life cycle of smart grid component software.

SYSTEM DEFINITION

An early step in creating security plans and establishing risk management programs is strictly defining the system in question. This ICS plan applies to the systems defined in the NRECA proposal and in Sections 2 and 3, above. Anything beyond the physical and logical boundaries of the described demonstration systems is out of scope for this document, although such topics may be discussed in order to provide context.

There is one overall demonstration architecture (based on the NIST reference architecture) for the demonstration project. This project comprises 4 subprojects that in turn comprise 10 activity types that in turn comprise approximately 100 activities. For each of the 100 activities, we will document the following:

- Unique identifier for that installation
- Primary function or purpose of that installation
- Architecture diagrams (physical, logical, and security) and data flow diagrams
- Installation inventory
- Details for interfaces and protocols
- Data types processed and the sensitivity of each
- Version or stock keeping unit (SKU) numbers for all physical and logical components and the criticality of each component

- Vendors and contact information
- Installation location and local cooperative contact information
- Assignment of local security responsibilities
- Any special interoperability or security concerns (for example, modems, Web interfaces, remote administrative access, and so on)
- Emergency contact information and procedures for everyone involved

For each activity type, we will also briefly document the associated major management, technical, operational, and physical security controls.

We will also follow the guidance in section 3.1, System Characterization, of NIST SP800-30, Risk Management Guide for Information Technology Systems.[22]

UNDERSTANDING THE REGULATORY ENVIRONMENT

The Energy Independence and Security Act (EISA) of 2007 defined the characteristics of a smart grid. It directed the FERC to provide, through rulemaking, a set of standards and protocols necessary to ensure smart grid functionality and interoperability. It directed the NIST to coordinate the development of a framework to achieve interoperability of smart grid devices and systems. In carrying out its mandate, the FERC examined, among other topics, the development of standards that address cyber security, communication, and coordination across interfaces.

In its Final Policy Statement of July 2009, the FERC directed the NIST to begin taking steps to ensure that the NIST's interoperability framework is consistent with the FERC and EISA requirements. Further, the FERC expects the NERC to monitor the evolving environment to ensure ongoing compatibility of the various guidance and standards with the approved CIP standards.

NIST continues its efforts in creating and harmonizing ICS guidelines. This document will keep pace with those changes, as appropriate.

APPLICABLE CYBER SECURITY STANDARDS

Several current and evolving documents establish cyber security requirements for cooperatives, including cyber security requirements specific to adopting smart grid technologies. Most of these references already include a discussion of the threat and attack environment applicable to new smart grid technologies. These references include the following:

- NERC CIPs[23]—The NERC CIPs are mandated for all entities responsible for the availability and reliability of the bulk electric system
- NIST IR 7628 (Draft, February 2010)[24]—Smart grid cyber security strategy and requirements

[22] See NIST SP 800-30, Risk Management Guide for Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)

[23] Found at http://www.nerc.com/page.php?cid=2|20.

- NIST SP800-53[25]—Recommended security controls for federal information systems and organizations
- NIST SP800-82[26]—Draft guide to industrial control system security
- AMI-SEC System Security Requirements v1.01[27]—security requirements for the AMI
- IEEE 1686-2007[28]—Security standard for substation intelligent electronic devices cyber security capabilities

Related documentation includes:

- Security Considerations in Implementing MultiSpeak®-Compliance Applications[29]

RISK ASSESSMENT METHODOLOGY

Risk assessment is the key process in risk management. It helps determine the applicable threats, attacks, system weaknesses, and the resulting risk of not meeting system and operational objectives. Risk is simply a representation of likelihood, a probability of whether a given future adverse event—successful exploitation of a weakness causing an undesirable outcome—will actually occur. Understanding the impact associated with that event allows us to make informed decisions on whether to invest in some combination of reducing the chances of its occurrence, in detecting its occurrence, in improving our ability to recover from its occurrence, and in transferring the risk to another entity (for example, buying insurance).

The risk assessment process comprises nine essential steps:

- System characterization—see Section 4.2.1. above
- Threat identification—create a short list of the entities likely to attack the systems and enumerate some attacks with which to be concerned; a realistic assessment of threats is a critical component of any risk assessment
- Vulnerability identification—a discussion of perceived or known weaknesses in the management, technical, operational, physical, or other control structures associated with the system; these weaknesses will be derived from previous assessments and audit reports, vulnerability lists, security advisories, vendor reports, testing and other analysis, and related activities

---

[24] Found at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/NISTIR7628Feb2010/draft-nistir-7628_2nd-public-draft.pdf.

[25] Found at http://csrc.nist.gov/publications/PubsSPs.html.

[26] Found at http://csrc.nist.gov/publications/PubsSPs.html.

[27] Found at http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/1.%20System%20Security%20Requirements/AMI%20System%20Security%20Requirements%20-%20v1_01%20-%20Final.doc.

[28] Found at http://smartgrid.ieee.org/standards/approved-ieee-smartgrid-standards.

[29] Found at http://www.multispeak.org/documents/MultiSpeak_Secure_Implementation_020805.pdf.

- Control analysis—enumeration of the controls implemented in the system and analysis of their ability to reduce the likelihood of a threat exploiting a vulnerability
- Likelihood determination—assigning a likelihood that given threats might exploit known vulnerabilities despite the controls in place
- Impact analysis—an analysis of the adverse impact of such exploits, given in business terms; important inputs to this analysis are system goals, system and data criticality, and system and data sensitivity
- Risk determination—an assignment of an overall risk level (for example, very high, high, medium, low, very low) with respect to the system meeting its business goals; see section 4.2.5 below
- Control recommendations—enumeration of additional controls considered necessary and a description of their risk reduction capability; see section on risks below

This methodology will remain a streamlined version of sections 3.2 through 3.7 of NIST SP800-30, Risk Management Guide for Information Technology Systems. We may also use Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems,[30] for low/medium/high ratings definitions, as well as relevant sections of NIST SP800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.[31]

RISKS AND MITIGATION

Our overall strategy is to examine known requirements, the components available from vendors, and participant environments to assess risks associated with fielding available equipment and protocols. While we will strive for risk prevention where practical, our strategy will certainly include a large of amount of risk management in balancing downside versus functional benefit. One benefit of such an approach is ensuring acceptable long-term impact on the participating cooperatives and the smart grid as a whole.

We will apply the methodology described above in both a bottom-up and a top-down analysis. The bottom-up analysis will focus on well-understood security problems and examine how they are addressed. Such problems include authenticating and authorizing users, authenticating devices and control data, protecting private data, protecting cryptographic material, and so on. The top-down analysis will start with threats and attacks, examine relevant requirements and attack surfaces, determine risks that must be mitigated, and provide recommended controls. Recommended controls may span a broad range of people, processes, and technology.

[30] NIST FIPS Publication 199, Standards for Security Categorization of Federal Information Processing Systems (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf).

[31] NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories (http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf).

We will apply risk mitigation strategies at each stage in the life cycles of the components and protocols core to the NRECA demonstrations. Each chosen strategy will be guided by answers to questions such as:

- Is the risk associated with this vulnerability acceptable to the business?
- Is the cost of fully remediating the risk reasonable?
- Who is responsible for remediating this risk?
- Are there any available compensating controls?
- Is the risk a compliance issue, a privacy issue, a technical issue, or some other issue?
- Does the mitigation deal primarily with people, process, or technology?

Throughout this demonstration project, we will maintain knowledge of threats, attacks, risks, and mitigations so that future activities can be secured as efficiently as possible. The knowledge will be tied directly to expected system lifecycle stages, including initiation, development or acquisition, implementation, operations and maintenance, and disposal. We will take additional guidance from NIST SP800-30, Risk Management Guide for Information Technology Systems, sections 8 and 9, as well as NIST SP800-27, Engineering Principles for IT Security.[32] We will leverage NIST SP800-53, Recommended Security Controls for Federal Information Systems and Organizations, the Department of Homeland Security (DHS) Catalog of Control Systems Security Recommendations, and similar guides when reasoning about mitigation controls for unacceptable risks.

CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

Confidentiality, integrity, and availability are common security objectives for any data processing system. To determine the impact of potential confidentiality, integrity, or availability issues, we will use the impact level definitions in NIST SP1108, Table 3.2.

It is important to note that availability—keeping electricity flowing to consumers—has been a primary power grid requirement for many decades as it directly supports overall reliability goals. Our analysis will reflect the growing importance of data and system integrity, data confidentiality, and data privacy as new applications, new devices, new protocols, and new technologies fundamentally change existing threat, attack, and risk models. In other words, we fully expect confidentiality and integrity to rise in importance based on changes in technology and the explosion of personal data maintained.

This fundamental change will also affect our choice of mitigation strategies. As noted earlier, the community has decades of experience in enhancing reliability in current electrical grid technology. Achieving such reliability in computer systems and software applications will require different approaches, and have different costs, compared with those employed by analog equipment and physical plants. As a simple example, achieving the ultra-high reliability of software applications may be prohibitively expensive for small cooperatives.

[32] NIST SP800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security) (http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf).

Confidentiality and integrity solutions for standard IT systems and networks are widely available and widely adopted in other industries. However, our analysis will have to assume that many demonstration participants are too small to afford enterprise-strength solutions. Controls recommendations must be scaled accordingly. However, recommendations will leverage cost-effective commodity tools and technology whenever possible.

LOGGING, MONITORING, AND NOTIFICATION

Logging, monitoring, and notification must occur in multiple contexts. We will ensure that each is present and sufficiently mitigates the relevant unacceptable risks.

Logging is the capture of data about system operations that later allows analysis in support of system management and event investigation. We will identify all such operations in each of the technologies core to the NRECA demonstrations and determine whether such activity is logged. These technologies include hardware components, software applications, and protocols. The exact criteria for determining what must be logged has yet to be determined, but it will certainly include the standard list of authentication, authorization, and related security functions.

Some operations will be deemed more important based on their impact on the overall system or their potential for misuse. For these operations, the ability to perform monitoring and notification will be expected. The acceptable methods for each will vary based on the context, and the standard risk management approach will be applied in determining sufficiency of existing functionality or recommending compensating controls.

VENDOR AND PARTNER MANAGEMENT

IT and software security does not begin and end at the boundary firewall. A cooperative's security posture will be directly impacted by its decisions regarding security controls, personnel education, governance and policy, and myriad other business concerns.

Similarly, decisions made by a cooperative's vendors and partners—their supply chain—can directly affect the cooperative's security posture. Bad decisions on their part with respect to security controls, secure software development, configurations, and related items can easily result in security failures for the cooperative and downstream effects for consumers.

Where appropriate and possible, the cyber security supply chain for core NRECA demonstration technologies will be included in the overall risk assessment. This supply chain will be assumed to include the entire set of key actors that produce the technology in question. For example, while the vendor for a given hardware device may be a local U.S. firm, the device may be programmed, manufactured, and assembled in multiple countries. Further, another firm in yet another country may provide customer service. All of these facts represent increased risk, and the nature of this risk will be assessed where feasible.

In many cases, these risks cannot be affected directly (for example, telling a vendor to stop getting components from a particular supplier). Instead, they must be managed by the cooperative through a variety of governance and technical controls. Examples of governance controls include service-level agreements and security-relevant acceptance criteria. Examples of technical controls include security testing in on-boarding processes.

The NRECA team will leverage supply chain security work previously done for the financial services community. Additional details can be found at http://www.fsisac.com/fsscc/.

DEMONSTRATING EFFECTIVENESS OF CONTROLS

Analysis can often show the absence or presence of controls in a very cost-efficient manner. However, testing is usually required to demonstrate the effectiveness of each control in mitigating a particular risk. The NRECA team approach will encompass several types of testing where each is appropriate and feasible.

It is important to understand that several types of testing may be required, each appropriate to a particular scenario. Here are some examples:

- Examination of contracts, service-level agreements, and other business-level instruments will require advice from legal counsel
- Testing of personnel awareness and capability will require tailored skills reviews
- Testing of security features and software logic will require manual penetration testing activities and tools
- Testing of software security will require static analysis tools
- Testing of Web applications will require dynamic testing tools
- Testing of protocols will require interoperability harnesses and fuzzing tools
- Testing of hosts and networks will require network penetration testing tools

All testing and tool use must be performed by skilled individuals. Efforts to control expense and time required for testing will be weighed against associated risks.

Testing documentation will take several forms, as appropriate to the situation:

- Test plans will be generated at various levels of detail, ranging from simple plans for basic testing to detailed plans for complex interoperability and security testing
- Engineering artifacts will be gathered when available and will be used to support analysis
- Reports from testing done by the NRECA team will be provided to the appropriate parties
- Reports created by independent or other external testing organizations will be leveraged whenever possible as a means of decreasing time and cost on other testing activities

CRITICAL CYBER ASSET IDENTIFICATION

The identification of critical cyber assets is a mandatory step in managing security risk. A risk-based methodology for identifying assets will ensure both completeness and sufficient accuracy. Briefly, the process entails:

- Identifying critical assets—this can be further refined as follows:
  - Identifying the asset types to be evaluated (for example, facilities, systems, equipment, applications, and so on) based on performance of a function that is essential to maintaining reliable operation of the bulk electric system. For a system, for example, this would be an asset type that supports wide-area reliability through capabilities such as situational awareness, automatic load shedding, and supervisory and control functions.

  - Enumerating the assets within each type; these will typically be facilities themselves or special systems
  - Listing the critical functions of each asset
  - Creating final list
- Identifying cyber assets associated with a critical asset
- Grouping cyber assets by application
- Identifying cyber assets supporting essential functions of critical assets
- Identifying cyber assets that use a routable protocol to communicate outside the Electronic Security Perimeter, or use a routable protocol within a control center, or are dial-up accessible (as required by NERC CIP-002-3).
- Compiling the list of critical cyber assets

We will also leverage NERC Security Guideline for the Electricity Sector: Identifying Critical Assets, as well as NERC Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets.

SECURITY MANAGEMENT CONTROLS

All utilities must have security management controls in place to protect critical cyber security assets. These include informed senior management, security policy, an exception management process, an information protection and access control program, and change management and configuration control procedures.

In addition to the security management guidance in NIST SP800-53, we will leverage the guidance in the International Organization for Standardization (ISO) 27000 series[33] of information security and management international standards.

LEADERSHIP

It is the executive management's job to establish risk management fundamentals within their organization. This includes a business framework for setting security objectives and aligning strategic risk management with business needs as well as external statutory and regulatory compliance drivers. Responsible senior managers will be identified by name and will be required to approve security exceptions. Overall, business leaders will ensure security management controls are established, implemented, operated, monitored, reviewed, maintained, and improved with a goal of addressing risk that may prevent meeting defined objectives.

We will leverage direction from ISO 27001, Information security management systems—Requirements, as appropriate in evaluating the leadership aspects of security management.

CYBER SECURITY POLICY

[33] See the IT Security Techniques standards at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306.

Policy represents management's commitment to securing critical assets. It must be available to all personnel who are required to comply with its requirements and must be reviewed periodically. At a minimum, cyber security policy must address the following:

- Purpose
- Scope and applicability
- Roles and responsibilities
- Topics addressed
- Compliance and exceptions
- Training and awareness
- Points of contact

We will leverage guidance from ISO 27001, Information security management systems—Requirements, and NIST SP800-12, An Introduction to Computer Security,[34] Chapter 5, when assessing security policies.

EXCEPTIONS

Policy exceptions occur for a variety of reasons. Simple examples include an overriding business need, a delay in vendor deliverables, new regulatory or statutory requirements, and temporary configuration issues. The exception process must ensure these circumstances are addressed in a manner that makes all stakeholders aware of the event, the risks, and the timeline for eliminating the exception.

INFORMATION PROTECTION

Protection of information associated with critical cyber assets is a foundational security practice. Proper information protection of such information must be defined in the context of organizational security policy and include provisions for identifying, classifying, and protecting such information. Critical cyber asset information to be protected, at a minimum and regardless of media type, includes:

- Operational procedures
- Network topology or similar diagrams
- Floor plans of computing centers that contain critical cyber assets
- Equipment layouts of critical cyber assets
- Disaster recovery plans
- Incident response plans

[34] NIST SP800-12, An Introduction to Computer Security: The NIST Handbook (http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf)

- Security configuration information
- Authentication and authorization information
- Private data

DATA PRIVACY

To ensure we have comprehensively identified all data meeting the threshold for requiring privacy protections, we will apply a test such as the one used in concert with the European Union Data Protection Act.[35] This test can be applied to data that is stored, processed, or transmitted. In brief, this test consists of enumerating characteristics about the data to facilitate its categorization. Example questions include:

- Can living persons be individually identified with the data?
- Do the data provide information that is known to be sensitive, such as social security numbers, credit card numbers, driver's license numbers, and so on?
- Does loss of the data have the potential to affect an individual?

To ensure we have comprehensively addressed the handling of data privacy, we will build a checklist and apply it to each type of data in the demonstration. The answers will guide decisions in architecture, access controls, procedures, assignment of criticality labels, and related items. Mitigation strategies for the associated risks will be guided by answers to questions such as:

- Do I really need this information about an individual or group of individuals? Do I know what I'm going to use it for?
- Do the people whose information I hold know that I have it, and are they likely to understand what it will be used for?
- Am I satisfied that the information is being held securely, whether it's on paper or on a computer? And what about my Web site? Is it secure?
- Am I sure the personal information is accurate and up to date?
- Do I, should I, and/or must I delete/destroy personal information as soon as I have no more need for it?
- Is access to personal information limited only to those with a strict need to know?
- If I want to put staff details on our Web site, have I consulted with them about this?
- If I use closed-circuit television (CCTV) or other personal surveillance, is it covered by the by any law I must follow? If so, am I displaying notices telling people why I have such surveillance? Are the cameras or other devices in the right place, or do they intrude on anyone's privacy?

[35] See http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/160408_v1.0_determining_what_is_personal_data_-_quick_reference_guide.pdf.

- If I want to monitor staff, for example by checking their use of email, have I told them about this and explained why?
- Have I trained my staff in their duties and responsibilities under applicable privacy laws, and are they putting them into practice?
- If I'm asked to pass on personal information to any other group or agency, am I and my staff clear when the law allows me to do so?
- Would I know what to do if one of my employees or individual consumers asks for a copy of information I hold about them?
- Do I have a policy for dealing with data protection issues?
- Do I need to notify any agency or group about the monitoring I am performing? If I have already notified, is my notification up to date, or does it need removing or amending?
- Whom do I notify if there is, or if I suspect there is, a security breach associated with any such data?

We will also leverage the ideas in NIST SP800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.[36]

ACCESS CONTROL

It is important to understand who within an organization grants access to resources. The organization must document, by name, those who are responsible for authorizing logical or physical access to protected resources. This list must be reviewed and updated at least annually.

CHANGE CONTROL AND CONFIGURATION MANAGEMENT

Managing change is essential to a robust ongoing security posture. Executive managers must establish and promulgate a change management process that is consistent with policy and compliance requirements. At a minimum, this process must address adding, modifying, replacing, or removing any critical cyber asset hardware, software, or related critical documentation. The change management process must also address vendor-related changes to any critical cyber assets.

PERSONNEL AND TRAINING

While it is a commonplace saying, it is nonetheless true: security is everyone's responsibility. However, organizations cannot levy this responsibility (for example, through policy) without providing sufficient training and ensuring diligence in the hiring and personnel review process.

We will leverage the guidance in NIST SP800-50, Building an IT Security Awareness and Training Program, and NIST SP800-16 Rev. 1, Information Security Training Requirements[37] in this area.

[36] NIST SP800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf).

AWARENESS AND TRAINING

Ongoing training is a key to high performance. The organization should first establish, document, implement, and maintain a security awareness program. At a minimum, this awareness program must include all personnel having authorized cyber access or authorized unescorted physical access to critical cyber assets. Awareness reinforcement should occur at least quarterly.

The organization should then establish a training program for those having authorized cyber access or authorized unescorted physical access to critical cyber assets. This training program must include at least the following:

- The policies, access controls, and procedures developed for critical cyber assets
- The proper use of critical cyber assets
- The proper handling of critical cyber asset information
- Action plans and procedures to recover or reestablish critical cyber assets, and the required access to these assets, following a cyber security incident

PERSONNEL RISK AND ACCESS

The participating organization must have a documented personnel risk assessment program that complies with applicable laws and is subject to existing collective bargaining agreements. Personnel subject to this program are those having authorized cyber access or authorized unescorted physical access to critical cyber assets. The personnel risk assessment will include, at a minimum, identity verification and seven-year criminal check. This information must be updated at least once every seven years (or for cause). The organization must also ensure that vendor personnel with similar access are also subject to such checks.

The organization will maintain a list of all personnel authorized cyber access or authorized unescorted physical access to critical cyber assets. This list will include each person's specific electronic and physical access rights to such assets. The list will be reviewed quarterly and updated within seven days of any change in a list member's access rights. Access will be terminated within 24 hours for personnel terminated for cause and within 7 days for personnel who no longer require such access.

ELECTRONIC SECURITY PERIMETER

The improper selection of security controls for a system will undermine its operations, its security, and, consequently, its acceptance in the market place. In the case of smart grid systems, poor controls can tarnish the image of this national goal and directly result in loss of life.

As we approach the analysis and selection of security controls, we will ensure we know the answers to several questions, including:

- What security controls are needed to adequately mitigate known risks?

---

[37] NIST SP800-16, Information Security Training Requirements: A Role- and Performance-Based Model (http://csrc.nist.gov/publications/drafts/800-16-rev1/Draft-SP800-16-Rev1.pdf)

- Have these security controls been implemented in a reasonable and testable fashion?
- What is the desired level of assurance that the security controls are effective?
- How can testing be cost-effectively performed to ensure the desired level of assurance has been met?

The answers to these questions are contextual to given implementations. They will also change over time as threat and attack models change and as hardware and software evolves. We will take primary guidance from NIST SP800-53, Recommended Security Controls for Federal Information Systems and Organizations. We will also leverage content from NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.

PERIMETER

As a matter of security design, assets should reside behind logical security protections. Each collection of logical security protections can be referred to as a electronic security perimeter, and the organization must ensure that every critical cyber asset resides inside one or more such perimeters. At a minimum, the organization must document the assets requiring an electronic security perimeter and the access points to the perimeters. It is important to note that any noncritical cyber asset inside a defined electronic security perimeter must be identified and afforded the same protections as critical cyber assets.

In many cases, we also want assets to include security protection mechanisms, not just reside within a defined perimeter. For certain wireless assets, we will also use the guidance in NIST SP800-97, Guide to IEEE 802.11i.[38]

ACCESS CONTROLS

As part of risk management, the organization must document and implement the processes and the technical and procedural mechanisms for control of electronic access at all electronic access points to the electronic security perimeters.

The mechanisms must use an access control model whose default setting is to deny access, thereby requiring explicit permission changes in order to enable access. Similarly, all access points to the electronic security perimeter should have enabled only the ports and services required for approved operations and monitoring. Remote interactive access to a point within the perimeter typically would be accompanied by strong procedural or technical controls to enforce authentication.

MONITORING

There must be documented and implemented electronic or manual processes for monitoring and logging usage of electronic perimeter access points. These processes must be operational at all times. Where technically feasible, these processes must detect unauthorized access attempts and

[38] NIST SP800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i (http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf).

alert specified personnel. If there is no ability to perform alerting, the organization must review the access logs at least every 90 days.

VULNERABILITY ASSESSMENT

Organizations must perform a cyber vulnerability assessment of the electronic access points to the electronic security perimeter. This assessment must be performed at least annually. It must include at least the following:

- A description of the vulnerability assessment process
- A review ports and services configurations
- A discovery of all access points to the electronic security perimeter
- Documented findings, a remediation plan, and the plan's execution status

As appropriate, we will leverage the process outlined in NIST SP800-30, Risk Management Guide for IT Systems, for these assessment activities.

DOCUMENTATION

The organization must ensure all documents produced as part of electronic security perimeter documentation, assessment, and remediation are kept up to date with current physical and logical configurations. The documents typically will be updated within 90 days of physical and logical changes. Electronic access logs typically will be maintained for at least 90 days.

PHYSICAL SECURITY

PLAN AND PROTECTION

Senior managers must document, implement, and maintain a physical security plan. This plan must address, at a minimum:

- Placement within an identified physical security perimeter, or within alternative measures if a completely enclosed border is not feasible, for all cyber assets within an electronic security perimeter.
- Identification of all physical access points through each physical security perimeter and measures to control entry at those access points
- Processes, tools, and procedures to monitor physical access to the perimeter(s)
- Appropriate use of physical access controls
- Review of access authorization requests and revocation of access authorization
- A visitor control program for personnel without authorized unescorted access to a physical security perimeter
- Physical protection from unauthorized access and a location within an identified physical security perimeter for cyber assets that authorize or log access or monitor access to a physical or electronic security perimeter

- Documentation and implementation of operational and procedural control to manage physical access at all access points at all times

MONITORING, LOGGING, AND RETENTION

The organization must document and implement the technical and procedural controls for monitoring physical access at all access points at all times. Unauthorized access attempts must be reviewed immediately and handled in accordance with procedures. Logging will be sufficient to uniquely identify individuals and the time of access. Physical access logs will be retained for at least 90 calendar days.

We will leverage the guidance in NIST SP800-92, Guide for Computer Security Log Management,[39] when performing this type of assessment.

MAINTENANCE AND TESTING

Each physical security system must be tested at least once every three years to ensure it operates correctly. Testing and maintenance records must be maintained at least until the next testing cycle. Outage records must be retained for at least one calendar year.

SYSTEMS SECURITY MANAGEMENT

Security management requires a variety of methods for determining that hardware and software technologies work as expected and do not adversely impact the overall system or existing cyber security controls. It is also necessary that such methods be documented and that the documentation be reviewed at least annually.

TEST PROCEDURES

The organization must ensure that new cyber assets and significant changes to existing cyber assets do not adversely impact the overall security posture of the system or of existing cyber security controls. Security patches, cumulative service packs, and version upgrades are all considered significant changes.

The organization will do this by creating, implementing, and maintaining cyber security test procedures. Testing must be performed in a manner that reflects actual production environments and the results must be documented.

In reasoning about test procedures, we will also leverage some guidance in NIST SP800-115, Technical Guide to Information Security Testing and Assessment,[40] and NIST SP800-42, Guideline on Network Security Testing.[41]

---

[39] NIST SP800-92, Guide to Computer Security Log Management (http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf).

[40] NIST SP800-115, Technical Guide to Information Security Testing and Assessment (http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf).

CONFIGURATION AND MAINTENANCE

The organization will document and implement processes that help ensure ongoing systems security. These include:

- Ensuring that only the ports and services required for normal and emergency operations are enabled
- Tracking, evaluating, testing, and installing applicable cyber security patches for all cyber assets within the electronic security perimeters
- Using and updating antivirus and malicious software prevention tools, where technically feasible
- Technical and procedural controls (for example, logs, user account review, account management, restricting use of shared accounts, password use) that enforce access authentication of and accountability for all user activity
- Restrictions on who can perform maintenance and repair, special procedures for emergency maintenance or repair, remote configuration and maintenance, and so on

We will also leverage guidance in NIST SP800-83, Guide to Malware Incident Prevention and Handling.[42]

MONITORING CAPABILITY

To ensure the security state of the system can be determined, it is necessary that all cyber assets, where technically feasible, include automated tools or have associated organizational process controls to monitor cyber-security-related system events. Each of these automation mechanisms or processes must be documented. The monitoring, whether automated or manual, must issue alerts for detected cyber security incidents. All such events will be logged and reviewed, and the log typically will be maintained for at least 90 calendar days.

DISPOSAL OR REDEPLOYMENT

To ensure sensitive information is not released accidentally, the organization will document and implement formal methods, processes, and procedures for disposal or redeployment of cyber assets that are within an electronic security perimeter. Procedures will include, at a minimum, destroying or erasing the data storage media and maintaining records of asset disposition.

We will also follow some of the guidelines in NIST SP800-88, Guidelines for Media Sanitization.[43]

---

[41] NIST SP800-42, Guideline on Network Security Testing (http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf).

[42] NIST SP800-83, Guide to Malware Incident Prevention and Handling (http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf).

[43] NIST SP800-88, Guidelines for Media Sanitization (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)

VULNERABILITY ASSESSMENT

Assessments broaden and deepen awareness of threats, attacks, vulnerabilities, and the effectiveness of existing controls. They also establish baselines against which future assessments can be gauged to determine if planned improvements have occurred. Assessments can also promote additional cyber security action by focusing management attention on important system details and how the failure of controls can adversely affect the business.

We conduct assessments to attain several objectives. Perhaps the most important is to identify all critical vulnerabilities in physical and cyber components, as well as in their interdependencies. However, the process also gives us the opportunity to identify and rank key assets, develop the business case for cyber security investment, and enhance the awareness of all cyber security stakeholders.

At a high level, a vulnerability assessment can be divided into phases of preassessment, assessment, and postassessment, which comprise the following activities:

- Preassessment
  - Define scope of assessment
  - Establish information protection procedures
  - Identify and rank critical assets
- Assessment
  - Analyze network architecture
  - Assess threat environment
  - Conduct penetration testing
  - Assess physical security
  - Conduct physical asset analysis
  - Assess operations security
  - Examine policies and procedures
  - Conduct impact analysis
  - Assess infrastructure dependencies
  - Conduct risk characterization
- Postassessment
  - Prioritize recommendations
  - Develop action plan
  - Capture lessons learned and best practices
  - Conduct training

We will leverage the process in the DOE Vulnerability Assessment Methodology—Electric Power Infrastructure,[44] and in the ISACA IS Auditing Procedure, Security Assessment–Penetration Testing and Vulnerability Analysis.[45]

CONTINGENCY PLANNING

Contingency planning establishes interim measures to recover personnel, process, and information technology capabilities following a disruption, outage, or emergency. The range of such measures is virtually unlimited; therefore, much of this initial discussion will occur at a high level.

PLANNING FOR FAILURE

Planning should follow a seven-step contingency process. These seven progressive steps are designed to be integrated into each stage of the system development life cycle:

- **Develop the contingency planning policy statement.** A formal policy provides the authority and guidance necessary to develop an effective contingency plan.
- **Conduct the business impact analysis (BIA).** The BIA helps to identify and prioritize critical IT systems and components.
- **Identify preventive controls.** Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life-cycle costs.
- **Develop recovery strategies.** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
- **Develop an IT contingency plan.** The contingency plan should contain detailed guidance and procedures for restoring a damaged system.
- **Plan testing, training, and exercises.** Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation. Both activities improve plan effectiveness and overall agency preparedness.
- **Plan maintenance.** The plan should be a living document that is updated regularly to remain current with system enhancements.

We will also leverage the methodology in NIST SP800-34, Contingency Planning Guide for IT Systems.[46]

INCIDENT REPORTING AND RESPONSE PLANNING

[44] DOE Vulnerability Assessment Methodology – Electric Power Infrastructure (http://www.esisac.com/publicdocs/assessment_methods/VA.pdf).

[45] ISACA IS Auditing Procedure, Security Assessment – Penetration Testing and Vulnerability Analysis (ISACA IS Auditing Procedure, Security Assessment–Penetration Testing).

[46] NIST SP800-34, Contingency Planning Guide for Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf).

Incident response is a critical part of cyber security management. Effective response requires a significant amount of advance planning that addresses a variety of personnel, process, and technology decisions. A brief list of planning activities includes:

- Creating an incident response policy and plan
- Developing procedures for performing incident handling and reporting, based on the incident response policy
- Setting guidelines for communicating with outside parties regarding incidents
- Selecting a team structure and staffing model
- Establishing relationships between the incident response team and other groups, both internal (for example, legal department) and external (for example, law enforcement agencies)
- Determining what services the incident response team should provide
- Staffing and training the incident response team

Ongoing vigilance is a key to preparedness. Recurring activities that help maintain incident response capability include:

- Establishing, documenting, maintaining, and exercising on-hours and off-hours contact and notification mechanisms for various individuals and groups within the organization (for example, chief information officer [CIO], head of information security, IT support, business continuity planning) and outside the organization (for example, US-CERT, incident response organizations, counterparts at other organizations).
- Planning and documenting guidelines for the prioritization of incident response actions based on changing business impacts.
- Preparing one or more individuals to act as incident leads who are responsible for gathering information from the incident handlers and other parties, and distributing relevant information to the parties that need it.
- Practicing the handling of large-scale incidents through exercises and simulations on a regular basis; such incidents happen rarely, so incident response teams often lack experience in handling them effectively.

We will leverage the methodology in NIST SP800-34, Contingency Planning Guide for IT Systems, as well as portions of NIST SP800-61 Rev. 1, Computer Security Incident Handling Guide,[47] and NIST SP800-86, Guide to Integrating Forensic Techniques into Incident Response.[48]

RECOVERY PLANS

[47] NIST SP800-61, Computer Security Incident Handling Guide (http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf).

[48] NIST SP800-86, Guide to Integrating Forensic Techniques into Incident Response (http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf).

Contingency planning defines interim measures that both help prevent and increase the speed with which organizations can recover from service disruptions. Such planning is unique to each system, and creating specific measures requires a detailed understanding of specific scenarios. This includes criticality of affected components and data, the associated technology, functions, security considerations, and related processes. Interim measures that are likely applicable across a broad range of disruptions include:

- Relocation of information systems and operations to an alternate site
- Recovery of information system functions using alternate equipment
- Performance of information system functions using manual methods

Planning generally follows a seven-step process that can ensure resulting plans will effective for local needs. These steps are as follows:

- **Develop the contingency planning policy statement.** A formal policy provides the authority and guidance necessary to develop an effective contingency plan.
- **Conduct business impact analysis (BIA)**. The BIA helps identify and prioritize information systems and components critical to supporting the organization's business functions. A template for developing the BIA is provided to assist the user.
- **Identify preventive controls.** Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life-cycle costs.
- **Create contingency strategies.** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
- **Develop an information system contingency plan.** The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.
- **Ensure plan testing, training, and exercises.** Testing validates recovery capabilities, training prepares recovery personnel for plan activation, and exercising the plan identifies planning gaps. Combined, the activities improve plan effectiveness and overall organization preparedness.
- **Ensure plan maintenance.** The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

An effective process of planning, documentation, and practice allows an organization to efficiently work through the disruption response phases of activation, recovery, and reconstitution.

We will leverage the methodology in Draft NIST SP800-34 Rev 1, Contingency Planning Guide for IT Systems, as well as portions of NIST SP800-61 Rev. 1, Computer Security Incident Handling Guide, and NIST SP800-86, Guide to Integrating Forensic Techniques into Incident Response.

FINANCIAL AND LEGAL TOOLS

Demonstration participants many rely on a variety of business software (for example, accounting packages) and agreements (for example, with subcontractors) to ensure effective and secure business operations. As applicable and appropriate, we will examine the impact of smart grid technology deployment on these systems and vice versa.

AUDIT

The operation or execution of every control important to reducing an unacceptable risk needs to be audited, both for whether it's performed and whether it's effective. In the larger context of the NRECA demonstrations, much of this work will be done by the NRECA IV&V team. However, audit as a high-level functional activity will also be addressed by the ICS Team as needed.

ONGOING REVIEW AND REVISIONS

The NRECA team will include periodic reviews of the decisions and approaches taken during this demonstration. At a minimum, a review will be triggered by large or significant changes in the statutory, regulatory, compliance, interoperability, or security drivers affecting our demonstration activities.

CYBER SECURITY ADVICE FOR COOPERATIVES

The NRECA team, as part of its demonstration activities, will use a selection of the technologies as discussed in Section 4 above to make and enforce security decisions for a demonstration activity type. As necessary, we can then work with participants to apply appropriate portions of Section 4 in a phased manner to specific instantiations of an activity type.

Safely and securely integrating demonstration technologies into the cooperative environments will likely require local changes to ensure new and ongoing risks are managed effectively. These changes will likely be needed in a variety of areas.

The NRECA CRN Cyber Security E-Handbook[49] describes the need for a cyber security program that mitigates risks, addresses compliance and regulatory requirements, and results in streamlined operations and increased productivity. Because this program must be successful in an environment with rapidly changing threats, requirements, laws, costs, and technology, it must also be robust and adaptable.

Computerization and common office networking have penetrated most cooperatives over the past few years. An increasing number of devices are capturing data that may have privacy implications. Consequently, these organizations have had to quickly become proficient in an array of technology-driven risk management processes, controls, and configurations. These include:

- Desktop and files:
  - Identity theft, phishing, data theft, flash/thumb drives, Spyware + Ad-ware, spam
- Controls:
  - Technical, operational, managerial, incident management, logs
- Messaging:
  - E-mail + attachments, instant messaging (IM) (internal and external)
- Physical security:
  - Access control + logs, video cameras, climate control, back-up power (UPS + generator), fire suppression
- SCADA:
  - Live data access, historical data access, control vs. monitoring, compliance agencies, network firewall, PC firewall
- Network and business applications:
  - Passwords + wireless, PCI compliance + DMZ, internal vulnerability scan, internet/extranet, remote access, patch management
- Cyber security:

[49] Cyber Security E-Handbook, November 2008, located at https://www.cooperative.com/crn.

  - Firewalls + appliances, external vulnerability scan, intrusion detection + intrusion prevention (IDS/IPS), honey pots, antivirus
- Other:
  - Back-up + restoration, internet insurance, separation of duties, security administration, security administration, staff certification

With the advent of the smart grid, there are now additional concerns that must be addressed in a cooperative's comprehensive risk management program. These include:

- The expanded and expanding regulatory and statutory environment
- New and evolving data communications protocols
- A broad array of software applications and technologies
- Greatly expanded data processing and data retention needs
- Fully automated operations
- Expanded need for incident response
- Detecting and responding to new types of fraud
- Service-level agreements and supply chain relationships that enforce cyber security requirements
- Awareness and technical training

It is important to understand that a sustainable risk management program will combine all of these elements, as appropriate, into a cohesive framework; it will not be a patchwork of individual activities. It is equally important to understand that, despite many similarities, each cooperative's risk management program will be uniquely shaped by local requirements, risks, resources, and culture.

The similarities are driven by the core security properties all cooperatives seek: confidentiality, integrity, availability, and nonrepudiation, as well as compliance. Achieving these to the extent necessary for a given environment will result from applying similar design approaches to implement security across disparate organizations. These secure design principles include:

- **Economy of mechanism.** A simple security design is essential because complex systems often host latent exposures. Concise design and implementation allow both fewer access paths and easier inspection of security features.
- **Fail-safe defaults.** In any large system, denial of access by default allows for secure operations and access paths: permissions can then be added as necessary. Permission errors in a fail-by-default system are easily noticed by enabling effective troubleshooting and maintenance procedures.
- **Complete mediation.** Complete mediation guarantees that security controls are universally applied to all subjects and objects in the intended domain. For example, a system that authenticates every user log-in respects this property.
- **Open security design.** Open design dictates that the security of a system not be reliant upon the secrecy of controls. Adherence to this principle allows security mechanisms to

be reviewed openly without risk to the system. The presumption of code or algorithm secrecy should never be relied upon to protect software or data, and no system should depend on the ignorance of attackers for security.

- **Separation of privilege.** This security design principle results in multiple controls over system resources. Multiple keys or required conditions for access afford additional protection against attacks.
- **Least privilege.** Employees should only be able to access the information necessary to complete the employees' job function, limiting the potential for errors or misuse of privileges. Constraining user privilege also reduces unnecessary interactions between privileged programs and the minimal levels required for operation.
- **Least common mechanism.** Sharing of programmable objects and resources among multiple users should be minimized. Mechanisms common to multiple users create possible information exchange that could compromise security. Common mechanisms typically do not allow separate levels of certification and functionality.
- **Psychological acceptability.** Security should always be easy to use; otherwise, employees will attempt to circumvent safeguards, rendering the security wholly ineffective. Employees will more likely abide by a security implementation with automatic protection mechanisms and simple use requirements. The implementation of security and the security goals of the employee should coincide.

As cooperatives, along with vendors and integrators, focus on lower-level secure implementation choices for processes, software, and other technologies, the local differences will begin to appear. These will likely manifest themselves in changes to policy, procedure, and technology configuration choices.

Configuration choices include, but are not limited to, logging thresholds, use of encryption, data polling intervals, password restrictions, data backup intervals, and so on. All of these decisions should be documented in local security policies and reinforced with procedures.

CYBER SECURITY ADVICE FOR VENDORS

The NRECA team, as part of its demonstration activities, will use a selection of the technologies as discussed in Section 4 above to make and enforce security decisions for a given demonstration activity type. As necessary, we can also work with vendors to help in applying appropriate portions of Section 4 in a phased manner to specific product engineering activities.

The NRECA team will provide advice to vendors on foundational security design and implementation approaches, testing, and responding to specific attacks and vulnerabilities. From an engineering process perspective, guidance to vendors will focus on appropriate security gates in their engineering processes. These gates typically include:

- **Threat modeling and control selection.** We must consider a system from the point of view of an adversary and the types of attacks to which a skilled attacker may subject a system. During this phase, the goals of an attacker are considered in terms of the system's assets that an attacker may try to compromise. For that purpose, the system's assets and the attack surface (for example, system entry points) are enumerated. Attack patterns are then systematically documented that may enable an attacker to compromise the confidentiality, integrity, or availability of various system assets.
- **Implementing risk-based controls.** Fundamentally, risk-based controls rely on empirical evidence to support the notion that the failure to implement a specific control in the target environment will result in an undesirable impact of some likelihood that cannot be dismissed. Such empirical evidence is usually obtained from exhaustive testing and simulation exercises that emulate all possible threats. However, because such exercises are time consuming and contain an almost limitless set of control variations and permutations, targeted testing is usually deployed to address controls unique to the environment and supplemented by industry best practices and standards, legal and regulatory frameworks, and the expertise and experience of the team members.
- **Implementing compliance-based controls.** While generally demonstrating significant overlap with risk-based controls, these controls are selected specifically because a law, regulation, or industry standard requires the control to be implemented. In some cases, a deviation may be allowed based on the feasibility of implementing the control and the potential risk of not implementing the control.
- **Documentation and design review**. This activity ensures that policies, procedures, plans, and schematics sufficiently identify all security controls. During the early stages of the development life cycle, this activity focuses on the initial security design and concept of operations and may include facilitated sessions where developers and system integrators offer up proposed designs, including security controls. The assessment team then compares the designs against the controls selected. During later stages, the review ensures that the documentation is complete from both a risk and compliance perspective.
- **Configuration and code analysis**. This exercise examines configuration settings of devices used for the project including meters, collectors, head-end systems (user interfaces), and MDM systems, and compares those settings to what the team views as best practices or necessary to meet compliance requirements. For commercial off-the-shelf (COTS)

products, it is understood that code review may not be possible. In that case, the team can analyze configuration settings and rely on other technical tests such as vulnerability scans and penetration tests to accomplish the objectives.

- **Vulnerability scanning**. As part of the testing process, a variety of vulnerability scanning tools can be leveraged to identify potential vulnerabilities in the network and the applications. In many cases, the proprietary nature of smart grid components means that standard vulnerability scanning tools will be of limited use. Consequently, the team can draw on penetration testing, configuration analysis, and design reviews to properly identify potential and actual vulnerabilities.
- **Penetration testing.** Penetration testing uses a combination of manual and automated techniques and is in many respects similar to the predeployment penetration tests performed during the development life cycle. Penetration testing on the Smart Grid should focus on the physical, network, software, and people aspects of security. A combination of technical attacks leveraging information obtained through social engineering techniques may be in scope of this approach.
- **Security test and evaluation** is also an iterative process that verifies the existence and effectiveness of security controls from a risk and compliance perspective. All portions of the process are deployed during the design, implementation, and operational stages of the life cycle. During each phase the test and evaluation process asks:
  - Are the security controls that are being designed or implemented sufficient to protect the system from the attack patterns that have been identified?
  - What in the system's design or implementation open up new attack vectors for an adversary? How do we address these?

If the controls selection and assessment process is deployed correctly, the security design and implementation process should be very simple.

CONCLUSION

This document has been written in response to a specific DOE requirement associated with DOE's contract award to NRECA for a Smart Grid Demonstration Program. The NRECA demonstration comprises a short Phase I that establishes project plans and approaches, and a multiyear Phase II that acquires, develops, integrates, deploys, and monitors smart grid technology.

This Interoperability And Cyber Security Plan (ICSP) represents the NRECA team's current thinking on executing program goals during Phase II of this project. The NRECA team comprises experts from multiple disciplines including power systems, smart grid protocols, software development, software security, independent validation and verification, and related disciplines. Together, these represent the core competencies required to successfully execute this project.

This ICSP demonstrates the breadth and depth of the NRECA approach to ensuring functional success of smart grid deployments that also exhibit appropriate cyber security functions and properties. Of course, there remain many unknowns at this point. Standards are still being defined and developed, statutory and regulatory guidance is evolving, vendors are responding to changing market forces, hackers and researchers are finding issues in current technologies, and all stakeholders are getting smarter as they focus resources on the issues at hand. Consequently, many foundational decisions will be made upon starting Phase II of this project.

As needed, this document may be revised during Phase II to ensure that all groups comprising the NRECA demonstration team are applying current and necessary interoperability and cyber security analysis and lessons learned.

APPENDIX A: 10 ACTIVITY TYPES

Table 17. Activities by Participant provides an overview of which activity types each participant will take part in. Note the grouping of activity types into three main categories—DR, distribution automation, and enabling technologies. Table 17 also provides a useful summary of the number of participants by activity type. For example, there is only one participant (New Hampshire Electric Co-op) with an interactive thermal storage project, while 15 of the 21 electric distribution cooperative participants have DR over AMI projects.

		Demand Response			Distribution Automation			Enabling Technologies			
Types	Participants	IHD/Web Portal Pilots	DR over AMI	Interac-tive Thermal Storage	Smart Feeder Switching	Advanced Volt/Var Control	CVR*	AMI	MDM	Comm	SCADA
Activities	Adams Electric Co-op, IL	X	X		X	X	X	X		X	X
	Adams-Columbia Electric Co-op, WI				X	X	X				X
	Clarke Electric Co-op, Inc., IA	X	X		X		X	X		X	X
	Consumers Energy, IA	X	X					X		X	
	Corn Belt Power Co-op, IA									X	
	Calhoun Co. ECA		X					X			
	Humboldt Co. REC		X					X			
	Iowa Lakes EC		X								
	Midland Power Co-op		X								
	Prairie Energy Co-op		X					X			
	Delaware County Electric Co-op, NY	X	X					X		X	
	Flint EMC, GA	X						X			
	Kaua'i Island Utility Co-op, HI	X	X					X	X	X	
	Menard Electric Co-op, IL	X				X					X
	New Hampshire Electric Co-op, NH	X	X	X				X		X	
	Nolin RECC, KY	X	X		X	X	X	X		X	X
	Owen Electric Co-op, Inc., KY	X	X		X	X	X	X		X	X
	Prairie Power, Inc., IL					X					X
	Salt River Electric Co-op Corp., KY				X						
	Snapping Shoals EMC, GA	X	X		X			X		X	X
	United REMC, IN	X	X		X	X	X		X	X	
	Washington-St. Tammany EC, LA				X					X	X

Table 17. Activities by Participant.

Table 18. In-Home Display and Web Portal Activity Type.

Activity Type:	IHD / Web Portal Pilots	
Activity category:	Demand response	
Description of objectives:	This program will study the consumer behavior modifications resulting from varying the energy price signals of residential electricity consumers. Critical peak pricing (CPP), time-of-use pricing (TOU), and a combination of these two rate signals will be studied. We will conduct additional study on the interaction between these dynamic pricing signals and the existence of in-home energy use displays and Internet-based energy use Web portals. This program will also study the consumer behavior modifications resulting from the availability to consumers of data detailing their electricity use.	
Major applications:	• A1—AMI • A3—MDM • A4—DR • A8—Distribution Automation • A13—CIS • A14—DRAS Server	• A15—Demand Management • A16—Load Forecast • A18—Market Services • A20—EMC
Key components:	• C9—Energy Services Interface • C10—Meter (RF) and / or C11—Meter (PLC) • C12—Customer EMS and IHD	• C13—Thermal Storage • C14—Thermostat • C17—Customer Appliances / Equipment
Standards / Protocols:	• MultiSpeak® • IEC 61968, Part 9 • ANSI C12.19 and C12.22	• NAESB and OASIS • ZigBee SEP (1.0, 2.0) • HomePlug
Integration concerns:	• Time frame for development of interface standards between the Distribution Operations domain and the Generation & Transmission and Markets domains.	
Interoperability concerns:		
Cyber security concerns:		

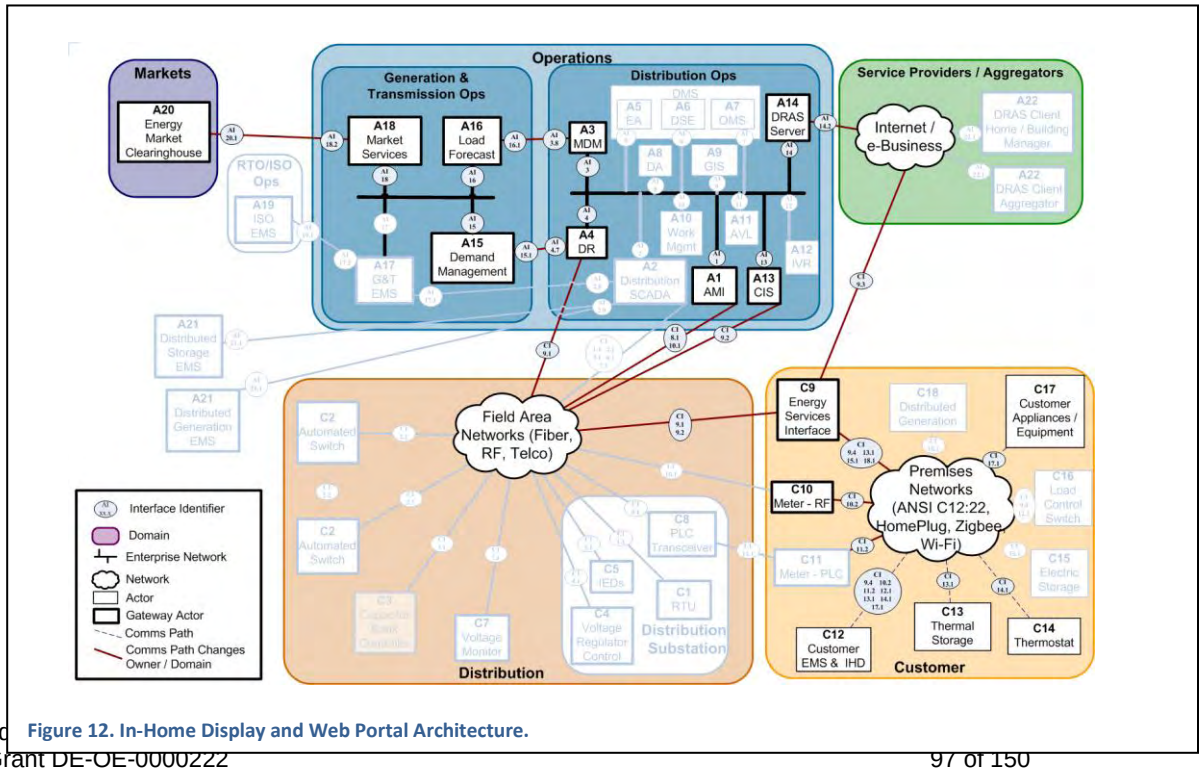


Figure 12. In-Home Display and Web Portal Architecture.

Table 19. Demand Response over AMI Networks Activity Type.

Activity Type:	Demand Response over AMI Networks	
Activity category:	Demand response	
Description of objectives:	This program will study the load impacts resulting from cooperative direct control of consumer water heaters and air conditioners. During high-cost periods, cooperatives will be able to remotely shut off end use water heaters and air conditioners.	
Major applications:	• A1—AMI • A3—Meter Data Management • A4—DR	• A13—CIS • A15—Demand Management • A15—Load Forecast
Key components:	• C8—PLC Transceiver • C9—Energy Services Interface • C10—Meter (RF) and / or C11—Meter (PLC) • C12—Customer EMS and IHD	• C13—Thermal Storage • C14—Thermostat • C16—Load Control Switch • C17—Customer Appliances / Equipment
Standards / Protocols:	• MultiSpeak® • IEC 61968, Part 9 • ANSI C12.19 and C12.22	• ZigBee SEP (1.0, 2.0) • HomePlug
Integration concerns:	• Timeframe for develop of interface standards between the Distribution Operations domain and the Generation & Transmission domain.	
Interoperability concerns:	• AMI	
Cyber security concerns:		

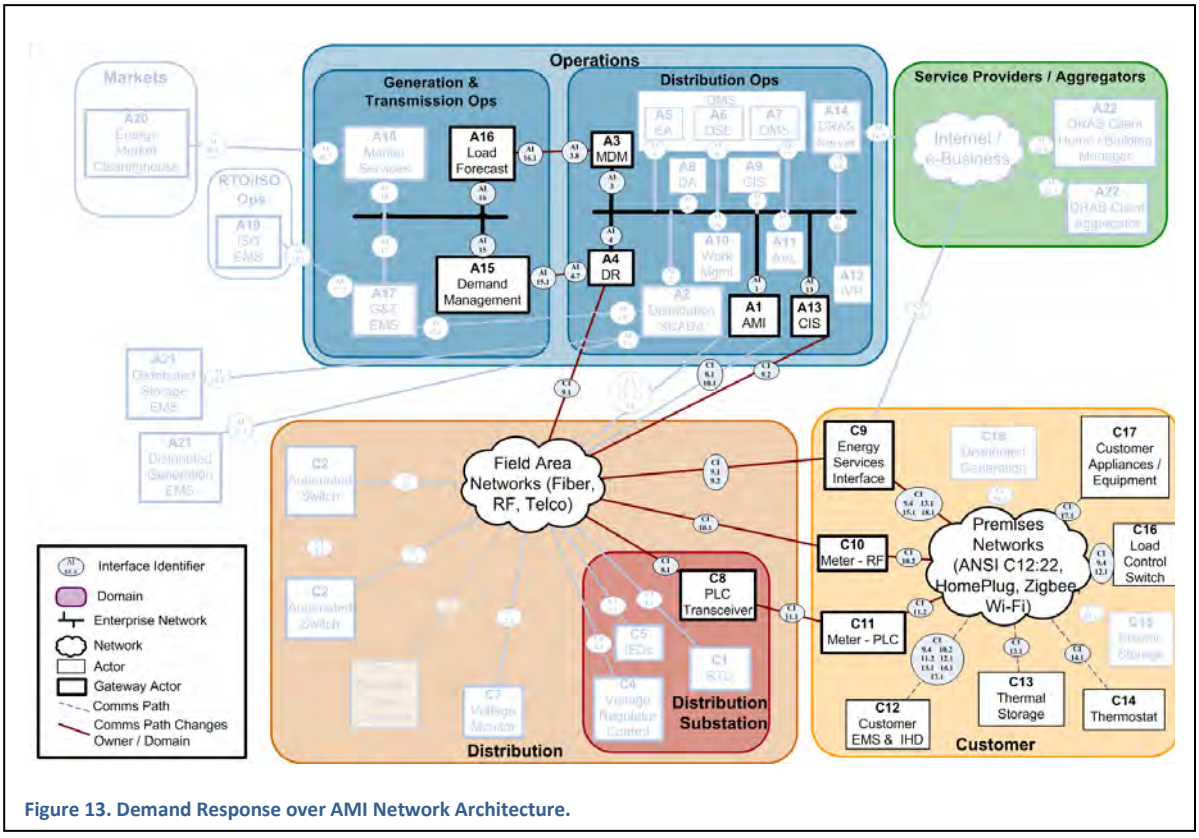


Figure 13. Demand Response over AMI Network Architecture.

Table 20: Interactive Thermal Storage Activity Type.

Activity Type:	Interactive Thermal Storage	
Activity category:	Demand response	
Description of objectives:	This demonstration activity will test and study the potential of using electric water heaters equipped with sophisticated control technology as distributed thermal storage units. The core conflict in direct load management is that consumers will perceive service degradation (in the form of increased household temperatures or of running out of hot water on demand). Historically, the approach to extending the control period without inconvenience to the end user was to encourage larger units with heavy insulation and high efficiencies. New technologies are superior in providing much more sophisticated control by pre-heating water to 170 degrees ahead of the desired control period. Coupled with cold-water mixing valves, this would substantially extend water heater control periods. If proven effective, this technology could serve to firm up wind generation or be bid into ancillary services markets.	
Major applications:	• A1—AMI • A4—DR	• A14—DRAS Server
Key components:	• C9—Energy Services Interface • C12—Customer EMS and IHD	• C13—Thermal Storage • C17—Customer Appliances / Equipment
Standards / Protocols:	• MultiSpeak® • IEC 61968, Part 9	• Proprietary PLC • ZigBee SEP • Home Plug
Integration concerns:	• Single manufacturer device. • Integration of Steffes load management control device with Distribution Operations systems such as AMI and DR.	
Interoperability concerns:	• Compatibility with Energy Services Interface and Customer EMS / IHD or standalone devices. • Steffes thermal storage system support for MultiSpeak® HAN communications standards.	
Cyber security concerns:		

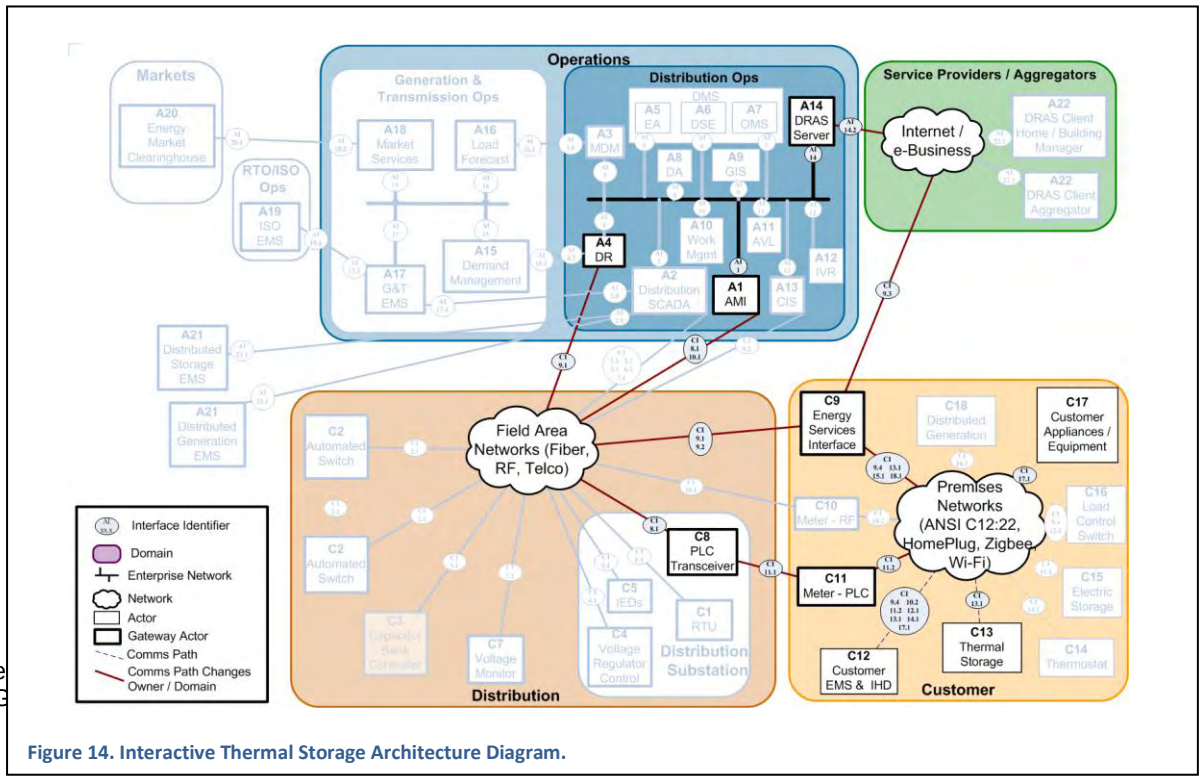


Figure 14. Interactive Thermal Storage Architecture Diagram.

Table 21. Smart Feeder Switching Activity Type.

Activity Type:	Smart Feeder Switching	
Activity category:	Distribution automation	
Description of objectives:	Smart Feeder Switching entails automated network reconfiguration of electrical distribution network to minimize interruptions and improve system reliability. Technically known as fault location, isolation, and service restoration (FLISR), this system should produce substantial improvements in the System Average Interruption Duration Index (SAIDI) and other indices.	
Major applications:	• A2—Distribution SCADA	• A8—Distribution Automation
Key components:	• C2—Automated Switch	
Standards / Protocols:	• MultiSpeak® • ICCP IEC 60870-6/TASE.2	• DNP3 • IEC 61850
Integration concerns:	• Most Automated Switches will support DNP3 for communications to SCADA and DA. Automated switchgear from vendors use proprietary controls. Migration to IEC 61850 as may be required by NIST. Priority Action Plan 6 maps DNP3 to IEC 61850.	
Interoperability concerns:	• There are commercially available protocol conversion gateways to convert DNP3 to IEC 61850 if required. • Proprietary vendor control algorithms will require all automated switches that are part of the activity to use common switch gear controls.	
Cyber security concerns:		

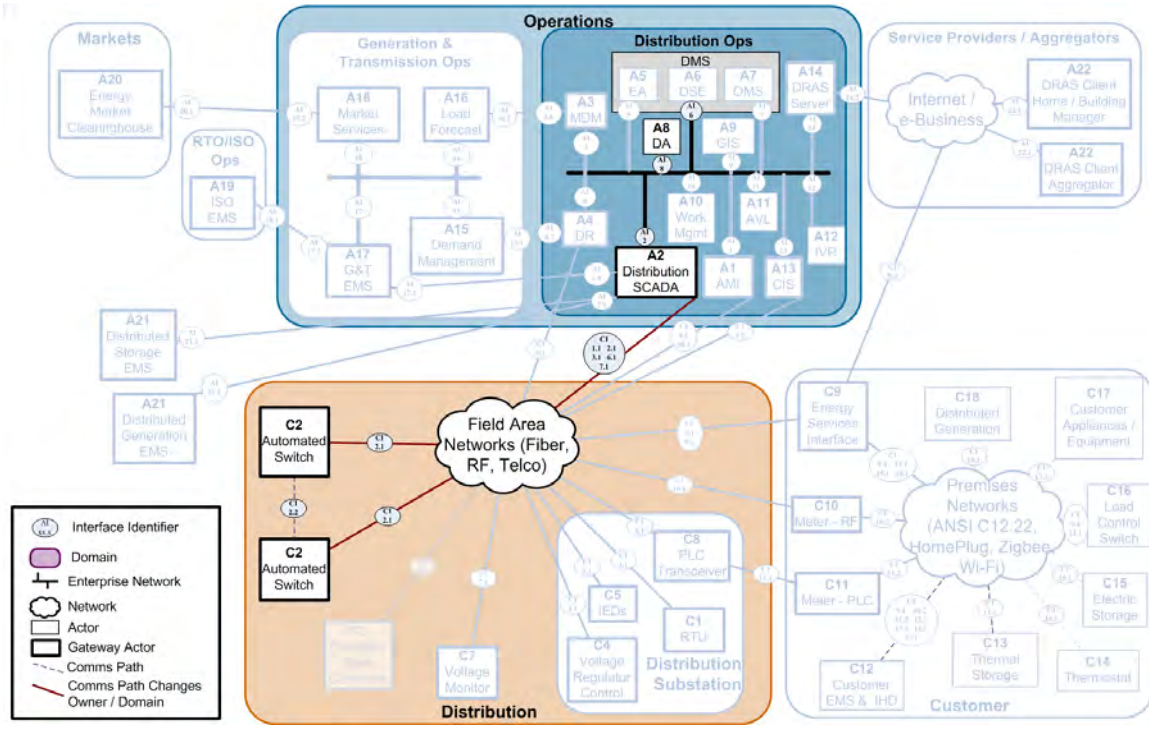


Figure 15. Smart Feeder Switching Architecture.

Table 22. Advanced Volt/VAr Activity Type.

Activity Type:	Advanced Volt/VAr	
Activity category:	Distribution automation	
Description of objectives:	Volt/VAr control of distribution feeders will result in improved voltage support on long distribution feeders while also minimizing distribution line energy losses.	
Major applications:	• A2—Distribution SCADA • A6—Distribution State Estimation	• A8—Distribution Automation
Key components:	• C3—Capacitor Bank Controller	• C7—Voltage Monitor
Standards / Protocols:	• MultiSpeak® • ICCP IEC 60870-6/TASE.2	• DNP3 • IEC 61850
Integration concerns:	• Most capacitor bank controllers and voltage monitors will support DNP3 for communications to SCADA and DA. Migration to IEC 61850 as may be required by NIST. Priority Action Plan 6 maps DNP3 to IEC 61850.	
Interoperability concerns:	• There are commercially available protocol conversion gateways to convert DNP3 to IEC 61850 if required.	
Cyber security concerns:		

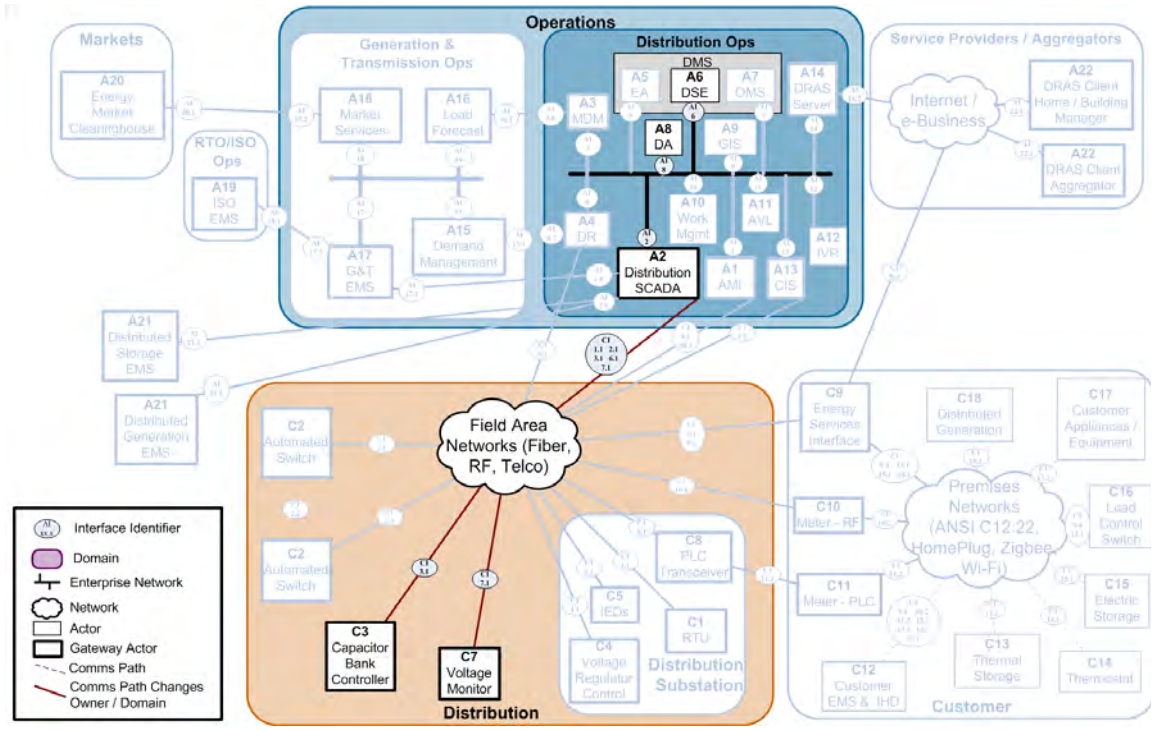


Figure 16. Advanced Volt/VAR Architecture.

Table 23. Conservation Voltage Reduction Activity Type.

Activity Type:	Conservation Voltage Reduction (CVR)	
Activity category:	Distribution automation	
Description of objectives:	Conservation voltage reduction is typically employed to accomplish reduction of peak demand during certain times of the day. Peak demand reduction during coincident peaks results in substantial wholesale power demand cost savings for utilities.	
Major applications:	• A2—Distribution SCADA	• A8—Distribution Automation
Key components:	• C4—Voltage Regulator Control	• C7—Voltage Monitor
Standards / Protocols:	• MultiSpeak® • ICCP IEC 60870-6/TASE.2	• DNP3 • IEC 61850
Integration concerns:	• Most voltage regulator controls and voltage monitors will support DNP3 for communications to SCADA and DA. Migration to IEC 61850 as may be required by NIST. Priority Action Plan 6 maps DNP3 to IEC 61850.	
Interoperability concerns:	• There are commercially available protocol conversion gateways to convert DNP3 to IEC 61850 if required.	
Cyber security concerns:		

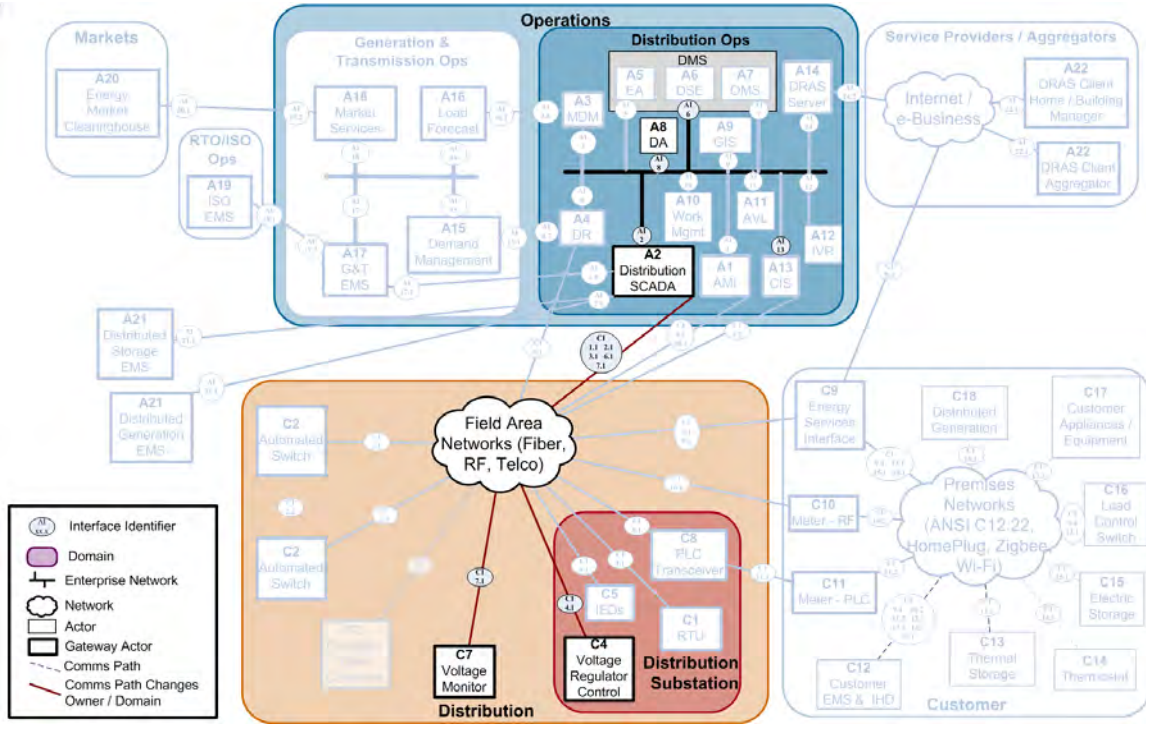


Figure 17. Conservation Voltage Reduction Architecture.

Table 24. Advanced Metering Infrastructure (AMI) Activity Type.

Activity Type:	**Advanced Metering Infrastructure (AMI)**	
Activity category:	Enabling technology for demand response	
Description of objectives:	Advanced metering infrastructure systems comprise state-of-the-art electronic and digital hardware and software, which combine interval data measurement with continuously available remote communications. These systems enable measurement of detailed, time-based information as well as frequent collection and transmittal of such information to various parties.	
Major applications:	• A1—AMI Head-end • A3—Meter Data Management • A5—EA	• A6—Distribution State Estimation • A7—OMS • A9—GIS • A13—CIS
Key components:	• C8—PLC transceiver • C11—Meter (PLC)	• C10—Meter (PLC)
Standards / Protocols:	• MultiSpeak® • IEC 61968, Part 9 • Proprietary vendor AMI PLC protocols	• ANSI C12.22 • ZigBee Pro and SEP • Proprietary vendor AMI RF protocols
Integration concerns:	• Integrating multiple AMI vendor systems with other enterprise applications such as meter data management.	
Interoperability concerns:	• AMI systems use proprietary RF, PLC and communications protocols. If a participant is migrating from Vendor A to Vendor B dual AMI networks and AMI head-ends will need to be used.	
Cyber security concerns:		

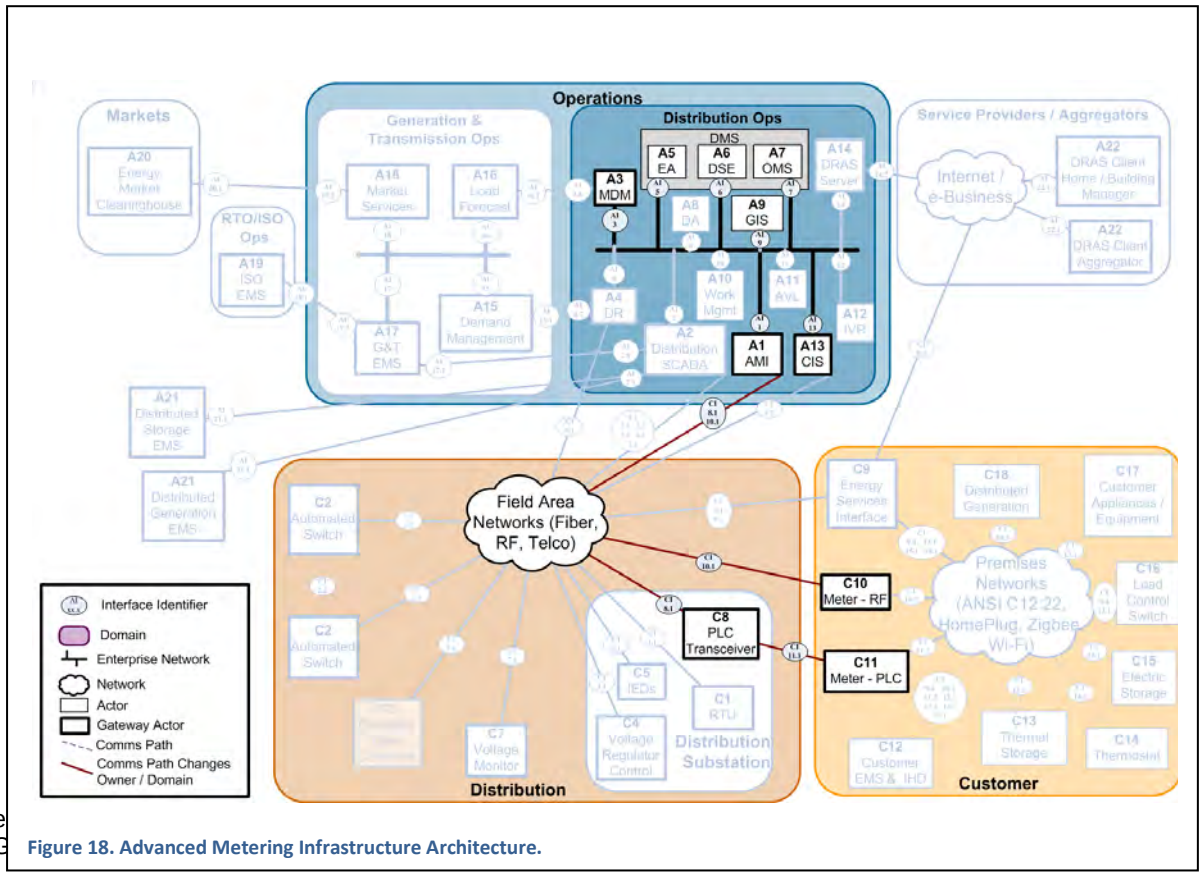


Figure 18. Advanced Metering Infrastructure Architecture.

Table 25. Meter Data Management Activity Type.

Activity Type:	Meter Data Management (MDM)	
Activity category:	Enabling technology for demand response	
Description of objectives:	An MDM system performs long-term data storage and management for the data that are now being delivered by smart metering systems. These data consist primarily of usage data and events that are imported from AMI systems. An MDM system will typically import the meter data then validate, edit, and evaluate (VEE) cleanse the data before making it available to end users.	
Major applications:	• A1—AMI Head-end • A2—Distribution SCADA • A3—Meter Data Management • A4—DR • A5—Engineering Analysis (DMS)	• A6—Distribution State Estimation (DMS) • A7—OMS • A13—CIS • A16—Load Forecast
Key components:	• None (component interfaces are via the AMI head-end, Distribution SCADA and DR systems)	•
Standards / Protocols:	• MultiSpeak® • IEC 61968, Part 9 •	• ANSI C12.19 • ZigBee SEP (1.0, 2.0)
Integration concerns:	• Integrating multiple AMI vendor systems	
Interoperability concerns:		
Cyber security concerns:		

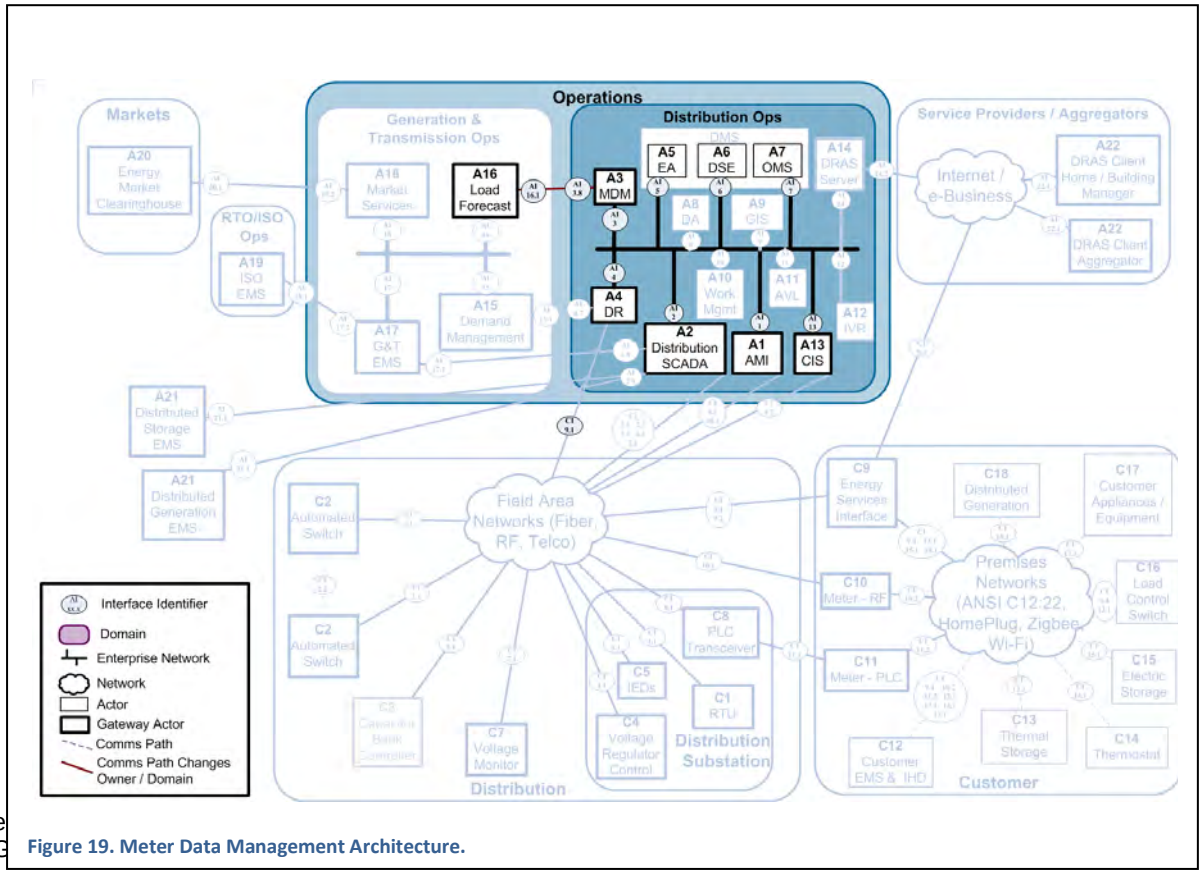


Figure 19. Meter Data Management Architecture.

Table 26. Communications Systems Activity Type.

Activity Type:	Communications Systems	
Activity category:	Enabling technology for demand response and distribution automation	
Description of objectives:	Communication is the means of getting information from one piece of equipment to another. This could be using microwave, unlicensed spread spectrum, licensed UHF, and so on. Communications system ICS were considered to be outside of the scope of this document but will be addressed as part of Phase II.	
Major applications:	Means of data transmission for home area networks (HAN), local area networks (LAN)—for example, within substation or AMI RF mesh, and wide area networks (WAN) to support AMI backhaul from substation to operations office and / or communications to field distribution automation devices.	
Key components:	• UHF/VHF radios • Microwave radios • Unlicensed spread spectrum radios • ZigBee radios	• Fiber optics • Telco (for example, DSL) • Cellular
Standards / Protocols:	• ZigBee Pro / SEP • CDMA/GSM • Proprietary vendor licensed and unlicensed radios	• WiMAX • SONET (Telcordia GR-253-CORE) • Etc.
Integration concerns:	• From a data communications perspective, the communications system should be transparent. • SNMP is most often used for communications network management systems.	
Interoperability concerns:	• Commercial wireless gateways are readily available, as most communications systems will deploy multiple technologies in a hierarchical manner. Most wireless systems now support Ethernet communications so managed switches may be used to integrate disparate systems.	
Cyber security concerns:		

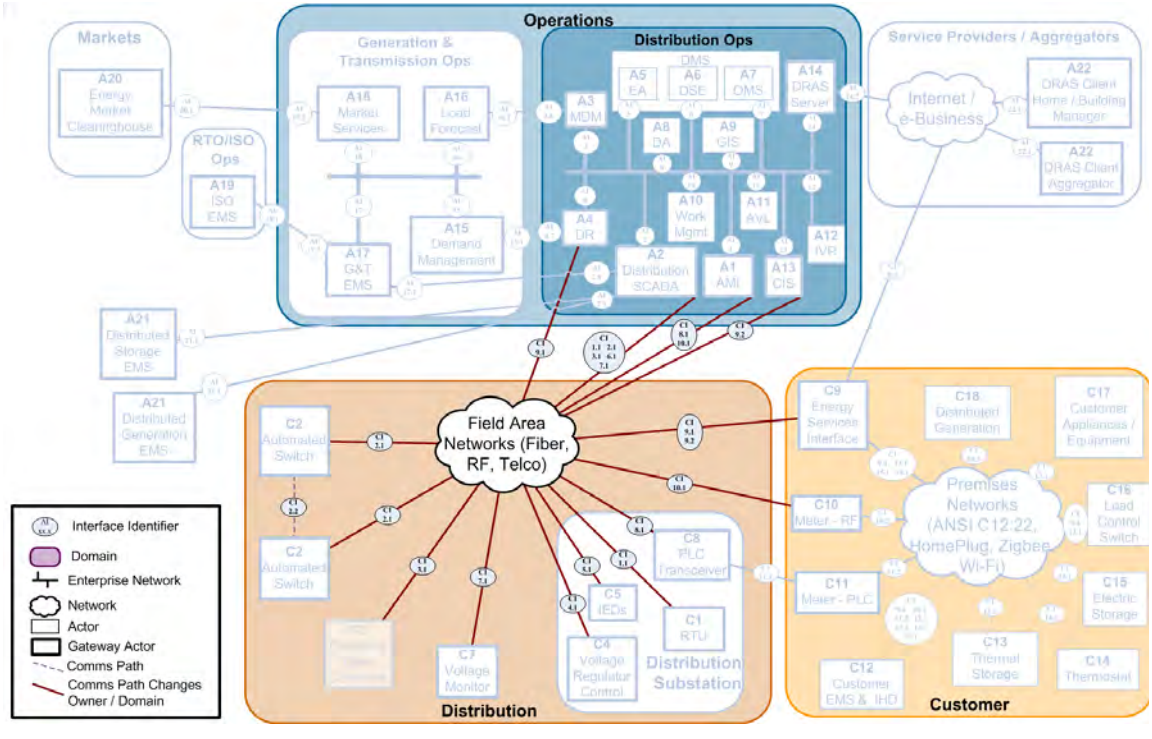


Figure 20. Communications Systems Architecture.

Table 27. Supervisory Control and Data Acquisition (SCADA) Activity Type.

Activity Type:	Supervisory Control and Data Acquisition (SCADA)	
Activity category:	Enabling technology for distribution automation	
Description of objectives:	SCADA provides a basic infrastructure to deploy basic and advanced substation and distribution system automation. It has the potential to vastly improve the operational efficiencies, and provides the tools required by operators and engineers to become more productive in their jobs. It is a key component in the process of evolving the smart grid.	
Major applications:	• A2—Distribution SCADA • A4—DR • A5—Engineering Analysis • A6—Distribution State Estimation	• A7—OMS • A8—Distribution Automation
Key components:	• C1—Remote Terminal Unit (RTU) • C2—Automated Switch • C3—Capacitor Bank Controller	• C4—Voltage Regulator Control • C5- Intelligent Electronic Devices (IED) • C7—Voltage Monitor
Standards / Protocols:	• MultiSpeak® • ICCP IEC 60870-6/TASE.2	• DNP3 • IEC 61850
Integration concerns:	• Most SCADA devices will support DNP3 for communications to SCADA and DA. Automated switchgear from vendors use proprietary controls. Migration to IEC 61850 as may be required by NIST. Priority Action Plan 6 maps DNP3 to IEC 61850.	
Interoperability concerns:	• There are commercially available protocol conversion gateways to convert DNP3 to IEC 61850 if required.	
Cyber security concerns:		

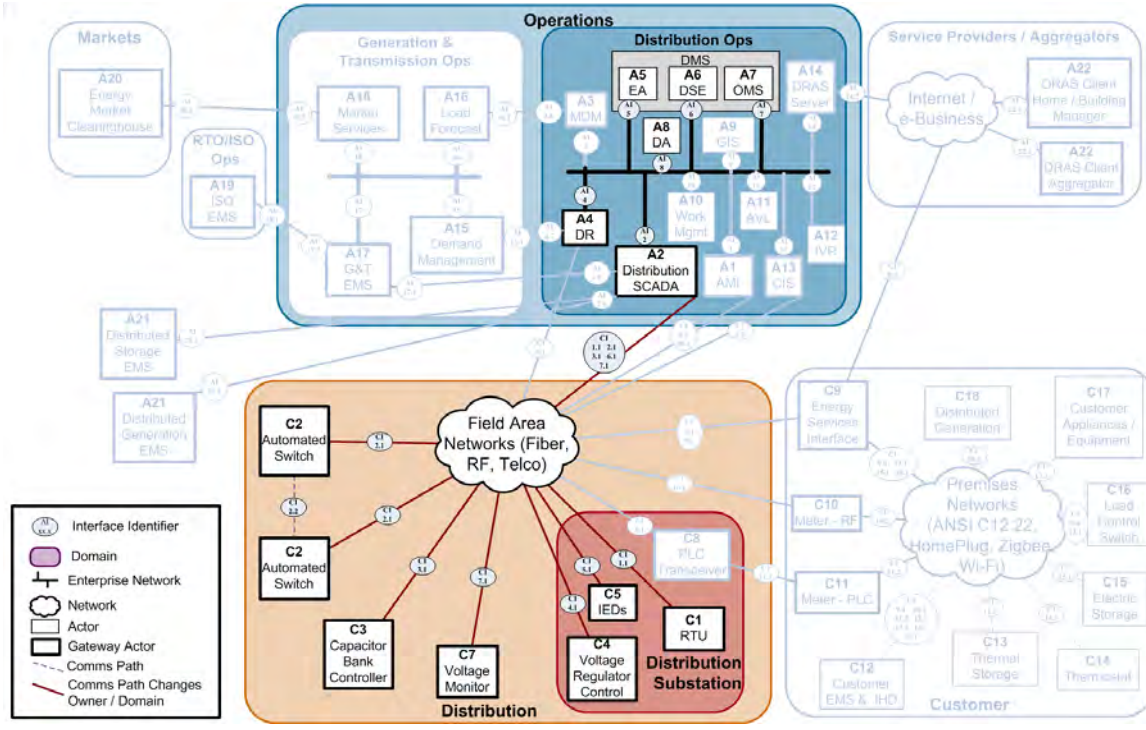


Figure 21. Supervisory Control & Data Acquisition Architecture.

APPENDIX B: ICSP AND SOPO REQUIREMENTS

The Phase I Scope of Work (SOW) from the DOE is limited to three activities. These are:

- Development of a detailed work plan
- Preparation and submission of the NEPA compliance document and, if necessary, environmental impact statements for any technology that does not earn a NEPA Finding Of No Significant ImpactThe ICSP

The Interoperability And Cyber Security Plan (ICSP) must address all of the following:

1. Understanding the regulatory environment
2. Assessing assets, deciding what is important
3. Developing policies
4. Developing procedures
5. Training
6. Providing physical security
7. Perimeter protection
8. Malware protection
9. Software security
10. Financial and legal tools
11. Monitoring
12. Audit
13. Planning for failure
14. Reviewing and revising to keep everything current

The following are the DOE's ICSP requirements from the Phase I Statement of Project Objectives (SOPO). The requirements are cross-referenced to document sections.

ID	DOE Requirements for ICSP from the Phase I SOPO	Document Cross-Reference
1	• A summary of the information exchange interfaces for communicating automation devices and systems (that is, their points of connection with other elements of the system)	Section 2.1, Section 2.2
2	• A summary of how the project will provide openly available and proprietary aspects of the interface specifications and how existing (legacy) communicating devices or systems will be integrated into the project	Section 2, Section 3.3.1, Section 3.3.2
3	• A summary of how the project will address response to failure and device upgrade scenarios, such that overall system impact is mitigated	Section 4.9.1
4	• A summary of how the project will support compatibility with NIST's emerging smart grid framework for standards and protocols	Section 3.1.2, Tables 6 and 7
5	• The information exchange interface points for each type of	Section 3.2.1,

ID	DOE Requirements for ICSP from the Phase I SOPO	Document Cross-Reference
	communicating automation device and system	Table 9
6	• The openly-available and proprietary aspects of the interface specifications	Section 3.3.1, Section 3.3.2
7	• Where a type of communicating device or system is expected in large numbers (for example, meters, sensors, consumer interfaces), the extent of support for multiple suppliers who will integrate their devices or systems that may be based on different technologies at the points of interface	Section 3.3.1
8	• If existing (legacy) communicating devices or systems are integrated into the project, the extent to which they integrate and interoperate at the points of interface with new components	Section 3.7, Section 3.2, Section 3.3
9	• The interface parties' anticipated response to failure scenarios, particularly loss of communication, such that overall system impact is mitigated in the event of such failure	Section 4.9.1
10	• The anticipated process for upgrading devices or systems (hardware and software) so that overall system operation impact is mitigated	Section 4.12
11	• The evidence that will be provided (interface, specifications, interoperability test plans and results, review, and other engineering artifacts) to ensure interoperability at the interfaces of communicating automation devices and systems	Section 3.3.1
12	• The project's ability to support compatibility with NIST's emerging smart grid framework for standards and protocols	Section 3.1.2, 3.2 and 3.3
13	• A summary of the cyber security risks and how they will be mitigated at each stage of the life cycle (focusing on vulnerabilities and impacts)	Section 4.2.5
14	• A summary of the cyber security criteria utilized for vendor and device selection	Section 3.3.1
15	• A summary of the relevant cyber security standards and/or best practices that will be followed	Section 4.2.3
16	• The methodology used to identify cyber security risks and the results of this assessment (for example, the assessment should consider the mission of the new smart grid project and also potential impacts to other critical grid control functions to which they are connected)	Section 4.2.4
17	• How cyber security risks will be mitigated at each phase of the engineering life cycle, including policy, procedural, and technical (logical and physical) controls, with emphasis on strategies for:	Section 4.2.5
18	○ Ensuring the confidentiality, integrity, and availability of device and system data and communications commensurate with the application requirements,	Section 4.2.5.1
19	○ Securing, logging, monitoring, alarming, and notification, and	Section 4.2.5.2

ID	DOE Requirements for ICSP from the Phase I SOPO	Document Cross-Reference
20	○ Applications where logical and physical security may not be under the direct jurisdiction of the installing entity	Section 4.2.5.3
21	• The relevant cyber security standards or best practices that will be used	Section 4.2.3
22	• The capability of the components or systems to be updated to meet future cyber security requirements	Section 3.3.1, Section 3.5
23	• How evidence will be provided (for example, a test plan, engineering artifacts, and independent testing and review) to demonstrate and validate the effectiveness of the cyber security controls.	Section 4.2.6

The following are NERC CIP requirements cross-referenced to document sections. While most NRECA demonstration participants are not required to meting NERC CIP requirements, the ICSP uses the requirements as a high-level structure for ensuring completeness.

ID	Document Cross-Reference	Document Cross-Reference
CIP-002-3	R1: Critical Asset Identification Method	Section 4.3
CIP-002-3	R2: Critical Asset Identification	Section 4.3
CIP-002-3	R3: Critical Cyber Asset Identification	Section 4.3
CIP-002-3	R4: Annual Approval	Section 4.3
CIP-003-3	R1: Cyber Security Policy	Section 4.4.2
CIP-003-3	R2: Leadership	Section 4.4.1
CIP-003-3	R3: Exceptions	Section 4.4.3
CIP-003-3	R4: Information Protection	Section 4.4.4
CIP-003-3	R5: Access Controls	Section 4.4.6
CIP-003-3	R6: Change Control and Configuration Management	Section 4.4.7
CIP-004-3	R1: Awareness	Section 4.5.1
CIP-004-3	R2: Training	Section 4.5.1
CIP-004-3	R3: Personnel Risk Assessment	Section 4.5.2
CIP-004-3	R4: Access	Section 4.5.2
CIP-005-3	R1:Electronic Security Perimeter	Section 4.6.1
CIP-005-3	R2: Electronic Access Controls	Section 4.6.2
CIP-005-3	R3: Monitoring Electronic Access	Section 4.6.3
CIP-005-3	R4: Cyber Vulnerability Assessment	Section 4.6.4

CIP-005-3	R5: Documentation Review and Maintenance	Section 4.6.5
CIP-006-3	R1: Physical Security Plan	Section 4.7.1
CIP-006-3	R2: Protection of Physical Access Control Systems	Section 4.7.1
CIP-006-3	R3: Protection of Electronic Access Control Systems	Section 4.7.1
CIP-006-3	R4: Physical Access Controls	Section 4.7.1
CIP-006-3	R5: Monitoring Physical Access	Section 4.7.2
CIP-006-3	R6: Logging Physical Access	Section 4.7.2
CIP-006-3	R7: Access Log Retention	Section 4.7.2
CIP-006-3	R8: Maintenance and Testing	Section 4.7.3
CIP-007-3	R1: Test Procedures	Section 4.8.1
CIP-007-3	R2: Ports and Services	Section 4.8.2
CIP-007-3	R3: Security Patch Management	Section 4.8.2
CIP-007-3	R4: Malicious Software Prevention	Section 4.8.2
CIP-007-3	R5: Account Management	Section 4.8.2
CIP-007-3	R6: Security Status Monitoring	Section 4.8.3
CIP-007-3	R7: Disposal or Redeployment	Section 4.8.4
CIP-007-3	R8: Cyber Vulnerability Assessment	Section 4.8.5
CIP-007-3	R9: Documentation Review and Maintenance	Section 4.8
CIP-008-3	R1: Cyber Security Incident Response Plan	Section 4.9.2
CIP-008-3	R2: Cyber Security Incident Documentation	Section 4.9.2
CIP-009-3	R1: Recovery Plans	Section 4.9.3
CIP-009-3	R2: Exercises	Section 4.9.3
CIP-009-3	R3: Change Control	Section 4.9.3
CIP-009-3	R4: Backup and Restore	Section 4.9.3
CIP-009-3	R5: Testing Backup Media	Section 4.9.3

APPENDIX C: BACKGROUND

The documents summarized below provide the primary guidance for the approach described in this document.

Energy Independence and Security Act

Title XIII of the Energy Independence and Security Act of 2007 (EISA) provides the following characteristics of a smart grid[50]:

(1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid

(2) Dynamic optimization of grid operations and resources, with full cyber security

(3) Deployment and integration of distributed resources and generation, including renewable resources

(4) Development and incorporation of demand response, demand-side resources, and energy-efficiency resources

(5) Deployment of ''smart'' technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation

(6) Integration of ''smart'' appliances and consumer devices

(7) Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles and thermal-storage air conditioning

(8) Provision to consumers of timely information and control options

(9) Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid

(10) Identification and lowering of unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services

EISA directs the National Institute of Science and Technology (NIST)[51] to coordinate the development of a framework to achieve interoperability of smart grid devices and systems, including protocols and model standards for information management. The GridWise Architecture Council in its Interoperability Path Forward whitepaper[52] describes interoperability as exchanging meaningful data between two or more systems and achieving an agreed-upon

[50] See http://www.ferc.gov/industries/electric/indus-act/smart-grid/eisa.pdf, Title XIII, Section 1301, Statement of Policy on Modernization of Electricity Grid.

[51] EISA sec. 1305(a), 2007.

[52] See http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf.

expectation for the response to the information exchange, while maintaining reliability, accuracy, and security.

EISA also defines smart grid functions in the context of federal matching funds for smart grid investments.[53] These include the following:

(1) The ability to develop, store, send, and receive digital information concerning electricity use, costs, prices, time of use, nature of use, storage, or other information relevant to device, grid, or utility operations, to or from or by means of the electric utility system, through one or a combination of devices and technologies

(2) The ability to develop, store, send, and receive digital information concerning electricity use, costs, prices, time of use, nature of use, storage, or other information relevant to device, grid, or utility operations to or from a computer or other control device

(3) The ability to measure or monitor electricity use as a function of time of day, power quality characteristics such as voltage level, current, cycles per second, or source or type of generation and to store, synthesize, or report that information by digital means

(4) The ability to sense and localize disruptions or changes in power flows on the grid and communicate such information instantaneously and automatically for purposes of enabling automatic protective responses to sustain reliability and security of grid operations

(5) The ability to detect, prevent, communicate with regard to, respond to, or recover from system security threats, including cyber security threats and terrorism, using digital information, media, and devices

(6) The ability of any appliance or machine to respond to such signals, measurements, or communications automatically or in a manner programmed by its owner or operator without independent human intervention

(7) The ability to use digital information to operate functionalities on the electric utility grid that were previously electromechanical or manual

(8) The ability to use digital controls to manage and modify electricity demand, enable congestion management, assist in voltage control, provide operating reserves, and provide frequency regulation

(9) Such other functions as the secretary may identify as being necessary or useful to the operation of a smart grid

FERC Statement on Smart Grid Policy

On July 16, 2009, the Federal Energy Regulatory Commission (FERC) issued a statement on smart grid policy.[54] The policy statement provides "guidance regarding the development of a smart grid

[53] EISA sec. 1306(d), 2007.

for the nation's electric transmission system, focusing on the development of key standards to achieve interoperability and functionality of smart grid systems and devices."

One purpose of the policy statement is to prioritize the development of key interoperability standards to provide a foundation for the development of many other standards. The proposed key priorities for standards development included system security and inter-system communication, along with other grid functionalities. To date, eight mandatory cyber security and physical critical infrastructure protection (CIPs) reliability standards[55] have been approved by FERC. However, the possibility that an adversary could disrupt or misuse millions of smart grid devices creates new and unknown challenges. Consequently, FERC adopted the position that cyber security standards are a key priority in protecting the electricity grid. Accordingly, FERC will require a demonstration that a proposed smart grid standard directly incorporates cyber security protection provisions or incorporates cyber security protection provisions from other smart grid or reliability standards.

The policy statement also establishes standards for inter-system interfaces as a key priority. There is a need for a common semantic framework (a full agreement as to meaning) and software models for enabling effective communication and coordination across inter-system interfaces. An interface is any point where two systems must exchange understandable data, regardless of the inner workings of individual systems. FERC noted that IEC Standards 61970 and 61968 (together known as the Common Information Model) and IEC Standard 61850 (Communications Networks and Systems in Substations) could provide a basis for addressing such communication and coordination.

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0

It will take a suite of technologies to allow successful integration of diverse smart grid technologies. Under EISA, NIST has "primary responsibility to coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems. Such protocols and standards shall further align policy, business, and technology approaches in a manner that would enable all electric resources, including demand-side resources, to contribute to an efficient, reliable electricity network."[56]

NIST published in January 2010 Special Publication 1108 (SP1108)[57], its Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. SP1108 describes a high-level conceptual reference model for the smart grid, identifies 75 existing standards that are applicable (or likely to be applicable) to the ongoing development of the smart grid, specifies 15 high-priority gaps and harmonization issues (in addition to cyber security) for which new or revised standards and requirements are needed, documents action plans with aggressive time lines by which designated

---

[54] See http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf, Smart Grid Policy, 128 FERC ¶ 61,060, July 16, 2009.

[55] See http://www.nerc.com/page.php?cid=2|20.

[56] EISA Title XIII, Section 1305, 2007.

[57] http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf.

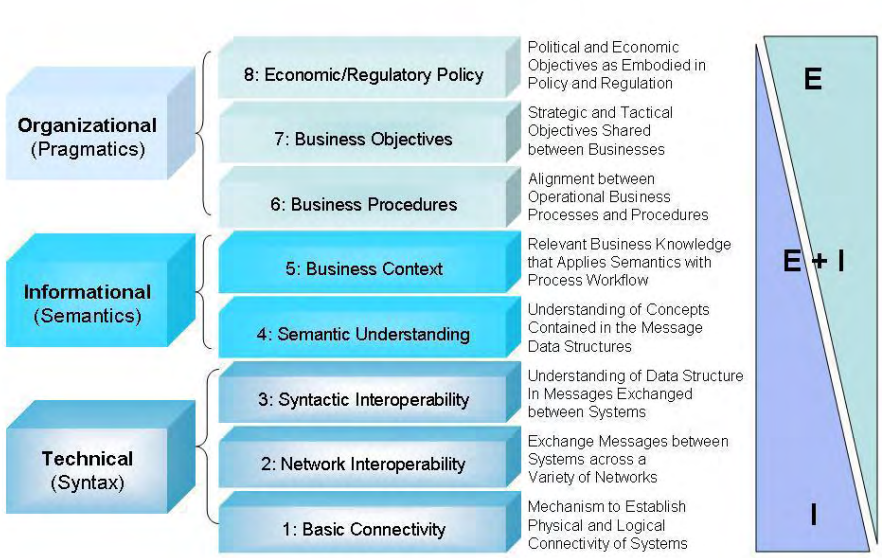
standards-setting organizations (SSOs) will address these gaps, and describes the strategy to establish requirements and standards to help ensure smart grid cyber security.

In addition, stakeholders identified gaps requiring entirely new standards to be developed. In all, a total of 70 such gaps or related issues were identified. Of these, NIST selected 15 for which resolution is most urgently needed to support one or more of the smart grid priority areas. The Priority Action Plans and targets for completion are as follows:

- Smart meter upgradeability standard (completed)
- Common specification for price and product definition (early 2010)
- Common scheduling mechanism for energy transactions (early 2010)
- Common information model for distribution grid management (year-end 2010)
- Standard DR signals (early 2010)
- Standards for energy use information (mid-2010)
- DNP3 Mapping to IEC 61850 Objects (2010)
- Harmonization of IEEE C37.118 with IEC 61850 and precision time synchronization (mid-2010)
- Transmission and distribution power systems models mapping (year-end 2010)
- Guidelines for use of IP protocol suite in the Smart Grid (mid-2010)
- Guidelines for use of wireless communications in the Smart Grid (mid 2010)
- Energy storage interconnection guidelines (mid-2010)
- Interoperability standards to support plug-in electric vehicles (year-end 2010)
- Standard meter data profiles (year-end 2010)
- Harmonize power line carrier standards for appliance communications in the home (year-end 2010)

Achieving cyber security requires incorporating security at the architectural level. To help visualize this problem and provide context for discussion, NIST used the GridWise Architecture Council's eight-layer stack.[58] This diagram provides a context for determining smart grid interoperability requirements and defining exchanges of information.

[58] From GridWise Interoperability Context-Setting Framework, GridWise Architecture Council, March, 2008.



NIST also identified 15 guiding principles for identifying and evaluating standards for implementation:

- Is well established and widely acknowledged as important to the smart grid
- Is an open, stable, and mature industry-level standard developed in consensus processes by a standards development organization (SDO)
- Enables the transition from the legacy power grid to the smart grid
- Has, or is expected to have, significant implementations, adoption, and use
- Is supported by an SDO or users group to ensure that it is regularly revised and improved to meet changing requirements and that there is strategy for continued relevance
- Is developed and adopted internationally, wherever practical
- Is integrated and harmonized, or there is a plan to integrate and harmonize it with complementing standards across the utility enterprise through the use of an industry architecture that documents key points of interoperability and interfaces
- Enables one or more of the framework characteristics as defined by EISA or enables one or more of the six chief characteristics of the envisioned smart grid
- Addresses, or is likely to address, anticipated smart grid requirements identified through the NIST workshops and other stakeholder engagement.
- Is applicable to one of the priority areas identified by FERC and NIST:
    - Demand Response and Consumer Energy Efficiency
    - Wide Area Situational Awareness
    - Electric Storage
    - Electric Transportation
    - Advanced Metering Infrastructure
    - Distribution Grid Management

    - Cyber Security
    - Network Communications
- Focuses on the semantic understanding layer of GWAC stack, which has been identified as most critical to smart grid interoperability
- Is openly available under fair, reasonable, and nondiscriminatory terms
- Has associated conformance tests, or a strategy for achieving said tests
- Accommodates legacy implementations
- Allows for additional functionality and innovation through the following:
    - Symmetry—facilitates bidirectional flows of energy and information
    - Transparency—supports a transparent and auditable chain of transactions
    - Composition—facilitates building of complex interfaces from simpler ones
    - Extensibility—enables adding new functions or modifying existing ones
    - Loose coupling—helps to create a flexible platform that can support valid bilateral and multilateral transactions without elaborate prearrangement*
    - Layered systems—separates functions, with each layer providing services to the layer above and receiving services from the layer below
    - Shallow integration—does not require detailed mutual information to interact with other managed or configured components

This process led to the identification of 25 primary standards and 50 additional standards.

NIST has worked with hundreds of participants to document use cases, assess risks, assess relevant standards, and develop a security architecture linked to the smart grid conceptual reference model. The results of these efforts have been published in NISTIR 7628.

NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements

The overall cyber security strategy for the smart grid comprises a mitigation strategy along with a response and recovery strategy, while helping to ensure interoperability of solutions across the entire infrastructure. A foundational part of a smart grid cyber security strategy is the definition of a cyber security risk assessment process. After conducting such a risk assessment, it is possible to knowledgeably select and tailor the security requirements.

Currently, only the NERC CIPs are mandatory for the bulk electric system. However, the following have been identified as having security requirements relevant to one or more aspects of the smart grid. The following standards are directly relevant to the smart grid:

- NERC CIP 002, 003-009
- IEEE 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
- Security Profile for Advanced Metering Infrastructure, v 1.0, Advanced Security Acceleration Project—Smart Grid, December 10, 2009
- UtilityAMI Home Area Network System Requirements Specification, 2008
- IEC 62351 1-8, Power System Control and Associated Communications—Data and Communication Security

The following documents are applicable to control systems:

- ANSI/ISA-99, Manufacturing and Control Systems Security, Part 1: Concepts, Models, and Terminology; and Part 2: Establishing a Manufacturing and Control Systems Security Program
- NIST Special Publication (SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems, August 2009
- NIST SP 800-82, DRAFT Guide to Industrial Control Systems (ICS) Security, September 2008
- Cyber Security Procurement Language for Control Systems, Version 1.8, Department of Homeland Security, National Cyber Security Division, February 2008
- Catalog of Control Systems Security: Recommendations for Standards Developers, Department of Homeland Security, 2009
- ISA SP100, Wireless Standards

Because of potential privacy risks associated with smart grid services, it is important to perform a privacy impact assessment.

The use cases, risk assessment, requirements, and privacy impact assessment should provide enough information to develop a security architecture. Given a security architecture, it will be possible to conduct a conformity assessment with the security requirements and determine if appropriate security can be accomplished.

Cyber Security Strategy. Cyber security must address not only deliberate attacks but also inadvertent compromises[59]. Additional risks include the following:

- Increasing the complexity of the grid could introduce vulnerabilities and increase exposure to potential attackers and unintentional errors.
- Interconnected networks can introduce common vulnerabilities.
- Increasing vulnerabilities to communication disruptions and malicious software could result in denial of service or compromise the integrity of software and systems.
- More entry points and paths offer more avenues for potential adversaries to exploit.
- Potential for compromise of data confidentiality, including the breach of consumer privacy, is increased.

Logical Architecture and Interfaces of the Smart Grid. The smart grid logical architecture includes several major domains: service providers, consumers, transmission, distribution, bulk generation, markets, and operations. A smart grid domain "is a high-level grouping of organizations, buildings, individuals, systems, devices, or other actors with similar objectives and relying on or participating in similar types of applications. Communications among actors in the same domain may have similar characteristics and requirements. Domains may contain subdomains. Moreover, domains have much overlapping functionality, as in the case of the transmission and distribution domains. An *actor* is a device, computer system, software program, or the individual or organization that participates in the smart grid. Actors have the capability to make decisions and to exchange information with other actors. Organizations

[59] Deliberate attacks might originate from disgruntled employees, industrial espionage, and terrorists. Inadvertent compromises might stem from user errors, equipment failures, and natural disasters.

may have actors in more than one domain." The functional logical architecture addresses all six application areas: electric transportation, electric storage, advanced metering infrastructure (AMI), wide area situational awareness (WASA), distribution grid management, and home area network/business area network (HAN/BAN) (formerly known as demand response, DR).

High-Level Security Requirements. There are similarities between security requirements for the smart grid information infrastructure and corporate information security requirements. The security requirements of back office and corporate systems can be identified through assessments similar to those described in Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. There are some differences. Specifically, power system operations of the smart grid are more closely aligned with Industrial Control Systems as described in NIST Special Publication (SP) 800-82, DRAFT Guide to Industrial Control Systems (ICS) Security.

One difference in security requirements relates to confidentiality, integrity, and availability. In general for corporate systems, the priority for the security objectives is confidentiality first, then integrity, followed by availability. For industrial control systems, including power systems, the priorities are availability first, integrity second, and then confidentiality. Even in that light, confidentiality is becoming more important, particularly with the increasing availability of consumer information online.

Recommended Security Requirements. There is no single set of cyber security requirements that addresses all of the smart grid logical interface categories. However, the information in the NERC CIPs, NIST SP 800-53, and the DHS Catalog forms a good starting point that can be augmented with material from NIST SP 800-82 and NIST SP 800-63. It is possible to group the security requirements into categories of Common Governance Risk and Compliance (GRC), Common Technical, and Unique Technical. Table 3.4 in NISTIR 7628 provides proposed cyber security requirements that support the priorities of availability and integrity.

Privacy. The ability to access, analyze, and respond to increasingly precise and detailed data from all levels of the electric grid is critical to achieving the major benefits of the smart grid, however, it is also a significant concern from a privacy viewpoint, especially when these data, and data extrapolations, are associated with individual consumers or locations. The privacy risks presented by smart appliances and devices on the consumer side of the meter are expanded when these appliances and devices transmit data outside of the HAN or building management system and do not have documented security requirements, effectively extending the perimeter of the system beyond the walls of the premises. Data may also be collected from electric vehicles and plug-in hybrid electric vehicles (EVs/PHEVs). Charging data may be used to track the travel times and locations for the EV/PHEV owners.

The following questions were identified and addressed in the process of performing a privacy impact assessment in July and August 2009:

- What personal information may be generated, stored, transmitted, or maintained by the smart grid?
- How is this information new or unique from personal information in other types of systems and networks?
- What are the new and unique types of privacy risks that may be created by smart grid components and entities throughout the grid network?

- Do existing laws, regulations, and standards apply to the personal information collected by, created within, and flowing through the smart grid components?
- What could suggested privacy practices look like for all entities using the smart grid so that following them would protect privacy, reduce risks, and support and/or enhance existing laws, regulations, and standards?

Potential privacy concerns include:

- Fraud—such as attributing energy consumption to another location or vehicle
- Determining personal behavior patterns and/or appliances used—this data may be of high value to appliance manufacturers, marketing firms, and burglars
- Performing real-time remote surveillance—access to live data can reveal whether people are home and what they may be doing
- Non-Grid commercial uses of data—Large amounts of data can reveal private lifestyle information to marketers, vendors, and others

Standards. The current NIST information on smart grid interoperability standards is embedded in NIST SP1108, *Framework and Roadmap for Smart Grid Interoperability Standards*. This guidance will continue to evolve. The information in Section 5 of NISTIR 7628 (February 2010) is slightly more recent than the information in NIST SP1108 (January 2010), and NIST SP1108 will updated again soon. The list includes standards documents, DHS catalog security families, security by OSI layer, and more.

System-level Topics. Modern distribution grids are built to withstand some level of tampering to meters and other systems that cannot be physically secured, as well as some degree of invalid or falsified data from HANs. The increased dependence in the smart grid on information and distributed and networked information management systems in SCADA, WAMS, and PLCs implies the smart grid will need much more than device authentication, encryption, failover, and models of normal and anomalous behavior, all of which are problems on their own given the scale and timeliness requirement of the smart grid. The smart grid is a long-term and expensive resource. Research is clearly needed to develop an advanced protection architecture that is dynamic (can evolve) and focuses on resiliency (tolerating failures, perhaps of a significant subset of constituents).

Research challenges include:

- Architecting for bounded recovery and reaction
- Architecting real-time security
- Calibrating assurance and timeliness trade-offs
- Legacy system integration
- Resiliency management and decision support
- Efficient composition of mechanisms
- Risk assessment and management, including advanced attack analysis, measuring risk, and risk-based cyber security investment
- Other security issues
    - Privacy and access control in federated systems
        - Managed separation of business entities

        - Authentication and access control in a highly dynamic federated environment
    - Auditing and accountability
    - Infrastructure interdependency issues
    - Cross-domain (power/electrical to cyber/digital) security event detection, analysis, and response

Use Cases

The following use cases can be considered to have key security requirements that may vary in vulnerabilities and impacts, depending on the actual systems, but that nonetheless can be generally assessed as having integrity, availability, and confidentiality (IAC).

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

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

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

- 4 milliseconds for protective relaying
- Subseconds for transmission wide-area situational awareness monitoring
- Seconds for substation and feeder SCADA data
- Minutes for monitoring noncritical equipment and some market pricing information
- Hours for meter reading and longer-term market pricing information
- Days/weeks/months for collecting long-term data such as power quality information

Confidentiality is generally the least critical security requirement for actual power system operations, although this is changing for some parts of the power system, as consumer information is more easily available in cyber form:

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

Critical Issues for the Security Requirements of Power Systems—The automation and control systems for power system operations differ in many regards from most business or corporate systems. Some particularly critical issues related to security requirements include the following:

- Operation of the power system must continue 24/7 with high availability (for example, 99.99 percent for SCADA and higher for protective relaying) regardless of any compromise in security or the implementation of security measures that hinder normal or emergency power system operations.
- Power system operations must be able to continue during any security attack or compromise (as much as possible).

- Power system operations must recover quickly after a security attack or compromised information system.
- The complex and manifold interfaces and interactions across this largest machine of the world—the power system—makes security particularly difficult since it is not easy to separate the automation and control systems into distinct security domains. And yet end-to-end security is critical.
- There is not a one-size-fits-all set of security practices for any particular system or for any particular power system environment.
- Testing of security measures cannot be allowed to impact power system operations.
- Balance is needed between security measures and power system operational requirements. Absolute security is never perfectly achievable, so the costs and impacts on functionality of implementing security measures must be weighed against the possible impacts from security breaches.
- The risk and the cost of implementing the security measures must be balanced.

Security Programs and Management—Development of security programs is critical to all use cases. These programs include the following:

- Risk assessment to develop security requirements based on business rationale (for example, impacts from security breaches of IAC) and system vulnerabilities.
    - The likelihood of particular threat agents, which are usually included in risk assessments, should play only a minor role in the overall risk assessment since the power system is so large and interconnected that appreciating the risk of these threat agents would be very difficult.
    - However, in detailed risk assessments of specific assets and systems, some appreciation of threat agent probabilities is necessary to ensure that an appropriate balance between security and operability is maintained.
- Security technologies that are needed to meet the security requirements:
    - Plan the system designs and technologies to embed the security from the start.
    - Implement the security protocols.
    - Add physical security measures.
    - Implement the security monitoring and alarming tools.
    - Establish Role-Based Access Control to authorize and authenticate users, both human and cyber, for all activities, including password/access management, certificate and key management, and revocation management.
    - Provide the security applications for managing the security measures.
- Security policies, training, and enforcement to focus on the human side of security, including the following:
    - Normal operations
    - Emergency operations when faced with a possible or actual security attack
    - Recovery procedures after an attack
    - Documentation of all anomalies for later analysis and reassessment of risk

- Conformance testing for both humans and systems to verify they are using the security measures and tools appropriately and not bypassing them:
    - Care must be taken not to impact operations during such testing.
    - If certain security measures actually impact power system operations, the balance between that impact and the impact of a security compromise should be evaluated.
- Periodic reassessment of security risks

There is a cross-walk of cyber-security documents in Appendix B. The documents are NIST SP800-53, NIST SP800-82, DHS Catalog of Control Security Requirements, and NERC CIPs.

Appendix C provides a discussion of vulnerability classes. Sources of vulnerability information include NIST 800-82 and 800-53, OWASP vulnerabilities, CWE vulnerabilities, attack documentation from INL, input provided by the NIST SGIP-CSWG Bottoms-Up group, and the NERC CIP standards.

Appendix D provides a bottom-up security analysis of the smart grid. Big issues discussed are authenticating and authorizing people and devices to each other, securing serial communications, securing dial-up access, access logs, key management, insecure firmware updates, side-channel attacks, securing and validating device settings, absolute and accurate time information, and certificates.

A Systems View of the Modern Grid, Resists Attack, v2.0, Appendix A3, Resists Attack

Here are some of the requirements that need to be met to move forward.

SYSTEM REQUIREMENTS

The systems approach to electric power security would identify key vulnerabilities, assess the likelihood of threats, and determine the consequences of an attack. The designers of the modern electrical grid can draw on the extensive experience of the Department of Defense in assessing threats and system vulnerabilities.

This approach would apply risk management methods to prioritize the allocation of resources for security, including R&D. Particular goals of security programs would include:

- Identification of critical sites and systems
- Protection of selected sites using surveillance and barriers against physical attack
- Protection of systems against cyber attack using information denial (masking)
- Dispersion of sites that are high-value targets
- Ability to tolerate a disruption (self-healing characteristics)
- Integration of distributed energy sources and use of automated distribution to speed recovery from attack

Resilience must be built into each element of the system, and the overall system must be designed to deter, detect, respond, and recover from man-made disruptions.

For the modern grid to resist attack, it must reduce:

- The threat of attack by concealing, dispersing, eliminating, or reducing single-point failures

- The vulnerability of the grid to attack by protecting key assets from physical and cyber attack
- The consequences of a successful attack by focusing resources on recovery

Therefore, its system requirements must include those that:

- Implement self-healing capabilities
- Enable “islanding” (the autonomous operation of selected grid elements)
- Provide greater automation, wide area monitoring, and remote control of electric distribution systems
- Acquire and position spares for key assets
- Use distributed energy resources
- Ensure that added equipment and control systems do not create additional opportunities for attack
- Rapidly respond to impending disruptions with the aid of predictive models and decision support tools

APPENDIX D: NERC CIP SECURITY REQUIREMENTS

The following are the cyber security requirements and measures from the NERC CIPs.

- CIP-001-1a – Sabotage Reporting
    - R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.
    - R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.
    - R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.
    - R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.
    - M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1.
    - M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3.
    - M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or RCMP officials to communicate sabotage events (Requirement 4).
- CIP-002-3 – Critical Cyber Asset Identification
    - R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

- R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
- R1.2. The risk-based assessment shall consider the following assets:
  - R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.
  - R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.
  - R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.
  - R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.
  - R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.
  - R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.
  - R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

- R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.
- R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
  - R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
  - R3.2. The Cyber Asset uses a routable protocol within a control center; or,
  - R3.3. The Cyber Asset is dial-up accessible.
- R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and

the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

- M1. The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.
- M2. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R2.
- M3. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R3.
- M4. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R4.

- CIP-003-3 – Security Management Controls
  - R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:
    - R1.1. The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.
    - R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
    - R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.
  - R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3.
    - R2.1. The senior manager shall be identified by name, title, and date of designation.
    - R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.
    - R2.3. Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.
    - R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.
  - R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

        - R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).
        - R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.
        - R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.
    - R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
        - R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
        - R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
        - R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.
    - R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
        - R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
            - R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.
            - R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.
            - R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

- R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

- R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.
- M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.
- M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.
- M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.
- M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.
- M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.
- M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

- CIP-004-3 – Personnel and Training
  - R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:
    - Direct communications (e.g. emails, memos, computer based training, etc.);
    - Indirect communications (e.g. posters, intranet, brochures, etc.);
    - Management support and reinforcement (e.g., presentations, meetings, etc.).
  - R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.
    - R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are

trained prior to their being granted such access except in specified circumstances such as an emergency.

- R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:
  - R2.2.1. The proper use of Critical Cyber Assets;
  - R2.2.2. Physical and electronic access controls to Critical Cyber Assets;
  - R2.2.3. The proper handling of Critical Cyber Asset information; and,
  - R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.
- R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

- R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:
  - R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.
  - R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.
  - R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-3.
- R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

        - R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.
        - R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.
    - M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.
    - M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.
    - M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.
    - M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.
- CIP-005-3 – Electronic Security Perimeters
    - R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
        - R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
        - R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.
        - R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
        - R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.
        - R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective

measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

- R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

- R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
  - R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
  - R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
  - R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
  - R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
  - R2.5. The required documentation shall, at least, identify and describe:
    - R2.5.1. The processes for access request and authorization.
    - R2.5.2. The authentication methods.
    - R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.
    - R2.5.4. The controls used to secure dial-up accessible connections.
  - R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.
- R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

- R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.
- R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

- R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
  - R4.1. A document identifying the vulnerability assessment process;
  - R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
  - R4.3. The discovery of all access points to the Electronic Security Perimeter;
  - R4.4. A review of controls for default accounts, passwords, and network management community strings;
  - R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.
- R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.
  - R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.
  - R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
  - R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.
- M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.
- M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

    - M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.
    - M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.
    - M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.
- CIP-006-3 – Physical Security of Critical Cyber Assets
    - R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
        - R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.
        - R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.
        - R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).
        - R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
        - R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
        - R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
            - R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.
            - R1.6.2. Continuous escorted access within the Physical Security Perimeter.
        - R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.
        - R1.8. Annual review of the physical security plan.
    - R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at

the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

- R2.1. Be protected from unauthorized physical access.
- R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

- R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.
- R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
  - Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
  - Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
  - Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
  - Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
- R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:
  - Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
  - Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.
- R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access

points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

- R7. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.
- R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:
  - R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.
  - R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.
  - R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.
- M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.
- M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.
- M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.
- M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.
- M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.
- M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.
- M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.
- M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

- CIP-007-3, Systems Security Management
    - R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
        - R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.
        - R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.
        - R1.3. The Responsible Entity shall document test results.
    - R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
        - R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
        - R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
        - R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
    - R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
        - R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
        - R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
    - R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

        - R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
        - R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.
    - R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
        - R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
            - R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.
            - R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.
            - R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.
        - R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
            - R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.
            - R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.
            - R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

        - R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:
            - R5.3.1. Each password shall be a minimum of six characters.
            - R5.3.2. Each password shall consist of a combination of alpha, numeric, and “special” characters.
            - R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.
    - R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
        - R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
        - R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
        - R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.
        - R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
        - R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.
    - R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.
        - R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
        - R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
        - R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.
    - R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
        - R8.1. A document identifying the vulnerability assessment process;

        - R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;
        - R8.3. A review of controls for default accounts; and,
        - R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.
    - R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.
    - M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.
    - M2. The Responsible Entity shall make available documentation as specified in Requirement R2.
    - M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.
    - M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.
    - M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.
    - M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.
    - M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.
    - M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.
    - M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.
- CIP-008-3, Incident Reporting and Response Planning
    - R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:
        - R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.
        - R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

        - R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.
        - R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.
        - R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.
        - R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.
    - R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.
    - M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.
    - M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.
- CIP-009-3, Recovery Plans for Critical Cyber Assets
    - R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:
        - R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).
        - R1.2. Define the roles and responsibilities of responders.
    - R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.
    - R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.
    - R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

- R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.
- M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.
- M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.
- M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.
- M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.
- M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

APPENDIX E: INTEROPERABILITY AND CYBER SECURITY

The following is a relevant portion of the DOE Request for Proposal:

Interoperability and Cyber Security

One of DOE's top smart grid priorities is the work with NIST and FERC on a framework for interoperability standards. This effort is focused on an accelerated timetable for the development of a standards development roadmap and a process for getting standards for interoperability in place as rapidly as possible. As the smart grid develops and the grid becomes more interconnected, the Nation needs to guard against introducing cyber related vulnerabilities that would allow for disruption of the grid. This could occur, at least in theory, either through unintended pathways from the Internet or less secure customer networks into the infrastructure control systems or through the ability of malicious actors to manipulate large numbers of small systems that would affect the load on the grid and thus destabilize grid operations. As smart grid technologies are placed into operation, careful consideration should be given to how these components affect the security of the grid as a whole by avoiding unnecessary connectivity or functionality or by providing by appropriately secured, authenticated activity while still allowing for the sharing of information necessary to enable innovation and cost savings. Particular care is required where different networks of varying security levels converge to share information, whether it is a utility interface to the home (e.g. smart meters) or a server belonging to a utility or a third-party service provider.

In addition to NIST and FERC, DOE is working on this activity with many other private organizations including the North American Electric Reliability Corporation, the Institute of Electrical and Electronic Engineers, the National Electrical Manufacturers Association, and the GridWise Architecture Council.

Interoperability

All applications shall include a section on the technical approach to addressing interoperability with respect to the integration of smart grid devices covering the application of procedures and practices involving interface identification, specification, testing, and lifecycle management. The technical approach to addressing interoperability should include:

- A summary of the information exchange interfaces for communicating automation devices and systems (i.e., their points of connection with other elements of the system)
- A summary of how the project will provide openly available and proprietary aspects of the interface specifications, and how existing (legacy) communicating devices or systems will be integrated into the project
- A summary of how the project will address response to failure and device upgrade scenarios, such that overall system impact is mitigated
- A summary of how the project will support compatibility with NIST's emerging smart grid framework for standards and protocols
- In addition, the Applicant, should further detail:
    - The information exchange interface points for each type of communicating automation device and system.
    - The openly-available and proprietary aspects of the interface specifications.
    - Where a type of communicating device or system is expected in large numbers (e.g., meters, sensors, customer interfaces), the extent of support for multiple suppliers who will integrate their devices or systems that may be based on different technologies at the points of interface.
    - If existing (legacy) communicating devices or systems are integrated into the project, the extent to which they integrate and interoperate at the points of interface with new components.

- The interacting parties' anticipated response to failure scenarios, particularly loss of communications, such that overall system impact is mitigated in the event of such failure.
- The anticipated process for upgrading devices or systems (hardware and software) so that overall system operation impact is mitigated.
- The evidence that will be provided (interface specifications, interoperability test plans and results, reviews, and other engineering artifacts) to ensure interoperability at the interfaces of communicating automation devices and systems.
- The project's ability to support compatibility with NIST's emerging smart grid framework for standards and protocols as information becomes available.

Cyber Security

Applicants must provide clear documentation that demonstrates that their proposed approach to cyber security will prevent broad based systemic failures in the electric grid in the event of a cyber security breach.

All applications shall include a section on the technical approach to cyber security. Cyber security should be addressed in every phase of the engineering lifecycle of the project, including design and procurement, installation and commissioning, and the ability to provide ongoing maintenance and support. Cyber security solutions should be comprehensive and capable of being extended or upgraded in response to changes to the threat or technological environment. The technical approach to cyber security should include:

- A summary of the cyber security risks and how they will be mitigated at each stage of the lifecycle (focusing on vulnerabilities and impact)
- A summary of the cyber security criteria utilized for vendor and device selection
- A summary of the relevant cyber security standards and/or best practices that will be followed
- A summary of how the project will support emerging smart grid cyber security standards
- In addition, the Applicant, should further detail:
  - The methodology used to identify cyber security risks and the results of this assessment (e.g., the assessment should consider the mission of the new smart grid project and also potential impacts to other critical grid control functions to which they are connected).
  - How cyber security risks will be mitigated at each phase of the engineering lifecycle, including policy, procedural, and technical (logical and physical) controls, with special emphasis on strategies for:
    - ensuring the confidentiality, integrity, and availability of device and system data and communications commensurate with the application requirements,
    - securing, logging, monitoring, alarming, and notification, and
    - applications where logical and physical security may not be under the direct jurisdiction of the installing entity.
  - The relevant cyber security standards or best practices that will be used.
  - The capability of the components or system to be updated to meet future cyber security requirements or technologies.
  - How evidence will be provided (e.g., a test plan, engineering artifacts, independent testing and review) to demonstrate and validate the effectiveness of the cyber security controls

The following is a relevant portion of the NRECA proposal:

Adequacy and completeness of approach to address interoperability, including the description of the automation component interfaces (devices and systems), how integration is supported to achieve interoperability, and how interoperability concerns will be addressed throughout all phases of the engineering lifecycle, including design, acquisition, implementation, integration, test, deployment, operations, maintenance, and upgrade.

NRECA is the developer and "owner" of the MultiSpeak protocol, the most widely deployed protocol for utility control. NRECA is fully committed to keeping MultiSpeak compliant and consistent with emerging standards at the National Institute of Standards and Technology (NIST) and the Institute of Electrical and Electronics Engineers (IEEE). This will extend to all code and/or specifications developed in the course of this project.

Originated by NRECA, the MultiSpeak® Initiative is a collaboration of leading software providers supplying the utility market, and utilities. The Initiative has developed and continues to expand with a specification that defines standardized interfaces among software applications commonly used by electric utilities. The MultiSpeak specification thus helps vendors and utilities develop interfaces so that software products from different suppliers can interoperate without requiring the development of extensive custom interfaces.

Originally targeted at small electric utilities and covering a limited number of back-office applications, the effort has expanded to where it now offers significant guidance for a range of applications to utilities of all sizes, primarily those that supply electricity, but increasingly for those that supply water and gas services as well.

The MultiSpeak specification defines what data need to be exchanged between software applications in order to support the business processes commonly applied at utilities. In order to accomplish this, it makes use of three components:

- *Definitions of common data semantics.* Data semantics are an agreement about a specific item used in a business process, say a customer or a service outage, which might be exchanged in the context of the outage management business process. Data semantics are documented in the form of an extensible markup language (XML) schema.
- *Definitions of message structure.* Once an agreement has been reached on what data need to be exchanged, it is necessary to define message structures to support the required data interchanges. In MultiSpeak, the XML-formatted data payload is carried as part of a Web services call for real-time exchanges and as part of a batch file for offline transfers.
- *Definition of which messages are required to support specific business process steps.* Web services method calls are linked together to accomplish each potential step in a utility business process. Such steps can then be strung together to support complete business processes.

Real-time MultiSpeak interfaces use Web services to define and implement the data transport. Each Web service consists of one or more methods. MultiSpeak uses Web services description language (WSDL) files to document the methods and define which messages are required to achieve the goals of each method.

Adequacy and completeness of approach for cyber security concerns and protections and how they will be addressed throughout the project, including the adequacy of the discussion of the integration of the new smart grid application into the existing environment, and how any new cyber security vulnerabilities will be mitigated through technology or other measures.

The NRECA team recognizes the importance of cyber security in Smart Grid development. The Smart Grid integrates information systems with utility operations, which opens doors to potential attacks. We must address this issue in the development of the MultiSpeak extensions, the software for end-to-end connectivity, and in the integration of the deployed components into utility operations.

To address this we have engaged a leading software developer (SAIC) and directed that the developer include security specialists on the team. We have also engaged Cigital, the premier software security company in an IV&V (independent validation and verification) and audit function. We address the qualification of the team in a later section and through the individuals' biographies. Here we discuss our approach to security through the software development lifecycle.

Addressing cyber security risk requires a holistic and systematic approach involving cyber security as a key element in all aspects of the project, from planning to requirements specification, architecture, acquisition, design, implementation, integration, testing, deployment, operations, maintenance—all the way through decommissioning. The NRECA team will address cyber security concerns during project planning and kickoff; will incorporate cyber security risk assessment and mitigation activities throughout the development lifecycle of the project; and will develop policies and guidance for cyber security activities to be applied during the full operational, maintenance and decommissioning phases of the delivered system's lifecycle.

From a security perspective, each stage of the development lifecycle comprises the following three elements:

- Security Assessment (Threat Modeling and Controls Selection)
- Security Controls Design/Implementation
- Security Assessment (Security Test and Evaluation)

Further, the following security principles will be considered as security controls and mechanisms are built into the project:

- Holistic (for example, physical, network, software, people)
- Compartmentalization (plan for failure)
- Defense in Depth (security must be multi-layered)
- Secure the Weakest Link
- Protect, Detect, Respond (controls must be multi-faceted)

Security Assessment Methodology

The iterative security assessment methodology to be applied by the NRECA team involves a wide range of activities but is comprised of the following two primary phases:

- Threat Modeling and Control Selection
- Security Test and Evaluation

Threat Modeling and Control Selection considers a system from the point of view of an adversary and the types of attacks to which a skilled attacker may subject a system. During this phase, the goals of an attacker are considered in terms of the system's assets that an attacker may try to compromise. For that purpose, the system's assets and the attack surface (for example, system entry points) are enumerated. Attack patterns are then systematically documented that may enable an attacker to compromise the confidentiality, integrity, or availability of various system assets. In this light, appropriate risk activity rigors and compliance considerations as well as the effectiveness of controls to protect the assets of the system are considered and possible weaknesses are noted. This process is initially used to help identify relevant controls.

Risk-based Controls. Fundamentally, risk-based controls rely on empirical evidence to support the notion that the failure to implement a specific control in the target environment will result in an impact of some likelihood. Such empirical evidence is usually obtained from exhaustive testing and simulation exercises that emulate all possible threats. However, because such exercises are time-consuming and contain an almost limitless set of control variations and permutations, targeted testing is usually deployed to address controls unique to the environment and supplemented by industry best practices and standards, legal and regulatory frameworks, and the expertise and experience of the team members.

Compliance-based Controls. While generally demonstrating significant overlap with risk-based controls, these controls are selected specifically because a law, regulation, or industry standard requires the control to be implemented. In some cases, a deviation may be allowed based on the feasibility of implementing the control and the potential risk of not implementing the control. However, such exceptions are just that. Among the compliance-based controls that will be evaluated against the selected controls in whole or in part include: NERC CIP, NIST SP 800-53, ISO 27001, AMI-SEC, and ISA SP 99. As many of these standards and regulations are still evolving, the NRECA team will continue to monitor their evolution. NRECA team members are currently part of a NIST team that is helping to define cyber security requirements for Smart Grid. Our members are also active participants with AMI-SEC and ISA SP 99 working groups.

Security Test and Evaluation is also an iterative process that verifies the existence and effectiveness of security controls from a risk and compliance perspective. All portions of the process are deployed during the design, implementation, and operational stages of the lifecycle. During each phase the test and evaluation process asks:

- Are the security controls that are being designed or implemented sufficient to protect the system from the attack patterns that have been identified?
- What in the system's design or implementation open up new attack vectors for an adversary? How do we address these?

This process will begin by the development of a test plan that will highlight the tests to be performed, a reference to the expected results, and the logistics for carrying out the test. To help answer the questions above, the testing and evaluation conducted will comprise the following activities in order:

Documentation and Design Review. This activity ensures that policies, procedures, plans, and schematics sufficiently identify all security controls. During the early stages of the development lifecycle, this activity focuses on the initial design and concept of operations and may include facilitated sessions where developers and system integrators offer up proposed designs, including security controls; the assessment team then compares the designs against the controls selected. During later stages, the review ensures that the documentation is complete from both a risk and compliance perspective.

Interviews. The interview activity will largely focus on individuals tasked with performing security-related activities during the operation stage. However, it also inquires as to whether developers are developing code securely and integrators are aware of and deploying the required controls correctly.

Observation and Inspection. This activity generally applies to physical controls in place for the facilities and components of the system proposed. This may include determining whether meters are implementing tamper proofing and tamper alerting mechanisms, whether computer systems are secured in restricted areas, and whether heat and cooling mechanisms are operating appropriately. For the most part, this task can be done after assuming that the environment planned for production does not change.

Configuration and Code Analysis. This exercise examines configuration settings of devices used for the project including meters, collectors, head end systems (user interfaces), and meter data management systems and compares those settings to what the team views as best practices or necessary to meet compliance requirements. For commercial off-the-shelf (COTS) products, it is understood that code review may not be possible. In that case, the team will analyze

configuration settings and rely on other technical tests such as vulnerability scans and penetration tests to accomplish the objectives.

Vulnerability Scanning. As part of the testing process, a variety of vulnerability scanning tools will be leveraged to identify potential vulnerabilities in the network and the applications. In many cases, the proprietary nature of Smart Grid components means that standard vulnerability scanning tools will be of limited use. Consequently, the team will draw on penetration testing, configuration analysis, and design reviews to properly identify potential and actual vulnerabilities.

Penetration Testing. Penetration testing performed here uses a combination of manual and automated techniques and is in many respects similar to the pre-deployment penetration tests performed during the development lifecycle. Penetration testing on the Smart Grid will focus on the physical, network, software, as well as people, aspects of security. A combination of technical attacks leveraging information obtained through social engineering techniques are all considered in the work scope. At the end of the day, it is imperative to not underestimate the adversary, taking into consideration a highly skilled, resourceful, and motivated attackers who will use all means at their disposal to attack critical infrastructures of the Smart Grid.

Security Controls Design/Implementation

If the controls selection and assessment process is deployed correctly, the security design and implementation process should be very simple. NRECA will draw upon the guidance provided and include the cyber security professionals in design and implementation, thereby avoiding the common problem of having the cyber security personnel being brought in too late after architectures are set in stone and cannot be changed without significant expense and delay.

APPENDIX F: LEXICON

Activity	An activity is a specific, independent element of work defined by a specific technology, study objective, and cooperative. An example is to install a SCADA system at a particular participant. Activities are tightly defined, relatively short in duration, and occur within one cooperative only and within one subproject only. There will be approximately 100 activities spanning the four subprojects.
Categories of Activities	There are three categories of activities—distributed automation, demand response, and other. There are several types of activities within each category. The "other" activities generally relate to efforts necessary to prepare for a study-related activity. An example is improvements to communications infrastructure.
Charter	A narrative defining the role of a team. This is prepared and maintained by the team, in coordination with the Management Team.
Contract	In the context of the project a "contract" is a contractual agreement between the DOE and NRECA for work to be completed in a phase. We anticipate that there will be only two contracts in the course of the project, for Phase I and Phase II.
Deliverable	A deliverable is a product that is conveyed to DOE. Deliverables are designated in the SOPO.
ICSP	The ICSP is the Interoperability and Cyber-Security Plan. This plan describes how the project will meet the DOE objective of advancing the interoperability of smart grid components and ensuring the security of the grid from disruption through electronic attack or attack on control components. The ICSP is one of the three Phase I deliverables.
NEPA Filing	The NEPA filing is the required assessment of the environmental impact of the activities. The NEPA filing is one of the three Phase I deliverables.
Phase	One of two major blocks of work which, together, comprise the project.
Phase I	The first phase of work; primarily involves planning. This phase has three deliverables: the Project Management Plan, the NEPA Compliance Filing, and the Interoperability and Cyber-Security Plan (ICSP).

Phase II	The second phase of work, including all of the purchasing, preparation, installation, configuration, integration and operation of hardware and software, the research studies, communications, and outreach.
PMP	The Project Management Plan, a detailed work plan that enumerates all of the tasks that must be completed to comply with the Phase II SOPO (Statement of Project Objectives). The PMP includes labor loading, budget, schedule, risks, mitigation strategies, deliverables, and milestones. The PMP is one of the Phase I deliverables. The PMP must be approved by DOE before we can proceed with subsequent tasks, including procurement.
Product	A product is a specific document, piece of software, account of work done, or other work product identified in the PMP. Most products are internal to the project—that is, not shared outside the project team and participants.
Program	Obsolete term, replaced with "activity."
Project	The entirety of the activities undertaken under the DOE Stimulus Grant.
Replanning Exercise	The exercise after each subproject during with we evaluate the work to date, improve our team and our approach, and update the plan for subsequent subprojects. All aspects of the project work may be examined.
SOPO	The Statement of Project Objectives is a high-level summary of the technical requirements of a contract between DOE and NRECA. There are specific SOPOs for Phase I and Phase II. The Phase I SOPO was prepared by DOE and became part of the Phase I contract. The Phase II SOPO will be completed during Phase II.
Statement of Work	A statement of work refers to the agreement between NRECA and a team or a subcontractor.
Subcontract	A subcontract is a contractual agreement between NRECA and individuals, companies, and other organizations to provide specific work in support of the contract.
Subcontractor	Recipient of a subcontract.
Subproject	Installation, configuration, integration, and operation of equipment, software, and systems will be done in four sequential subprojects. The term *subproject* is synonymous with *tranche*.

Swim lane	A swim lane is a collection of tasks related by a common objective or skills required. Swim lanes are established to define groups of tasks that are largely independent of one another, helping teams to understand what is in their scope and what is not.
Task	A task is the smallest element of the project management plan (PMP). Activities are accomplished through a number of tasks. Each task has a designated responsible team, though tasks may involve the work of multiple teams.
Team	The individuals working on the project are organized into teams. Each team has a specific role (charter) and statement of work.
Tranche	Obsolete term replaced with *subproject.*
Type of Activity	The activities will be grouped, for purposes of reporting and analysis, based on similar technologies and research objectives. Some activities will match the activities described in our proposal and reflected in the Statement of Project Objectives (SOPO).