Austin Energy ADMS-SCADA RFP

Specifications

December 2011

Table of Contents

0. Introduction to ADMS-SCADA Technical Requirements 1
0.1 Project Context 1
0.2 Proposal Objectives 1
0.3 Infrastructure Overview 2
0.4 Organization of the Specification 4

0. Introduction to ADMS-SCADA Technical Requirements

0.1 Project Context

R[1] Austin Energy (AE) is the municipal electric utility of the City of Austin, Texas. AE is the nation's 9th largest community-owned electric utility and is engaged in the generation, transmission, and distribution of electrical services to a service territory of 421 square miles with over 410,000 customers in Travis County and portions of Williamson County.

R[2] AE has approximately 10,000 miles of power lines, over 140,000 utility poles, 40,000 transformers plus many other assets modeled in a GE Smallworld GIS.

0.2 Proposal Objectives

R[1] AE is seeking responses for a firm fixed price proposal to procure software, implementation, and commissioning services from qualified vendors for an Advanced Distribution Management System with SCADA (ADMS-SCADA).

R[2] AE defines the ADMS-SCADA as a single integrated system that shares a common database and performs traditional DMS functions, newer/advanced applications, Outage Management functions and traditional EMS or SCADA functions. The ADMS-SCADA will be capable of continued operations during maintenance or data base upgrading of non-related areas of the system. The Outage Management functions will have an interface to the existing AE SCADA/EMS ABB Network Manager Release 4 (NMR4) to allow for coordination of transmission and distribution system operators.

R[3] AE desires a contract with a single Proposer that can provide a turnkey solution—one that has a strong history of successful implementations of the proposed system.

R[4] AE prefers to minimize customizations to the implemented system.

R[5] Within reason, AE will adjust its processes to align with the proposed solution.

R[6] The AE project team shall use this document as a guideline for evaluating the Proposers' total business solution. If a proposed software solution does not perform a task described in this document, then the Proposer shall describe how the proposed solution will meet the task requirements through alternative means.

0.3 Infrastructure Overview

R[1] The elements below provide an overview of AE infrastructure relevant to the ADMS-SCADA project.

R[2] Details regarding most of these elements are provided within the sections of the document.

R[3] If there are discrepancies, the detailed section descriptions shall be used.

SUBSTATION EQUIPMENT

R[1] AE has 73 distribution substations with approximately 500 feeders (including spare and dedicated feeds).

R[2] Many of the feeder breakers have solid-state relays that support fault magnitude measurements and analogs per phase.

R[3] AE will be installing a Lindsey line monitor when deploying DA (Distribution Automation) equipment where the feeder does not have the analog and fault current data per phase to support the advanced applications.

REMOTE DEVICES AND COMMUNICATION

R[1] AE currently has 67 DA devices including 40 remotely controlled gang operated air-switches, 10 remotely controlled capacitor banks, 24 remotely controlled reclosers and 4 Lindsey line monitoring devices.

R[2] The DA field devices communicate using the Landis+Gyr mesh radio network.

R[3] The L+G mesh radio network uses a proprietary protocol and interfaces with the Intelligent Communication Gateway (ICG) product by DC Systems hosted locally on AE servers.

R[4] The OMS/DMS will poll the ICG using standard DNP (Distributed Network Protocol) protocols for all DA device communication and control.

R[4.A] Note: With technology advancements, other devices have taken on functions traditionally performed by an RTU. For the purposes of this report, AE will use the term RTU to also include this expanded group of devices.

SECURITY AND NETWORK

R[1] To protect its internal network, AE utilizes a variety of firewall technologies, intrusion detection, and anti-virus software and application white listing to meet NERC requirements and follow industry best practices.

R[2] Client network capacity is currently limited to 100 megabits per second.

OTHER RELATED PROJECT APPLICATIONS

R[1] The list below is not comprehensive, but highlights some of the applications and tools that will integrate with the ADMS-SCADA.

R[2] The ADMS-SCADA shall be designed to exchange data with external systems, AE applications, and other systems on the AE Corporate Network.

R[3] These systems are listed below. Refer to Section 13.5 for ADMS-SCADA external interface details. External interfaces:

R[3.A] GoalArt Alarm and Event processesor or equivalent.

R[3.B] iFactor Storm Center

R[3.C] Ecologic Meter Data Management System (MDMS)

R[3.D] ICCP data to and from other systems

R[3.E] Data Concentrators (Intelligent Communication Gateway (ICG), etc.)

R[3.F] IBM Websphere Process Server

R[3.G] GE Smallworld GIS

R[3.H] GE Electric Office GIS

R[3.I] Oracle Customer Care and Billing (CC&B) CIS

R[3.J] Automated meters (AMI) will be interfaced directly with Landis + Gyr or the local Ecologic Meter Data Management System (MDMS) for power out, power up reporting and pinging.

R[3.K] AECall – an internally developed corporate trouble call recording application

R[3.L] 21st Century High Volume calling system – an externally hosted automated call answering service

R[3.M] iFactor Storm Center v1.5.1 – internal and external web based outage location viewing and trouble call submittal tool

R[3.N] Historian Server

R[3.O] Oracle Mobile Workforce Management

R[3.P] Automatic Vehicle Locator (AVL)

R[3.Q] Transmission Outage Application (TOA)

R[3.R] Primate Video Wall Presentation Software

R[3.S] Network Model Manager (NMM)

R[3.T] AE SCADA/EMS System ABB NMR4 (Network Manager Release 4)

0.4 Organization of the Specification

R[1] This ADMS-SCADA Specification is organized as follows:

Technical Requirements Sections

Section 0, Introduction – High-level summary of the ADMS-SCADA Specification technical contents

Section 1, Project Management – ADMS-SCADA Project Management Requirements

Section 2, Architecture – Description of the architecture, configuration and failure management, availability, and standards for the ADMS-SCADA

Section 3, Capacity and Performance – Defines the hardware and software capacity and performance requirements

Section 4, User Interface – Functional description of the requirements for alarm and event processing, user interface design standards and general features, trending, hardcopy, and displays

Section 5, Hardware Requirements – Provides a description of the major hardware elements and characteristics that will support the ADMS-SCADA

Section 6, Data Acquisition and Processing – Functional description of the requirements for data acquisition, data exchange, supervisory control, and data processing

Section 7, Information Storage and Retrieval – Functional description of the requirements for the short-term and long-term archival data requirements

Section 8, Documentation – Describes the standard and custom documentation requirements

Section 9, Quality Assurance and Testing – Describes the requirement for quality assurance and factory and site testing

Section 10, Training – Describes the training requirements

Section 11, Project Implementation – Describes the project implementation responsibilities, project organization, project documents, and responsibilities for testing, shipping, and commissioning the ADMS-SCADA

Section 12, Cyber Security Requirements – Provides the cyber security requirements to ensure compliance with NERC CIP requirements

Section 13, ADMS-SCADA Function Requirements – Provides the requirements for the DMS subsystem

Section 14, Operator Training Simulator – Functional description of the requirements for an Operator Training Simulator used as a training facility

Appendices

Appendix A - Glossary

Table of Contents

1. ADMS-SCADA Project Management Requirements 1

1. ADMS-SCADA Project Management Requirements

Understanding the AE project management philosophy is critical to the success of the ADMS-SCADA project. The AE standard of project management is adequately described as adhering to the Project Management Body of Knowledge (PMBOK) and all Project Management Institute (PMI) best practices for managing complex projects. The methodology provides the Vendor, AE project manager and other stakeholders with insight into how projects are selected by AE management and implemented by project teams. These processes have been recognized as best practice and are applied globally and across industry groups.

AE requires the Vendor to provide and ensure expert project management of the ADMS-SCADA project throughout the entire project life cycle. The project life cycle describes the tasks that must be completed to produce a product that meets the requirements outlined in the scope of work. The Vendor's project manager shall be experienced in the execution of complex projects using the PMI standards.

Working with the AE Project Manager, the Vendor will present a methodology for managing the complete life cycle of the project. The life cycle will include initiation, pre-planning, gap analysis, project kick-off, work breakdown structure development, training, execution of work, control of work, testing, commissioning and final acceptance; all phases of the project. The Vendor will be required to manage each PMBOK knowledge area as described in ANSI/PM 99-001-2011 Standard included in the PMBOK publication.

Vendor will have complete and total responsibility for development and maintenance of the project schedule using Microsoft Project 2007. The project schedule details will include baseline start and baseline finish, percent complete of each task, percent complete of project and milestones, project completion date, resource allocation for each task, project deliverables and other information as directed by AE. The project schedule will include identification of tasks using descriptions that are easy to understand by all stakeholders. The project schedule will include all necessary logical relationships to ensure the AE project manager can easily track the critical path. Changes in project baseline will be included in the schedule as a milestone date for tracking. If Vendor development work is required, the project schedule will include development tasks required to meet the requirements included in this scope of work.

The Vendor is responsible for keeping the project schedule up to date at all times. The Vendor is responsible for including accurate and up to date resource calendars; calendars must be accurate up to one month in advance of scheduled work and will include vacations, holidays and absences of all resources. Changes that delay the project completion date by more than 10 business days shall be approved by AE and if approved the Vendor will develop a revised baseline. All baselines will be numbered and carried in the project schedule for the duration of the project life cycle.

The Vendor project manager will have a minimum of 5 years of experience in managing SCADA and advanced application projects. The Vendor's project manager will have experience managing complex projects using industry standard and best practice methodology. Vendor will provide examples of project manager's previous work. A complete plan following the Project Management Body of Knowledge (PMBOK) guidelines and best practices for all deliverables, including project scheduling is required. The Vendor shall provide evidence of the project manager's experience in managing previous projects requiring the installation of the Vendor's existing product.

The project management of the ADMS-SCADA project will require significant effort on the part of the Vendor. The project will not be managed by monthly status reports. The Vendor will provide a monthly report as a tool for the AE project manager to update the project stakeholders. The reports will be formatted as required by AE and will include the projected completion date with up to date Microsoft project schedule, baseline start and finish, and total slippage or advancement in calendar days. Vendor will provide all information requested by AE in the monthly status report.

The responsibility for ensuring that the methodology is being followed consistently across the utility is shared by many stakeholders at AE. The AE project manager and AE project sponsor will ensure that the methodology is being followed for the ADMS-SCADA project.

Requirements stated here may be duplicated in section 11.

Table of Contents

2. ADMS-SCADA Architecture 2-2
  2.1 Logical System Configuration 2-2
    2.1.1 Energy Control System 2-2
    2.1.2 System Redundancy 2-4
    2.1.3 Program Development System (PDS) 2-5
    2.1.4 Distribution Operator Training Simulator (OTS) 2-6
    2.1.5 Quality Assurance System (QAS) 2-6
    2.1.6 Communications Overview 2-7
    2.1.7 External Interfaces 2-10
  2.2 Software Architecture 2-11
    2.2.1 Open Systems Interfaces 2-12
    2.2.2 XML Interface 2-12
    2.2.3 System Services 2-12
    2.2.4 Application and System Development 2-14
    2.2.5 Database & Display Construction 2-17
  2.3 Configuration Control, Redundancy, and Failure Management 2-23
    2.3.1 ADMS-SCADA Configuration Management 2-24
    2.3.2 Independent System Health Monitor 2-30
    2.3.3 Inter-site Switchover for ECS 2-31
  2.4 System Availability 2-32
  2.5 Standards 2-34

2. ADMS-SCADA Architecture

R[1] This specification describes the conceptual expectation of the ADMS-SCADA architecture. The vendor shall provide AE with proposed details and diagrams for the architecture necessary to provide the requirements described.

R[2] The overall ADMS-SCADA architecture must be flexible and scalable to support the future migration of the system hardware and software. The ADMS-SCADA component architectures shall be expandable to support new application software as AE’s functional requirements evolve and to support future expansion.

2.1 Logical System Configuration

R[1] The ADMS-SCADA system comprises several component systems: redundant Energy Control Systems (ECS Prod 1 and ECS Prod 2), a Distribution Operator Training Simulator (DOTS), a Program Development System (PDS), and a Quality Assurance Test System (QAS).

R[2] This division of the components of the ADMS-SCADA and the distribution of functionality among the components are conceptual.

R[3] It is required that any ADMS-SCADA workstation may access any of these systems as a result of a logon selection & account permissions.

R[4] The following definitions are provided as the perceived role for each component system.

2.1.1 Energy Control System

R[1] The redundant Energy Control Systems (ECS) shall support the real-time operation of the electric distribution system. The designations ECS Prod 1 and ECS Prod 2 shall be used to distinguish between the two systems when necessary for clarity only. Both ECS Prod 1 and ECS Prod 2 are intended to support identical functionality. In this RFP, the term ECS shall refer to both systems. The ECS shall consist of the components described below.

R[1.A] Energy Control System (ECS)

R[1.A.i] The ECS is the real-time core of the ADMS-SCADA and shall provide the functionality required to monitor and control the AE electric distribution system.

R[1.A.ii] The ECS shall consist of high-availability (99.98%) systems characterized by high-speed data collection and presentation functions.

R[1.A.iii] All of the ADMS-SCADA applications that support operation of the electric distribution system shall execute on this platform.

R[1.A.iv] The ECS shall be fault-tolerant and redundant using clustering or Storage Area Network (SAN) architecture (or other advanced fault-tolerance techniques), to enhance the performance characteristics of the system.

R[1.A.v] The ECS shall be designed to support all workstations and their associated performance requirements in its operating area.

R[1.B] Distributed Front End Processors (FEPs)

R[1.B.i] The ECS shall include distributed FEPs [(located at System Control Center (SCC) & Back-Up Control Center (BUCC)) to allow the data acquisition function to be performed independent from the SCADA function and other application servers, regardless of the number and location of both the host and backup data center sites.

R[1.B.ii] The main feature of these distributed FEPs is that they will enable the collection and processing of field data, support AE's legacy communication facilities, and provide a transition tool for system checkout and parallel operation when the new systems are being installed and commissioned.

R[1.C] User Interface

R[1.C.i] AE intends to develop multiple control centers to house distributions operations.

R[1.C.iii] The arrangement of operating permissions and of alarm presentation and management capabilities must be flexible to support varying staff and location requirements associated with off-prime-time shifts, storm support, or emergency operations due to the loss of a control center.

R[1.C.iv] Also, the design of the proposed system shall be flexible to allow AE to add, delete, or move control centers as determined by business needs.

R[1.C.vi] The ADMS-SCADA shall include operator workstations as required for each Operations Control Center as part of each component system.

R[1.C.vii] The ADMS-SCADA will need to support a large volume of users during storm conditions, while maintaining high levels of cyber security within the secure network.

R[1.C.viii] The User Interface equipment (e.g., workstations and printers) may be isolated from the ADMS-SCADA servers with a DMZ that is designed to isolate this equipment and provide an additional level of security.

R[1.C.ix] Workstations shall operate as common facilities shared among all component systems, however. It shall be possible for any viewport at any workstations to be assigned (logically connected) to any component system assuming that a suitable communications path exists between the workstation and the component system.

R[1.C.x] Please note that there will be some specific exceptions to this logical inter-connectivity to ensure security and reliability of the systems, e.g., the separation of the QAS from the Production ECS.

R[1.D] Information Storage and Retrieval System

R[1.A.i.a] The IS&R functions shall execute on a high-availability platform dedicated to the historical data storage functionality.

R[1.A.i.b] The IS&R shall be scalable to support other business applications in addition to those required of the ADMS-SCADA.

R[1.A.i.c] It shall serve ADMS-SCADA users and shall interface to a historian server to serve a number of non- ADMS-SCADA users.

2.1.2 System Redundancy

R[1] ECS Prod1 shall be located remotely from ECS Prod 2.

R[2] Operation of the ADMS-SCADA will be moved between the two systems periodically, with the other serving as backup in case of catastrophic loss of the other system.

R[3] The hardware and software technology shall be the same at both locations such that the incremental maintenance costs for hardware, software, database, display, and report updates and training are minimized.

R[4] ECS Prod 1 and ECS Prod 2 shall have a one-to-one match regarding configuration, redundancy, and functionality of the other.

R[5] Each system shall be a “hot” backup for the other, kept up-to-date with real-time updates of data for the ECS.

R[6] The ADMS-SCADA shall enable a smooth and rapid switchover between the two systems in the event of an emergency, for periodic tests and for transfer of operations. Please refer to Section 2.3.3, Inter-site Switchover for additional information regarding this functionality.

R[7] Procedures shall be provided to enable this manual transfer between the two systems.

R[8] The ADMS-SCADA shall be designed to protect the each system from corruption or failure due to a failure of the other.

R[9] The development databases shall also be maintained between sites with tools to allow the user to transfer changed databases, when they have been tested and are ready for distribution. Please refer to Section 2.2.4, Application and System Development, for additional details of this process.

2.1.3 Program Development System (PDS)

R[1] A stand-alone PDS, with ADMS-SCADA functionality and hardware, shall support AE’s development and testing of ADMS-SCADA applications, database, displays, and reports.

R[2] The PDS shall be initially delivered with basic database and display generation capabilities as described in both Sections 2.2.5 and 13.2.

R[3] The initial PDS shall include the Vendor‘s software and support tools sufficient to enable AE to perform display development and import of feeder diagrams and modeling information, and RTU point checkout.

R[4] The initial PDS shall also include software development tools, such as compilers, source control, and development kits necessary to support any future porting of AE-supplied applications to the ADMS-SCADA platform.

R[5] The PDS equipment (e.g., workstations and printers) shall be isolated from the ADMS-SCADA production ECS with a DMZ that is designed to isolate this equipment and provide an additional level of security.

2.1.4 Distribution Operator Training Simulator (OTS)

R[1] A dedicated, stand-alone distribution OTS shall execute on hardware dedicated to that functionality.

R[2] It shall provide the capability to train System Operators by simulating both the distribution system and the ADMS-SCADA functions.

R[3] The DOTS equipment shall be isolated from the production ECS with a DMZ that is designed to isolate this equipment and provide an additional level of security.

2.1.5 Quality Assurance System (QAS)

R[1] A stand-alone ADMS-SCADA QAS shall provide a platform for testing of system revisions and upgrades before the changes are installed on the Production Systems.

R[2] The QAS equipment shall be isolated from the ADMS-SCADA with a DMZ that is designed to isolate this equipment and provide an additional level of security.

R[3] The QAS hardware and software shall be the same as the production systems so that the QAS correctly reflects the configuration to allow accurate and complete testing.

R[4] The QAS shall be configured to allow the use of other ADMS-SCADA workstations during testing and QA sessions.

R[5] The QAS shall be capable of simultaneously acquiring real-time data directly from data sources (via the QAS data acquisition facilities by redirecting communication circuits) and from the PDS or other ADMS-SCADA component systems using automated and manually initiated tools to transfer real-time data for testing purposes.

R[6] Control commands issued from the QAS shall be communicated to field devices only if those devices are directly and solely attached to the QAS.

R[7] Commands directed to devices communicating through production system components shall be disabled, even though the QAS may be collecting data from the devices via the production system components.

R[8] The QAS FEPs shall be sized both to include sample channels for each RTU protocol and to emulate the largest and most diverse set of front-end channels.

R[9] The ADMS-SCADA shall also include a patch management facility to receive, test, install, and distribute cyber-security and other patches (Section 12.20).

R[10] The facility shall include all hardware and software to accurately manage and track the patch process.

2.1.6 Communications Overview

R[1] The Vendor shall supply and implement all communications facilities not marked as Supplied by AE in Section 5 Hardware Requirements.

2.1.6.1 Local and Wide Area Networks

R[1] The ADMS-SCADA LAN shall be considered a "trusted" network.

R[2] It shall be a virtual LAN running on the AE corporate LAN/WAN.

R[3] Due to the distributed nature of the AE facilities, AE has established a high-speed Wide-Area Network (WAN) for control systems use that interconnects the multiple control centers.

R[4] All servers connected to the trusted network will be individually firewalled to prevent access to the rest of the system, should one be compromised.

R[5] The Vendor shall identify the ADMS-SCADA WAN bandwidth required to meet the performance requirements of this Specification.

R[6] AE expects to provide high-speed WAN interconnections that extend the ADMS-SCADA LAN to all control center sites. The ADMS-SCADA LAN will operate over dedicated circuits on AE's WAN. Any system or user connected to the ADMS-SCADA LAN shall be subject to user

ID and password access authorization. Password requirements are discussed in Section 2.1.6.2.

R[7] The redundant ADMS-SCADA LAN shall use load balancing to minimize the LAN capacity utilization.

R[8] Communications Network Processors shall support the connection between and the ADMS-SCADA and those external systems communicating to the ADMS-SCADA via the ICCP protocol.

R[9] The ADMS-SCADA Production ECS shall be isolated from the QAS, PDS, OTS, and user interface equipment (e.g., workstations and printers) by creating DMZs for these non-Production systems and peripherals.

R[10] The ADMS-SCADA shall be connected to the Corporate WAN via firewall. The firewalls shall provide protection from possible security threats occurring via the Corporate WAN. More detail is provided in Section 5.4.3.

2.1.6.2 ADMS-SCADA Access Security

R[1] A mechanism for defining and controlling user access to the ADMS-SCADA shall be provided.

R[2] Even though a user has logged onto the ADMS-SCADA network or a processor, access to the ADMS-SCADA functionality shall be subject to these additional security checks.

2.1.6.2.1 User Login

R[1] Password security shall be provided for authorized access to the ADMS-SCADA.

R[2] The ADMS-SCADA shall include a redundant pair of LDAP servers at each of the ECS locations with Active Directory single sign-on capability to simplify the AE password maintenance and control process and user sign-on process across the full suite of ADMS-SCADA applications and servers.

R[3] This facility shall allow the administrator to request a report of users, to be used to periodically compare to the AE corporate users/employee information.

R[4] The report shall include, as a minimum: employee name, an invariant key to uniquely identify each user, employee ID, 256-character free-form text, and other user permission information.

R[5] Users shall log in by entering a user ID and a password. Each password shall be validated against the corresponding user information stored in the database. A procedure shall be provided for users to log off.

R[6] ADMS-SCADA user IDs and passwords shall be encrypted at the workstations and transmitted over the network using secure communications techniques (e.g., ssh or ssl) and stored in encrypted form.

R[7] The ADMS-SCADA shall enforce configurable password construction rules as defined in Section 12.17, Authentication Methods and Password Construction.

R[8] Each of the password rules shall be configurable by AE, which will include the ability to enable or disable each rule individually.

R[9] Users shall be able to change their own passwords. Changed passwords shall be propagated throughout the ADMS-SCADA as necessary and without additional user intervention.

2.1.6.3 RTU Network

R[1] Communications between the ADMS-SCADA and “outstations” (Remote Terminal Units (RTUs), data concentrators, IEDs, etc.) are carried over digital circuits, analog (voice-grade), IP networks, MPLS, leased Telco facilities, and/or Frame Relay, JMUX, point-to-point, and multi-point channels using third-party communications and AE’s communications infrastructure.

R[2] The RTU channels are terminated at AE both individually and as consolidated groups of circuits using larger digital communication pipes.

2.1.6.4 Remote Maintenance Access

R[1] AE will provide its own functionality for Vendor remote access that will leverage port level control and Virtual Private Network (VPN) security.

R[2] The ADMS-SCADA shall include a function where an authorized user can, with a single action, isolate the ADMS-SCADA from the Corporate WAN, from the Production ECS, QAS, and OTS, and from all external systems.

R[3] This function shall be implemented with system features and scripts to minimize the steps required to enable the isolated operation mode.

R[4] In isolated operation, the only communication links from the ADMS-SCADA shall be those to the redundant ECS and to data sources and power system devices.

R[5] In no event shall any ADMS-SCADA function, other than communication with external systems or the Corporate WAN users, be affected by any queue or buffer overflows.

2.1.7 External Interfaces

R[1] The ADMS-SCADA shall be designed to exchange data with external systems, AE applications, and other systems on the AE Corporate Network.

R[2] These systems are listed below. Refer to Section 13.5 for ADMS-SCADA external interface details. External interfaces:

R[2.A] GoalArt Alarm and Event processesor or equivalent.

R[2.B] iFactor Storm Center

R[2.C] Ecologic Meter Data Management System (MDMS)

R[2.D] ICCP data to and from other systems

R[2.E] Data Concentrators (Intelligent Communication Gateway (ICG), etc.)

R[2.F] IBM Websphere Process Server

R[2.G] GE Smallworld GIS

R[2.H] GE Electric Office GIS

R[2.I] Oracle Customer Care and Billing (CC&B) CIS

R[2.J] Automated meters (AMI) will be interfaced directly with Landis + Gyr or the local Ecologic Meter Data Management System (MDMS) for power out, power up reporting and pinging.

R[2.K] AECall – an internally developed corporate trouble call recording application

R[2.L] 21st Century High Volume calling system – an externally hosted automated call answering service

R[2.M] iFactor Storm Center v1.5.1 – internal and external web based outage location viewing and trouble call submittal tool

R[2.N] Historian Server

R[2.O] Oracle Mobile Workforce Management

R[2.P] Automatic Vehicle Locator (AVL)

R[2.Q] Transmission Outage Application (TOA)

R[2.R] Primate Video Wall Presentation Software

R[2.S] Network Model Manager (NMM)

R[2.T] AE SCADA/EMS System ABB NMR4 (Network Manager Release 4)

2.2 Software Architecture

R[1] AE prefers a distributed computing environment that ensures adequate flexibility for the evolution of the ADMS-SCADA.

R[2] In view of the requirements imposed by the NERC CIP cyber security standards, AE prefers to use Microsoft Windows operating system.

R[3] The distributed computing environment shall be able to use both local area networks and wide area networks transparently, such that there will be no restrictions on the geographic dispersal of applications and data among the servers of the ADMS-SCADA.

2.2.1 Open Systems Interfaces

R[1] AE requires documented open Application Programming Interfaces (APIs) that will support integrating AE- or third-party-developed applications.

R[2] Vender will provide a list of APIs that they support.

2.2.2 XML Interface

R[1] Data import and export capabilities via XML with secure data transport mechanisms shall be provided.

R[2] Messages shall be defined via XSD (the XML Schema Definition language). Vendor shall produce, and AE shall have review and approval of, interface specifications for the data.

R[3] Various types of information shall be exchanged through this facility, including, for example:

R[3.A] Power system device real-time information including point values, quality (Section 6.3.1), and attributes

R[3.B] Events, safety tags, and memos

R[3.C] Equipment operating information

R[3.D] Planned outages

R[4] Vendor shall provide the capability within the database construction and maintenance environment to enable a programmer/engineer to define and maintain the content, format, schedule (e.g., time-of-day, periodicity, report-by-exception), and destination of the data to be transferred.

R[5] Additionally Vendor shall provide the capability to define, maintain, and export the mapping of data objects between the ADMS-SCADA and external systems.

2.2.3 System Services

R[1] System services provide facilities to the application systems that run in the ADMS-SCADA distributed computing environment.

R[2] Where appropriate, the Vendor shall use the services provided by the operating system. These services shall include:

R[2.A] Global Naming Service – Objects of interest in the ADMS-SCADA shall be assigned names in a global directory, which shall allow users to reference DMS objects in the directory both by name and by type of service.

R[2.B] Network File Service – Services shall be provided to give authorized users of the ADMS-SCADA access to files from anywhere in the network, subject to restrictions imposed to meet cyber-security requirements (e.g., securing NFS mounts). The file system shall provide a reliable, consistent interface that offers the same performance and ease of access for both network and locally resident files.

R[2.C] Scheduling Services – Scheduling services shall include a centralized facility for scheduling application activity based on time-of-day, period, and other events.

R[2.D] Time Services – Time services shall maintain a common system time across all processors and devices. The ADMS-SCADA vendor shall include GPS based time reference appliances included as part of each ECS Production server cluster as the official time references. System time shall be periodically synchronized to the time standard. The Time Service function shall include the ability for an authorized user to modify the Daylight Savings Time start and end dates and times. This capability shall be provided for Vendor-developed software, for Operating System software, and for third-party-developed software.

R[2.E] Print Services – Hard-copy output resources in the computing network shall be assigned as network (rather than local) resources configurable by the System Administrator, and shall be available for use from any node in the network.

R[2.F] Distributed Backup and Archiving – Services to back up, archive, and restore all ADMS-SCADA software, operating system image, displays, and data independently of its location shall be provided on the ADMS-SCADA networks. The backup information shall include the ADMS-SCADA and network configuration information, such as database table and queue sizing, router tables, and firewall access rules.

2.2.4 Application and System Development

R[1] The ADMS-SCADA shall include tools to allow AE to develop applications and their components such as executable application images, user interface definitions (displays and display interactions), data sets, messages, and reports, all working together to deliver a particular functionality.

2.2.4.1 Software Configuration Management

R[1] An integrated source code development subsystem supporting C, Java, and C++ and all other programming languages used in the ADMS-SCADA shall allow teams of programmers to work together effectively, including allowing concurrent activity by AE and Vendor personnel.

R[2] The Vendor shall provide a software configuration management system to define the elements and the associated attributes of the applications provided in the ADMS-SCADA.

R[3] Source definitions for the application's elements (e.g., source code, display formats), the residency requirements (e.g., local, shared), and any access attributes shall be defined through the software configuration management system.

R[4] The source code development subsystem shall support numerical version identification to reflect updates or changes to the code and associated databases and shall provide the capability to revert to any previous version, thereby allowing AE to recover/remove changes when required.

R[5] Procedures for completely regenerating executable images and run-time files shall allow individual applications to be rebuilt and installed. Applications shall be made part of any application system by a straightforward procedure that requires no modification to application sources.

2.2.4.2 Compilers

R[1] Compilers with code optimization features shall be provided for all programming languages used in the ADMS-SCADA.

R[2] Compilers shall conform to the latest applicable standards (e.g., ANSI and IEEE standards).

R[3] Program source code shall use symbolic interfaces for all application system services. The compiler shall provide extensive error-checking facilities, explicit error messages, and complete output listings.

2.2.4.3 Interactive Debugger

R[1] An interactive debugger shall be supplied that includes full or selective (interpretative) trace, memory alter and dump, snapshot with or without memory dump, and search capabilities.

R[2] The interactive debugger shall use symbolic references to statements and variables.

R[3] It shall also provide simultaneous presentation of the source code with an indication of program flow (i.e., the currently executing statement).

2.2.4.4 Diagnostics

R[1] The ADMS-SCADA shall include all diagnostic software provided by the manufacturers of all hardware, including processors and peripheral devices, supplied with the ADMS-SCADA.

R[2] The ADMS-SCADA shall also support error detection and diagnostic tools sufficient to support the requirements of this section.

R[3] Diagnostics for communications with data sources and external computer systems shall provide, as a minimum, at least the following capabilities:

- R[3.A] Select any communications channel for test
- R[3.B] Select a request message for transmission to data sources and computer systems
- R[3.C] Select single or cyclic message transmissions to data sources and computer systems for test purposes
- R[3.D] Monitor and display information sent to and received from data sources and computer systems
- R[3.E] Monitor and display data communication device status
- R[3.F] Provide communication statistics including the number of errors, retries, bytes transferred, etc.

R[4] The communications diagnostics shall include a "trace" facility for messages as they are sent and received.

R[5] The trace facility shall trace a selected set of or all logical channels, and shall provide explicit trace information at each level of the protocol stack.

R[6] It shall be possible to trigger the trace facility manually as well as by program status flags and inter-program messages.

2.2.4.5 SCADA Database (SCDB) Access

R[1] A library of event routines shall be the preferred means for application programs to interact with the SCDB, using a callable interface (API) to these routines.

R[2] These event routines shall serve as generic APIs for database access thereby eliminating proprietary database function calls at the application level.

R[3] The SCDB shall provide the following general capabilities:

- R[3.A] Interfaces to the database shall be by logical names.
- R[3.B] ADMS-SCADA users, including technical staff maintaining applications or databases, shall not be exposed to internal identifiers of database items, such as indexes into tables.
- R[3.C] Application interfaces to the database shall support direct access to the individual elements comprising an entry in the database.
- R[3.D] Multiple concurrent accesses to the database.
- R[3.E] Support services shall be provided for deadlock prevention, locking, and access authorization.
- R[3.F] Transaction monitoring and rollback (i.e., version control)
- R[3.G] Database administration and utility functions, including as a minimum: automatic recovery and restart, triggering of program actions resulting from database updates, logging facilities on tapes and disks to save transactions, import/export utilities to migrate data to other databases, and performance monitoring and tuning utilities, such as those for the compression and compaction of data, division of data over different storage units, automatic reorganization of index schemes, and computation of performance statistics.
- R[3.H] A distributed database environment, including: verification of data integrity and automatic navigation through the database where access to the data is transparent to the user, developer, or application program

2.2.4.6 Adjustable Parameters

R[1] All parameters in the ADMS-SCADA shall be defined in the database and shall be adjustable by authorized system personnel.

R[2] Adjustments made to parameters shall become effective without having to recompile programs or regenerate all or portions of the database.

R[3] All time periods contained in this Specification shall be considered initial values for planning purposes, but all software parameters must be adjustable by AE personnel.

2.2.4.7 Data Conversion

R[1] The Vendor shall load the following existing data into the ADMS-SCADA.

R[1.A] SCADA – the data will be supplied in a mutually agreed format.

R[1.B] Distribution System Model – the vendor shall load the AE circuit information from AE's Smallworld GIS database. Other data sources may include engineering planning tools such as Milsoft and/or ABB FeederAll.

R[1.C] Historical outage information – AE operates an existing outage management system. The outage information on this system must be remapped and loaded in the ADMS-SCADA archive database.

R[2] The conversion tools shall include features to facilitate the conversion of similar, but not identical attributes, and to generate default attributes for items not found in the existing databases.

2.2.5 Database & Display Construction

R[1] The Vendor shall provide a database and display development environment on the PDS system.

R[2] The development environment shall be able to manage the database and display construction and maintenance work required to support the ADMS-SCADA and shall satisfy the performance requirements of Exhibit 3-5, Software Maintenance.

2.2.5.1 Database Construction and Maintenance

R[1] Database construction refers to the definition of the initial database structure, population of the structure with its initial contents, and revision of the structure when necessary.

R[2] Database maintenance refers to the subsequent addition of new database contents and the modification of existing contents.

R[3] The Vendor's database construction and maintenance tools shall allow construction and maintenance of all databases within the ADMS-SCADA, including the TASE.2 databases as described in Sections 6.2, the Distribution System Operations Model as described in Section 13.2 and the IS&R/PI databases described in Section 7.

R[4] The tools shall provide the ability to update just a changed portion of the database (Incremental Update) or perform a Complete Database Regeneration.

R[5] The tools used by the Vendor for the development and maintenance of the Source Database (SDB) shall be delivered with the ADMS-SCADA.

R[6] The ADMS-SCADA shall include a single logical repository for all on-line data needed for applications to model the historical, current, and future state of the power system and ADMS-SCADA applications – the Source Database (SDB).

R[7] (Note that, dependent on the recommended database maintenance philosophy and tools provided, the PDS may contain an independent copy of the Source Database that is transferred to the QAS and/or production systems when initiated by the user.)

R[8] All information needed to describe the models and database configuration parameters on which the ADMS-SCADA operates shall be defined once in the centralized, fully integrated SDB and made available to all ADMS-SCADA applications, real-time database, and user interface maintenance tools that need the information.

R[9] The SDB shall also include parameters controlling execution of ADMS-SCADA functions.

R[10] The ADMS-SCADA shall include the capability to maintain a backup SDB at the backup PDS instance located at the BUCC using automated tools when manually initiated by the database users.

R[11] The SDB, its associated tools, audit logs, and code management systems shall fully support the following four major data database definition components:

R[11.A] Global ADMS-SCADA Database Parameters
R[11.B] SCADA/ICCP Data Definitions
R[11.C] Network Analysis (NA) Data Model Definitions
R[11.D] Distribution System Operations Model

R[12] The SDB shall also accept interactive user commands and scripted SQL statements to provide at least the following functions:

R[12.A] Storage of the database data definitions, including schemas, relational tables, views, and fields.

R[12.B] An active repository component that provides the capability to organize, manage, and control information about users, applications, and programs that access the data.

R[12.C] On-line access to review the structure of the database and its data definitions.

R[12.D] On-line access to all SCADA data to allow updates and additions to the on-line database without requiring a system restart or failover to make the changes operational. This feature shall also create database change transactions to reflect the on-line changes back into the maintenance version of the SDB.

R[12.E] Development of new databases including batch-load capability from external database sources (e.g., Access databases, text files).

R[12.F] Comparison of the on-line “production” database with a new database to identify previous on-line database changes that might not have been incorporated into the new database.

R[12.G] Copying of existing database structures.

R[12.H] Modification of the database definition without unloading/loading the database.

R[12.I] Modifying existing databases, such as adding attributes (“columns” in a table-row-column structure). The addition of attributes shall not disrupt access to existing attributes.

R[12.J] Listing of all information on database parameters, attributes, etc.

R[12.K] For a given relation or table, a list of relations referencing this relation table and a list of relations referenced by this relation or table. Preferably, these relationships shall be shown graphically.

R[12.L] Support for command lists or catalogued procedure input.

R[12.M] Automatic time and date stamp on output.

R[12.N] Name-change utilities that identify all uses of an entity name throughout the ADMS-SCADA databases and facilitate selective and global changes to an entity's name.

R[12.O] The ADMS-SCADA shall enforce naming standards based on the AE naming conventions (to be provided during project discovery phase). The process for integrating and finalizing the initial set of naming conventions into the Vendor's standard SDB structure shall be demonstrated as part of the data engineering workshop described in Section 10.3.3.

R[12.P] Processing of the SDB into the data structures used by the ADMS-SCADA for on-line applications – the "run-time" databases.

R[12.Q] If a point name has been changed or deleted, the database generator shall identify the displays and reports that are affected by the change, and at a user request, update the point names in the affected displays and reports.

R[12.R] Initiate the CIM import/export process for exchanging power system modeling information with other computer systems.

R[12.S] All entries to the SDB shall be checked for validity, both syntactic and semantic. Effective use shall be made of menu selections, dialog boxes, list boxes, text boxes, and selection entries. Old values shall be displayed in conjunction with the request for new values during database modifications. All database modifications, including detailed listings of old and new data values shall be maintained in a time-stamped audit log along with the user identification. The log shall be displayed on a workstation and printed upon demand.

R[12.T] Data not modified when a database is maintained, including run-time data, shall not be changed or reset to default values. The current items in the run-time database shall be retained in the modified database, except for those specific items modified. This requirement specifically applies, but is not limited to:

R[12.T.i] Values and attributes of telemetered and calculated points.
R[12.T.ii] Models and execution parameters for applications.
R[12.T.iii] Save cases (refer to Section 13.4.3).
R[12.T.iv] Data entered manually by users.

R[13] Modified portions of the ADMS-SCADA databases shall be buffered and shall not be used until commanded by a user.

R[14] A copy of the pre-modification database shall be retained until a subsequent user command indicates that the new database is acceptable.

R[15] At any time during the "temporary" use of the new database, the user shall be able to command the ADMS-SCADA to revert to operation using the previous unmodified database.

R[16] The ADMS-SCADA shall support multiple files ("work areas") of in-progress modifications, such that several users can be preparing database modifications at any time.

R[17] In addition, the ADMS-SCADA shall include the capability to separately undo recent individual database changes and revert to the pre-modified state.

2.2.5.2 Display Construction and Maintenance using ADMS-SCADA Data Maintenance

R[1] An interactive tool shall be provided for creating the operational displays and interfaces associated with each application.

R[2] With this tool, the user shall draw the contents of application windows, define dynamic linkages to any ADMS-SCADA data, and sensitize display elements to respond to user input actions (such sensitized elements are typically referred to as cursor targets and function keys).

R[3] The ability to link to any ADMS-SCADA data, not only real-time data, shall allow interactive graphic displays to be constructed for all applications in the ADMS-SCADA via the display building tool.

R[4] The display tool shall include an automatically generated Hierarchical Display Menu Directory as described in Section 4.7.

R[5] The editor shall support displays constructed as world coordinate spaces and displays constructed as fixed spaces and shall allow XML based editing.

R[6] The display editor shall be fully compatible with the database generation and editing function.

R[7] The display editor shall be fully interactive and shall provide "What You See Is What You Get" (WYSIWYG) capabilities.

R[8] The display editor shall maintain a complete audit trail of edit activity as part of software configuration management.

R[9] New displays shall be constructed beginning from a blank display, from an existing display definition, or from display templates within a library.

R[10] The editor shall support the creation of libraries of standard and custom symbols or components to be created, modified, and used to facilitate the editing process.

R[11] The display editor shall support the listing, dumping, reloading, and validating of display definitions.

R[12] The list function shall provide for partial and full summaries (directories) of displays cross-referenced to their use in applications.

R[13] The list function shall also produce detailed documentation of the contents of any display showing all elements and provide tools to find on which displays a given piece of data is referenced.

R[14] Dumping and reloading of displays shall be provided for individual displays, display libraries, individual applications, or an entire application system.

R[15] The display editor shall produce displays compatible with every workstation of the ADMS-SCADA. AE shall not have to develop multiple versions of displays for each type of workstation or for different GUI products included with the ADMS-SCADA.

R[16] The display editor shall support, as a minimum, the following construction features:

R[16.A] Editing features to copy, move, paste, rotate, delete, and modify selected groups of information and to undo/redo the previous actions.

R[16.B] Building a display at any scale (zoom) level.

R[16.C] Visible and invisible snap-grids at specifiable increments with snap-to-placement of objects on the grid.

R[16.D] Various font sizes, line types, and line thickness.

R[16.E] Linking of any defined graphics symbol to any database point.

R[16.F] Pop-up menus for selection of points for linkages by default. The points shall be those in a user-defined substation for which the display is being built. The user, however, shall be able to request a menu list of all available points.

R[16.G] Ability to establish different symbol or display conventions for the same database point on the same or on different displays.

R[16.H] Ability to display the short or long name for a database point.

R[16.I] Definition of dynamic display linkages to any ADMS-SCADA database variable on any ADMS-SCADA display.

R[16.J] Building and modification of display icons and store them in an easily accessible library.

R[16.K] Protection of any data field on any display against user entry based on log-on area of responsibility (AOR) identifiers, reference Section 4.2.4.

R[16.L] Activation of displays within any application system or across all application systems by a simple procedure that does not require a failover and that causes no noticeable interruption of on-line ADMS-SCADA activity.

R[16.M] A scripting tool to facilitate the modification of displays to incorporate AE changes on top of any Vendor product upgrades and to port existing AE displays and third-party products into the Vendor’s system.

R[16.N] Using drawing files in .dxf format as input.

R[16.O] The ability to export ADMS-SCADA display definitions using a .dxf file format.

R[16.P] The ability to link applications data on scrollable, list-based displays.

R[17] If a display definition is stored in multiple locations (for example, a copy in each workstation), a validation function shall be provided to ensure that all definitions over all workstations in all systems are consistent and up-to-date.

2.3 Configuration Control, Redundancy, and Failure Management

R[1] This section presents requirements for monitoring and managing the ADMS-SCADA hardware and software.

2.3.1 ADMS-SCADA Configuration Management

R[1] The ADMS-SCADA shall include a centralized management function that includes services for the configuration, control, and monitoring of ADMS-SCADA resources, including processors, peripheral device, network devices, applications, and databases.

R[2] Configuration management tools shall be accessible from any node in the ADMS-SCADA and shall be capable of managing resources anywhere in the network, subject to security restrictions and the performance criteria in Exhibit 3-4 Configuration Management Performance.

R[3] Management tools shall facilitate the orderly start-up, shutdown, and tuning of any ADMS-SCADA resource without affecting the availability of the other elements of the ADMS-SCADA.

R[4] Commercially available, standards-based network management products shall be used, particularly products employing the SNMP standards.

R[5] Products supporting both SNMP version 1 (SNMPv1) and community-based SNMP version 3 (SNMPv3) are preferred.

R[6] All ADMS-SCADA resources shall include SNMP agents for use by the ADMS-SCADA management function and by AE-supplied system and security management tools.

R[7] It shall be possible to add resources outside the ADMS-SCADA to the ADMS-SCADA configuration management scheme.

R[8] This may require modifications to these applications, databases, processors, or devices, such as the addition of agents or other software plug-ins in the future.

R[9] However, the ADMS-SCADA management function shall include documentation describing the interface requirements for both new ADMS-SCADA and non-ADMS-SCADA resources.

R[10] All errors and other events detected by the ADMS-SCADA configuration management function shall be recorded and reported to the user.

R[11] Fatal errors shall be reported as alarms.

R[12] Where an error causes the ADMS-SCADA management function to reconfigure the ADMS-SCADA (such as bringing a backup resource to the primary state), the reconfiguring action shall be reported as an alarm along with the error report.

2.3.1.1 Processor and Device States

R[1] Processor and device states identify the operating condition of each processor and peripheral device of the ADMS-SCADA and shall be used to determine the system's reaction when restart and failover operations take place as follows:

R[1.A] Primary – A primary processor or device performs any or all of the ADMS-SCADA functions

R[1.B] Backup – A backup processor or device replaces a primary processor or device in the event of primary failure or upon user command

R[1.C] Down – A down processor or device is not communicating with other elements of the ADMS-SCADA and is not capable of participating in any ADMS-SCADA activity

2.3.1.2 Processor and Device Interconnections

R[1] Interconnections shall be provided among all processors within a group, among all processor groups, and among all processor groups and all workstations.

R[2] This Specification assumes the use of local- and wide-area-networks, including necessary firewall security, for all interconnections.

R[3] The state of each processor connection to a network and the network itself shall be changeable by the user.

2.3.1.3 ADMS-SCADA Backup Databases

R[1] Backup databases shall be supported in a hot standby mode at both the primary sites and the backup sites so that ADMS-SCADA operation may continue immediately in the event of processor, device, or software failure. The backup databases shall be updated as changes occur with the current contents of the primary databases such that all real-time changes to a primary database are reflected in the backup database as they occur. Operator changes shall be transmitted by-exception on completion of the Operator action. Failure of a processor shall not preclude access to current data by the processor assuming the functions of the failed processor. The information maintained in the backup databases shall include:

R[1.A] Telemetered (i.e., both ICCP and RTU) data, manually entered data, and calculated values and their attributes, including quality codes, control-inhibit state, and safety tag data

R[1.B] ADMS-SCADA function execution and control parameters and input and output data, including save cases, displays, and contingency definitions.

R[1.C] Data maintained by the IS&R functions, including attributes

R[1.D] Alarm, event, and summary displays (such as off-normal, control-inhibit, and alarm-inhibit displays) or sufficient information to rebuild the displays in their entirety (including the time and date of the entry, not the time and date the display was created)

R[2] Changes to the quantity of information to be backed up resulting from the addition or deletion of items in an existing database shall be automatically accommodated by the backup function.

R[3] The addition, deletion, or restructuring of databases in the ADMS-SCADA shall be accommodated by the backup function without requiring changes to the code.

2.3.1.4 Error Detection and Failure Determination

R[1] All processors, devices, and functions shall be monitored for fatal and recoverable errors. All detected errors and failures shall be recorded for maintenance purposes. These records shall include the dates and times of the failures, the reason for the failure, and of the subsequent automatic or manual return to service.

R[2] The following shall be monitored:

R[2.A] Processor and Device Errors – All fatal and recoverable errors of all processors operating in the primary and backup states shall be detected. When the count of recoverable errors exceeds a threshold, a fatal error shall be declared.

R[2.B] Software Errors – Execution errors in functions that are not resolved by program logic internal to the function shall be considered fatal software errors (such as division by zero). A process that aborts and is considered to be vital shall initiate a failover. The non-fatal errors shall also produce an event informing the user of the error.

R[2.C] Reasonability of Data – All input data and parameters, whether collected automatically or entered by a user, shall be checked for reasonability and rejected if they are unreasonable with appropriate error messages.

R[2.D] All intermediate and final results shall be checked to prevent unreasonable data from being propagated or displayed to the user.

R[2.E] All programs and the system shall continue to operate in the presence of unreasonable data.

R[2.F] All calculations using the unreasonable data shall continue to use the last reasonable data, unless an alternate data source is selected.

R[2.G] Processing of Alarms – An independent health check monitor, independent of the alarm subsystem, shall be provided to ensure the ADMS-SCADA is actively processing all real-time system alarms (refer to Section 2.3.2).

2.3.1.5 Processor Redundancy and Failure Management

R[1] When a failure of a primary processor in a redundant group is detected, the ADMS-SCADA shall invoke the appropriate failover and restart actions so that functions assigned to the failed processor are preserved.

R[2] When a failure of a primary processor in a non-redundant group is detected, the ADMS-SCADA shall not invoke failover or restart actions.

R[3] Failures of processors in the backup state shall not initiate restart or failover actions.

R[4] The ADMS-SCADA shall only change the processor state to down.

R[5] The ADMS-SCADA shall support the following:

R[5.A] Function Restart – Function restart shall be invoked during system startup, manually by a user, and automatically to recover from hardware and software failures. Function restart shall proceed to completion without user intervention.

R[5.B] Processor Failover – In the event of failure of any primary processor in a redundant processor group, the ADMS-SCADA shall initiate a failover operation, restarting the functions of the failed processor in a functioning processor.

R[5.C] Where the ADMS-SCADA is configured such that functions are distributed (shared) across multiple primary processors, failover shall be implemented by reassigning the failed processor's tasks to another primary processor.

R[5.D] If backup processors are not available or sufficient primary processors are not available to perform the required functions, the ADMS-SCADA shall attempt to restart the failed primary processor.

R[5.E] After a failover, alarm conditions as shown on the alarm summaries and other displays shall be current as of the time of the last update of the backup databases prior to the failover.

R[5.F] All data, including calculated, manually-entered data such as overridden telemetered values, supervisory control device tags and control inhibits, function execution and control parameters, displays, application files, and input and output data, shall also be current as of the time of the last backup database updates.

R[5.G] Alarm conditions detected after the time of the last backup database update shall be annunciated as new alarms.

R[5.H] Processor Start-Up – Processor start-up shall be performed when commanded by a user such that the operating environment of the processor is established prior to restarting its functions. The start-up of a processor in a redundant pair shall not cause a failover operation.

R[5.I] System Power-On Start-Up – The ADMS-SCADA shall automatically restart itself when input power is interrupted and restored.

R[5.J] System restart shall include processor start-up, initialization of all network devices, initialization of all peripheral devices, initialization of all communications with data sources and external computer systems, resumption of all ADMS-SCADA functions, and notification to the users that start up has completed.

R[5.K] A processor shall restart to its prior state, if possible, or to the highest state available.

R[5.L] The system shall also include the capability to perform a Cold Start when selected by the user.

R[5.M] The Cold Start shall reload the system database from the un-initialized version that does not contain the real-time information from the previously on-line system.

2.3.1.6 Device Redundancy and Failure Management

R[1] Devices shall be configured as redundant or non-redundant as depicted in the System Architecture diagrams.

R[2] When a failure of a redundant device is declared, the ADMS-SCADA shall invoke the appropriate device failover actions so that on-line functions using the failed device are preserved. Processor failover shall not be necessary to recover from device failure.

R[3] When a failure of a non-redundant device is declared, the ADMS-SCADA shall not invoke processor or device failover or function restart actions.

R[4] On-line functions using a failed, non-redundant device may be lost until the failed device is restored to service.

R[4.A] Device Failover – The device failover function shall direct an orderly transfer of operation in the event of any primary, redundant device failure. Device failover shall accommodate the following special cases:

R[4.A.i] Workstations – Although workstations are configured as non-redundant devices, the failover logic shall ensure that all of the areas of responsibility assigned to a failed workstation are assigned to at least one other workstation.

R[4.A.ii] Archive storage – In lieu of an automated failover process, the user shall be able to direct output to or read data from any archive storage device.

R[4.A.iii] LANs and WANs – Recovery from failures of networks and network devices shall be managed by rerouting of communications. Failover to backup processors or devices in order to recover from network failures shall be attempted only where no network route to the primary processor or device is available. Network failure of a single communications path of a redundant LAN shall not cause a workstation failure and/or operator log off.

R[4.B] Device Reinstatement – Manually disabled devices shall be reinstated by user command. Failed communications to data sources or computer systems connected to the ADMS-SCADA shall be periodically retried.

R[4.C] When reliable communications are reestablished, the RTU, data source, or communication channel shall be automatically returned to operation.

2.3.2 Independent System Health Monitor

R[1] The ADMS-SCADA shall include an Independent System Health Monitor to ensure the availability of all ADMS-SCADA component systems (e.g., ECS, IS&R, PDS, QAS, and OTS) and functions as delivered.

R[2] In order to determine whether ADMS-SCADA functions are performing correctly and to give advance notification of a possible ADMS-SCADA problem, a monitor shall be employed to periodically check the conditions of the ADMS-SCADA as defined in Exhibit 3-4, Function Periodicity and Execution Time.

R[3] The monitor shall be independent of the ADMS-SCADA to be monitored so as to not be affected by any failures in the ADMS-SCADA itself. The monitor shall support multiple concurrent users and shall be capable of notifying the appropriate personnel if an abnormal condition is detected.

R[4] At a minimum, the following conditions shall be monitored:

R[4.A] Alarm Processing – The monitor shall verify that alarms are being processed and presented to System Operators in a timely fashion. This shall include a check for the generation of alarms created from derived values if this process is separate from SCADA-produced alarms. In addition, the ability to check for an abnormally high alarm rate (alarms issued per second) shall be provided.

R[4.B] Response Time – The monitor shall detect sustained abnormal response times to user actions.

R[4.C] Data Acquisition – RTU and ICCP communications are actively collecting and processing real-time data.

R[4.D] Service Task and Process Execution – The monitor shall check whether ADMS-SCADA service tasks and processes are executing and operating as scheduled.

R[4.E] CPU Utilization – Overall processor utilization shall be monitored, with alarms for sustained utilization over some predefined threshold. There shall be the ability to graph CPU utilization in real-time. In addition to overall utilization, the monitor shall also be able to display utilization on a task/thread level.

R[5] Independent System Health Monitor shall issue its own independent alarm messages and process the following alarm notification options:

R[5.A] Audible alarm;

R[5.B] E-mail (out-bound only, in-bound email shall not be allowed)

R[5.C] Text messaging (out-bound only, in-bound text messaging shall not be allowed)

R[5.D] Workstation pop-up window

R[6] Alarms shall be reissued on a periodic basis as long as an abnormal condition exists even if the original alarm was acknowledged.

R[7] In addition to any abnormal alarms that might be issued, a visual "heartbeat" indication shall be displayed on a regular basis to indicate the viability of the operator workstation connection to the health monitor.

R[8] This shall be done to negate the "no alarms = everything is OK" assumption.

2.3.3 Inter-site Switchover for ECS

R[1] In the event of failure of the ADMS-SCADA (ECS Prod 1 or ECS Prod 2), the other ECS (Alternate) shall assume monitoring and control of the entire power system. (This action is termed "inter-site switchover" to differentiate it from intra-site failover actions.)

R[2] To support this requirement, the Alternate shall be maintained in a state where it can assume full control.

R[3] The appropriate personnel shall be notified of the ADMS-SCADA failure, but the inter-site switchover process shall be initiated only by authorized user command.

R[4] Once initiated, the process shall proceed without intervention. A process and procedures shall also be provided to allow the automated portion of the switchover process to be manually completed incrementally through user controlled steps.

R[5] The Alternate's data shall be maintained hot such that a requested switchover will occur promptly and data shall be stored and processed in a bumpless manner.

R[6] This shall include the transfer of all data, including but not limited to telemetered data (all sources including ICCP), safety tag data, manually replaced data, study case data, and IS&R historical data.

R[7] After inter-site switchover, the databases of the Alternate shall be current to within the time specified in Exhibit 3-5, Configuration Management Performance, and all data and all displays available on the ADMS-SCADA shall be available on the Alternate.

R[8] The inter-site switchover actions shall specifically include connection of the Alternate to all data sources, including corporate interfaces required to maintain the system core functionality.

R[9] If the Alternate cannot connect to data sources or other computer systems, the Alternate shall alarm the users. The Alternate shall not attempt further inter-site, intra-site, or other failover or restart actions.

R[10] The ADMS-SCADA shall be able to assign front-end processors (FEPs) and ICCP communication processors at the Alternate as the primary source for collecting selected RTU data without causing a failover of the SCADA servers or an inter-site switchover.

2.4 System Availability

R[1] The Core ADMS-SCADA systems (the ECS systems) are essential to maintaining control of the AE Distribution power system, and shall exhibit a measured availability of 99.98% during the availability test. The ADMS-SCADA shall include the capability to record the availability statistics including recording information about scheduled (Hold Time, Section 9.12) and unscheduled outages.

R[2] The Core ADMS-SCADA shall have no single point of failure. That is, there shall be no hardware or software element that, as a result of its failure, renders the Core ADMS-SCADA unavailable.

R[3] Individual Core ADMS-SCADA devices, including processors, shall each exhibit an availability of no less than 99%.

R[4] The Core ADMS-SCADA software shall be considered available when all of the functions described in this Specification are operating as specified, at their scheduled periodicity.

R[5] The Core ADMS-SCADA hardware shall be considered available when sufficient processors, peripheral devices, and interfaces to data sources and computer systems external to the ADMS-SCADA are operating, and the Core ADMS-SCADA is satisfying its performance requirements.

R[6] The following minimum hardware complement is required to be operating for the ADMS-SCADA system:

R[6.A] Auxiliary memory sufficient to support the operating processors. For RAID memory, no more than one storage unit (disk) of each enclosure (chassis) shall be down.

R[6.B] All operating workstations except two shall be fully operational at any time.

R[6.C] At least four maintenance workstations

R[6.D] At least ONE color printer

R[6.E] At least ONE archive device (removable media)

R[6.F] Connections to the corporate WAN sufficient to support communications with all nodes/interfaces on that network

R[7] The availability applied to the other ADMS-SCADA component systems shall be separately applied. The other component systems include:

R[7.A] Operator Training Simulator

R[7.B] Program Development System

R[7.C] Quality Assurance System

R[8] Each component system of the ADMS-SCADA that is not included in the Core ADMS-SCADA shall individually satisfy the following availability requirements:

R[8.A] The system shall exhibit a measured availability of 99% over any one-month period. That is, the ratio of total time minus downtime to total time shall be equal to or greater than 0.99.

R[8.B] The system shall be considered available when all functions and all the hardware are operating. This requirement shall also be verified during the availability test.

R[8.C] Individual devices, including processors, shall each exhibit an availability of no less than 99% over any one-month period. This requirement shall also be verified during the availability test.

2.5 Standards

R[1] The design, construction, and performance of all equipment and software supplied by the Vendor shall conform at a minimum to the latest applicable standards listed below:

R[1.A] International Electrotechnical Commission (IEC)
R[1.B] International Organization for Standardization (ISO)
R[1.C] International Telecommunications Union (ITU)
R[1.D] American National Standards Institute (ANSI)
R[1.E] Institute of Electrical and Electronic Engineers (IEEE)
R[1.F] Electronic Industries Association (EIA)
R[1.G] National Electrical Manufacturers Association (NEMA)
R[1.H] North American Electric Reliability Corporation (NERC)/Electric Reliability Organization (ERO), including the NERC CIP standards (refer to Section 12).

R[2] In addition, the recommendations of the Electric Power Research Institute (EPRI) regarding preferred suites of approved standards for electric utility use (e.g., CIM, CCAPI) shall be used throughout the ADMS-SCADA.

Table of Contents

3. Capacity and Performance 3-1
3.1 ADMS-SCADA..3-1
3.2 ADMS-SCADA Capacity..3-3
3.3 ADMS-SCADA Performance 3-4
3.3.1 ADMS-SCADA Activity Scenarios 3-4
3.3.1.1 Base Conditions 3-4
3.3.1.2 Steady-State Scenario 3-6
3.3.1.3 High-Activity Scenario 3-8
3.3.1.4 Degraded Operation 3-10
3.3.2 Resource Utilization..3-11
3.3.3 User Interface Response 3-12
3.3.3.1 Display Request 3-12
3.3.3.2 User Requests..3-13
3.3.4 Resource Monitoring..3-13

List of Exhibits:

Exhibit 3-1: Number of Users..3-1
Exhibit 3-2: Distribution System Model Sizing 3-2
Exhibit 3-3: User Interface Response 3-14
Exhibit 3-4: Function Periodicity and Execution Time..3-15
Exhibit 3-5: Configuration Management Performance 3-16
Exhibit 3-6: Software Maintenance 3-17

3. Capacity and Performance

R[1] The ADMS-SCADA shall be designed to meet the capacity and performance requirements defined in this section while meeting:

R[1.A] The performance requirements of Section 3.3, ADMS-SCADA Performance.

R[1.B] The availability requirements of Section 2.4, System Availability.

R[1.C] The ability to interface with other systems such as PI Historian, SCADA EMS, Substation Based Mini SCADA systems.

R[1.D] The ability to handle real time non operational data for condition monitoring and make them available to an enterprise DB. Handling of this data shall neither compromise the performance of the ADMS-SCADA nor burden real time with alarms related to such data, which shall be directed via email or cell phone to designed technical personel.

R[1.E] The ability to handle EID's such as intelligent transformers

R[1.F] The ability to identify and categorize extremely high volume of automatic (last gaps) calls without unduly burden the dispatchers,

3.1 ADMS-SCADA

R[1] It is intended that the ADMS-SCADA be sized to support the following numbers of users.

Exhibit 3-1: Number of Users

		Concurrent users	
	Installed clients	Event	Day
ECC	10	8	5
BUCC	5	--	--
CE	2	2	2
SE	5	3	2
ITT	1	1	1
Trouble Shooters	1	1	1
Totals	24	15	11

R[2] The distribution system model shall be sized to represent the following:

Exhibit 3-2: Distribution System Model Sizing

Facility counts	2011	2015
Distribution Substations	73	80
Feeders	500	550
Airswitches	1,764	1,800
Remotely Controlled Airswitches	40	80
Disconnects	1,801	2,000
Sectionalizer	4	50
Capacitors	745	850
Remotely Controlled Capacitors	10	50
Recloser	50	75
Remotely Controlled Recloses	24	200
Regulator	11	30
Switch Gear	309	400
Primary Meter	159	400
Overhead Transformer	42,757	50,000
Pad Mount Transformers	34,285	40,000
Submersible Transformers	654	700
Line-monitors	4	30
AE Owned Poles	148,516	175,000
Telco owned poles	13,906	17,000
Line Fuses	5,727	8,000
Riser Fuses	7,799	9,000
Risers	14,136	17,000
Manholes	2,364	3,000
Pull boxes	33,772	40,000
Service boxes	51,487	60,000
OH primary conductor	2,370	2,750
OH secondary conductor	931	1,200
OH service conductor	1,513	1,750
OH streetlight conductor	661	750
UG primary conductor	2,898	3,500
UG secondary conductor	787	850
UG service conductor	1,509	1,600
UG streetlight conductor	650	700

Facility counts	2011	2015
Customer Meters	410,000	500,000
Customer Calls per hour (including AMI)	100	150
Max Customer Calls per hour	30,000	35,000

3.2 ADMS-SCADA Capacity

R[1] The ADMS-SCADA functions and their associated databases shall be dimensioned to support AE's 2015 requirements as defined in Exhibit 3 2: Distribution System Model.

R[2] ADMS-SCADA functions and their associated databases shall be architected to allow expansion in order to support anticipated future growth also defined in Exhibit 3 2: Distribution System Model.

R[3] The ADMS-SCADA functions and databases shall be capable of growing with AE's needs. Vendor shall state the total capacity limitations as part of their proposal.

R[4] Specific capacity requirements as follow:

R[4.A] *Processor Memory* – The main memory of each processor and workstation shall be expandable to twice the delivered capacity within the delivered enclosures by AE using hand tools and without replacing existing memory chips.

R[4.B] *Auxiliary Memory* – Fifty percent of the delivered auxiliary memory of each processor, workstation, or storage unit shall be unused (spare), and completely available for future use by AE.

R[4.B.i] The auxiliary memory of each processor, workstation, and storage unit shall be expandable to twice the delivered capacity within the delivered enclosures by AE using hand tools.

R[5] Auxiliary memory dedicated to IS&R data storage is exempted from the unused capacity requirement. (It is expected that this memory will be largely unused at delivery, as IS&R data will not be collected until the ADMS-SCADA is near to its commissioning date.)

R[6] This storage shall, however, satisfy the requirement for expansion to three times its delivered capacity within the delivered enclosures.

3.3 ADMS-SCADA Performance

R[1] Satisfaction of the performance requirements will be verified during both the factory test and the site test.

R[2] To this end, the ADMS-SCADA shall satisfy the performance and capacity requirement of this specification with up to eight physical workstations (four monitors each) and the interface to the Primate Video Wall Software.

R[3] The loading on the system introduced by additional workstations will be simulated.

3.3.1 ADMS-SCADA Activity Scenarios

R[1] The ADMS-SCADA performance shall be tested under the following activity scenarios:

R[1.A] The base conditions define ADMS-SCADA activities and conditions upon which the steady state and high activity scenarios are layered.

R[1.B] The steady-state scenario represents field operating conditions during a minor event over a 60-minute period.

R[1.C] The high-activity scenario represents field operating conditions during a 240-minute period such as might be experienced during a sever event.

R[1.D] The tests shall be designed such that each test run is repeatable as much as possible, so that the results between successive runs can be compared.

3.3.1.1 Base Conditions

R[1] The following conditions shall apply to both the steady-state and high-activity scenarios:

R[1.A] The ADMS-SCADA shall be configured with all hardware and functions required by this Specification operating, including hardware and functions specified as optional that have been selected by AE.

R[1.A.i] AE will determine the interfaces that will be tested during SAT.

R[1.B] All anti-virus and related software with all current patches installed and operational.

R[1.C] All ADMS-SCADA function execution parameters shall be as determined by mutual agreement between Vendor and AE.

R[1.D] The ADMS-SCADA software and databases shall be configured in accordance with the requirements of Appendixes B and C of the ADMS-SCADA Specification.

R[1.E] The contents of the ADMS-SCADA network model databases shall be an import of actual data from the AE data and the display and report definitions shall be as determined by AE.

R[1.E.i] The database contents will not be greater than the delivered capacity and the integrity of the data shall be agreed upon between Vendor and AE.

R[1.F] Each workstation (including operations, support, and management workstations) shall present all "common information" deemed by AE to be part of the normal display arrangement including, display title and window border, alarm zone, operator message area, time and date area, and top-level menu bar.

R[1.F.i]Common information that is part of the normal display shall be agreed upon between Vendor and AE before the start of pre-FAT.

R[1.G] Panning and zooming of the distribution graphical views shall be performed during the duration of the test as the users execute the various functions on the system.

R[1.H] Normal compliment of windowing capability

R[1.I] The test environment will mimic calls coming in from AECall

R[1.J] The test system will mimic web based status queries initiated from Storm Center

R[1.K] The test system will be running IVVC while executing the Steady State Scenario

R[1.L] The test system will be running Fault Isolation and Service Restoration during the execution of both the Steady State and the High Activity Scenarios

3.3.1.2 Steady-State Scenario

R[1] The Steady-State Scenario shall consist of the Base Conditions and the following activities over a sixty-minute period:

R[1.A] The system will be preloaded with 500 trouble calls

R[1.B] The system will be preloaded with 100 existing, predicted outages

R[1.C] A minimum of 250 new trouble calls coming into the system from the message queue evenly spread out over the duration of the test.

R[1.C.i] 15% of these not be associated with an existing outage

R[1.D] A minimum of 1000 new power outage reports from AMI 75% of these not be associated with an existing outage

R[1.E] A minimum of 90 web queries from SC

R[1.F] A total of 8 workstations will be logged in, capable of full ADMS-SCADA functionality

R[1.F.i]4 workstations staffed by AE personnel, performing the functions of a System Operator, running the Full Client, each logged into an area of responsibility covering 100% of the service territory, users will be executing test procedures consisting of:

R[1.F.i.a] Run Distribution Circuit Fault Location

R[1.F.i.b] Verify an outage

R[1.F.i.c] Assign a crew

R[1.F.i.d] Add a tag

R[1.F.i.e] Remove a tag

R[1.F.i.f] Restore an outage

R[1.F.i.g] Right size an outage (force upstream and downstream)

R[1.F.i.h] Dispatch and arriving crews

R[1.F.i.i] Enter estimated arrival times and restoration times

R[1.F.i.j] Close outage and non-outage events

R[1.F.i.k] Group and ungroup related events together

R[1.F.i.l] Assign un-located events to the correct location

R[1.F.i.m] Manually create switch orders

R[1.F.i.n] Automatically create switch orders

R[1.F.i.o] Run DPF

R[1.F.i.p] Execute switch orders

R[1.F.i.q] Place Cuts and Jumpers

R[1.F.ii] 4 workstations staffed by AE personnel performing the functions of System Engineering, each logged into an area of responsibility covering 100% of the service territory. Users will be executing test procedures consisting of:

R[1.F.ii.a] Running distribution power flow

R[1.F.ii.b] Performing Distribution Load Forecasts

R[1.F.ii.c] Running Integrated Volt/Var Control

R[1.F.ii.d] Administrative functions

R[1.G] One hundred restoration estimate inquiries from the AECall

R[1.H] Two sets of fault isolation and service restoration switching sequences requiring up to 10 separate controls each per staffed live user workstation.

R[1.I] Outage data capture for Storm Center updating every 15 minutes

3.3.1.3 High-Activity Scenario

R[1] The high-activity performance scenario shall consist of the base conditions and the following scenario for a 240-minute time period.

R[2] During this test, customer callback functionality shall be limited to calling back only those customers who have requested a callback:

- R[2.A] A minimum of 1,500 calls will be in the system at the start of the test
- R[2.B] A minimum of 200 orders will be in the system at the start of the test
  - R[2.B.i] 150 predicted to isolating devices (fuse, recloser, sectionalizer)
  - R[2.B.ii] 50 predicted to transformer
- R[2.C] A total of 50,000 geographically diverse new trouble calls shall be received over the test period. They shall be received in the following pattern sequence:
  - R[2.C.i] 30,000 during the First Hour
    - R[2.C.i.a] 28,000 from AMI
    - R[2.C.i.b] 2,000 from AECall
  - R[2.C.ii] 15,000 during the Second Hour
    - R[2.C.ii.a] 10,000 from AMI
    - R[2.C.ii.b] 5,000 from AECall
  - R[2.C.iii] 2,500 during the Third Hour
    - R[2.C.iii.a] 1,000 from AMI
    - R[2.C.iii.b] 1,500 from AECall
  - R[2.C.iv] 2,500 during the Fourth Hour
    - R[2.C.iv.a] 1,000 from AMI

R[2.C.iv.b] 1,500 from AECall

R[2.D] A total of 15 workstations will be logged in, capable of full ADMS-SCADA functionality

R[2.D.i] 8 workstations staffed by AE personnel, performing the functions of a System Operator, running the Full Client, each logged into an area of responsibility covering 100% of the service territory, users will be executing test procedures consisting of:

R[2.D.i.a] Verify an outage

R[2.D.i.b] Assign a crew

R[2.D.i.c] Add a tag

R[2.D.i.d] Remove a tag

R[2.D.i.e] Restore an outage

R[2.D.i.f] Right size an outage (force upstream and downstream)

R[2.D.i.g] Dispatch and arriving crews

R[2.D.i.h] Enter estimated arrival times and restoration times

R[2.D.i.i] Close outage and non-outage events

R[2.D.i.j] Group and ungroup related events together

R[2.D.i.k] Assign un-located events to the correct location

R[2.D.i.l] Running Distribution Circuit Fault Location

R[2.D.i.m] Running Fault Isolation and Service Restoration

R[2.D.i.n] Manually create and execute switch orders

R[2.D.i.o] Automatically create and execute switch orders

R[2.D.i.p] Place Cuts and Jumpers

R[2.D.ii] 7 workstations staffed by AE personnel performing the functions of System Engineering, each logged into an area of responsibility covering 100% of the service territory. Users will be executing test procedures consisting of:

R[2.D.ii.a] Running distribution power flow

R[2.D.ii.b] Performing Distribution Load Forecasts

R[2.D.ii.c] Running Integrated Volt/Var Control

R[2.D.ii.d] Administrative functions

R[2.E] Over the duration of this scenario restoration estimate inquiries from AECall will be spread evenly over the hour.

R[2.E.i] First Hour 2,000 inquiries

R[2.E.ii] Second Hour 5,000 inquiries

R[2.E.iii] Third Hour 1,500 inquiries

R[2.E.iv] Fourth Hour 1,500 inquiries

R[2.F] Five data entries shall occur at each operating workstation every minute.

R[2.G] Outage data capture for Storm Center updating every 30 minutes

3.3.1.4 Degraded Operation

R[1] AE expects that the ADMS-SCADA will infrequently experience operating conditions beyond those embodied in the high-activity scenario.

R[2] The ADMS-SCADA shall continue to operate under such conditions and may exhibit degraded performance under such conditions.

R[3] However, the ADMS-SCADA shall include features to minimize the degradation and the ensuing effects on power system operations.

R[4] The ADMS-SCADA shall be configured to give priority to the following when operating in a degraded state:

R[4.A] Issuing Operator-initiated controls to field devices

R[4.B] Detecting and annunciating exception conditions (alarms) in the power system

R[4.C] Presenting data to the users through the workstations – priority shall be given to users at operating workstations

R[4.D] Maintaining coherency of the database – specifically including data used as inputs to functions and the outputs produced by the functions

R[5] Any actions taken by the ADMS-SCADA to mitigate degraded operating conditions shall be alarmed to the users.

3.3.2 Resource Utilization

R[1] Utilization is defined as the average utilization over the time of the test scenario and shall be calculated as the used capacity of the resource divided by the total available capacity of the resource.

R[2] For example, processor average utilization may be calculated as busy time divided by total time.

R[3] LAN average utilization may be calculated as the quantity of data transferred (Mbytes) divided by the LAN data rate (Mbytes/second) multiplied by total time (seconds).

R[4] The ADMS-SCADA shall meet the following:

R[4.A] Steady State Utilization - The average resource utilization of each ADMS-SCADA resource during the steady state scenario shall not exceed:

R[4.A.i] Utilization of the processing capacity of any processor used for executing application functions shall not exceed 35%.

R[4.A.ii] Utilization of the transfer capacity of each auxiliary memory device shall not exceed 30%.

R[4.A.iii] Utilization of any non-deterministic LAN (such as Ethernet) shall not exceed 5%; the loading of any deterministic LAN shall not exceed 10%.

R[4.B] High Activity State Utilization – The average resource utilization of each ADMS-SCADA resource during the high activity scenario shall not exceed:

R[4.B.i] Utilization of the processing capacity of any processor used for executing application functions shall not exceed 40%.

R[4.B.ii] Utilization of the transfer capacity of each auxiliary memory device shall not exceed 40%.

R[4.B.iii] Utilization of any non-deterministic LAN (e.g., Ethernet) shall not exceed 10%; the loading of any deterministic LAN shall not exceed 25%.

3.3.3 User Interface Response

R[1] The ADMS-SCADA shall provide rapid and consistent response to power system events and user inputs.

R[2] Responsiveness to events and inputs shall be within the following requirements under both the steady state and high activity scenarios.

R[3] User Interface response times shall conform to the requirements shown in Exhibit 3-3.

3.3.3.1 Display Request

R[1] The display response time is defined as the elapsed time from a user's request for a display until the requested display is presented complete with current data retrieved from the ADMS-SCADA databases.

R[2] Display response times shall be demonstrated for the ADMS-SCADA operating in the steady state and the high activity scenarios.

R[3] The display response time for each request shall conform to the display response time requirements shown in Exhibit 3-3, User Interface Response.

3.3.3.2 User Requests

R[1] The response to user requests shall be measured from the time the user completes all information necessary to define the request or any step of a sequence that makes a request, until the time the requested action is completed.

R[2] Completion of the request shall include production of all results, storage of the results in the ADMS-SCADA database, and updating of all relevant displays.

R[3] The default response time shall be met for all other user requests not specifically included in this RFP.

3.3.4 Resource Monitoring

R[1] Resource utilization shall be measured, calculated and displayed for the ADMS-SCADA processors, devices, and networks.

R[2] The minimum set of parameters to be presented includes:

R[2.A] Time utilization (percent processor utilization) of each function per processor

R[2.B] Time utilization (percent disk utilization) of each function per disk

R[2.C] Disk data transfers per disk

R[2.D] Utilization of memory and disk

R[2.E] Performance of LANs, bridges, routers, switches, firewalls and other network devices.

R[2.E.i] All active network elements shall respond to RMON (groups 1-5, 9 as a minimum) and SNMP level 1 data requests

R[3] Statistical sampling and accumulation techniques shall be used to collect these parameters over a user-selected time period.

R[4] Typical study periods shall be ten seconds to sixty minutes, and typical sampling frequencies shall be once per fifty milliseconds.

Exhibit 3-3: User Interface Response

Action	Maximum Response Time (For Local/WAN)		Notes
	Steady State	High Activity	
Default response	1/2 second	1.5/3 seconds	98% of actions complete within the maximum time. 100% within 1.5 times the maximum.
Display request	1/2 seconds	2/3 seconds	98% of actions complete within the maximum time. 100% within 1.5 times the maximum.
Distribution Circuit schematic display callup	2/5 seconds	3/6 seconds	98% of the actions complete within the maximum time. 100% within 1.5 times the maximum.
IS&R display requests	2/4 seconds	4/6 seconds	98% of actions complete within the maximum time. 100% within 1.5 times the maximum.
Display data update (subsequent to the initial presentation of data)	1/1 seconds	1/1 seconds	˜ 4 second periodicity (time shall be updated at a 1 second periodicity) ˜ 98% of actions complete within the maximum time. 100% within 1.5 times the maximum.
Alarm and event annunciation	1/2 second	1.5/3 seconds	98% of actions complete within the maximum time. 100% within 1.5 times the maximum.
Viewport creation	1/1 second	1.5/1.5 seconds	98% of actions complete within the maximum time. 100% within 1.5 times the maximum.
World-map panning	5/5, 20-pixel steps per second	5/5, 20-pixel steps per second	No visible flicker.
World-map zooming	2/2, 10% steps per second	2/2, 10% steps per second	No visible flicker.
Pop-up menu, pull down menu, dialog box, etc.	1/2 second	1.5/3 seconds	Not to exceed 150% of the maximum under any condition
Display hardcopy	10/10 seconds	15/15 seconds	98% of actions complete within the maximum time. 100% within 1.5 times the maximum.
Workstation user logon	10/10 seconds	10/10 seconds	98% of actions complete within the maximum time. 100% within 1.5 times the maximum.

R[1] UI Workstation Connections:

R[1.A] Local = connected on ADMS-SCADA LAN (e.g. workstations on ECS, QAS, OTS and PDS) WAN = workstation in control room located at a site other than ECS

R[2] Note: The above user interface response requirements are based on the required bandwidth and latency defined by the Vendor for each workstation type and supplied by the Vendor or AE as defined in this Specification.

R[3] Note 2: The above response times require that samples are taken at even intervals over the testing period.

Exhibit 3-4: Function Periodicity and Execution Time

Function	Periodicity	Maximum Execution Time		Notes
		Steady State	High Activity	
Data Acquisition (any data source)	Sizing Tables in Appendix B	1 second	1 second	Execution time is measured from the receipt of the message containing the changed data until all processing is complete, the changed data is stored in the database, and the alarm lists have been updated.
Supervisory Control	-	1 second	1second	Execution time is measured from the time the user executes the command until the command exchange with the data source is complete.
IS & R Alarms & Events	Sizing Tables in Appendix B & C & D	As occurring	As occurring	All alarms & events transferred to Historian
DMS Functions	-			
Distribution Power Flow	-	10 seconds	20 seconds	Entire DSOM
Distribution Fault Location		2 seconds	3 seconds	Entire DSOM
Fault Isolation and Service Restoration	-	3 seconds	5 seconds	Entire DSOM
VAR Control	60 seconds	2 seconds	3 seconds	Entire DSOM

Function	Periodicity	Maximum Execution Time		Notes
		Steady State	High Activity	
Insert cuts and jumpers	30 minutes	1 second	2 seconds	The time from the user executes the command until the time the system has installed a jumper and reconfigured the connectivity
Independent System Health Monitor Monitor Function Analysis	 10 seconds Multiple of monitor	 10 seconds	 10 seconds	 Or more frequent if triggered Configurable multiple
Outage related functions Predictions Engine Operator Actions -Push outage up/ down - close out order Calculate Parameters for Reliability Performance	Continuous 30 seconds As requested Hourly	 10 seconds 2 seconds -	 20 seconds 3 seconds -	 On event/call occurrence with configurable delay - Distribution service reliability statistics and daily reports

Exhibit 3-5: Configuration Management Performance

Action	Performance	RFP Reference
Backup (Redundant Standby) Database Update User entries	Updated on occurrence of manual initiation	Section 2.3.1.3
ECS Database Update User entries OMS Historical database	Updated on occurrence Updated within 2 minutes.	Section 2.3.1.3
Detection and annunciation of processor or device failure and initiation of restart/failover process	Within 10 seconds	Section 2.3.1.4
Function restart/processor failover Restart/failover at same control center	Within 30 seconds	Section 2.3.1.5

Action	Performance	RFP Reference
Recovery from communications failure LAN or WAN failure	Within 10 seconds	Section 2.3.1.6
Device failover	Within 10 seconds	Section 2.3.1.6
Complete System startup (from power-off condition)	Complete, with all functions scheduled for execution, within 20 minutes	Section 2.3.1.5
Processor startup	Complete, with all functions scheduled for execution, within 10 minutes	Section 2.3.1.5

Exhibit 3-6: Software Maintenance

Action	Performance	Reference
Complete database regeneration (1)	2 hours	Section 2.2.6
Incremental Database Update (Typical) (2)	30 minutes	Section 2.2.6
Complete system software build, including operating system, applications, and databases	6 hours	Sections 2.2.6
Software build or all applications and databases	3 hours	Sections 2.2.6
Software build of a single applications and databases	30 minutes	Section 2.2.6
Installation of a single, new display including distribution to all workstations	60 seconds	Section 2.2.6
Reinstallation of all displays	60 minutes	Section 2.2.6
On-line update of a database parameter and propagation of the change to the source data	60 seconds	Section 2.2.6

Table of Contents

4. User Interface 4-1
  4.1 User Interface General Features 4-2
    4.1.1 Display Selection 4-3
    4.1.2 List Displays..4-4
    4.1.3 Scaling and Translation 4-4
    4.1.4 Supervisory Control Initiation..4-5
    4.1.5 Data Entry..4-6
    4.1.6 User Control Action and Operator Action Recording 4-7
    4.1.7 Interlocks 4-8
    4.1.8 Sticky Notes...4-8
    4.1.9 Inactivity Timeout..4-8
    4.1.10 User Guidance..4-8
    4.1.11 User Help...4-9
    4.1.12 Display Hardcopy...4-10
  4.2 ADMS-SCADA Access Security 4-10
    4.2.1 User Login 4-10
    4.2.2 Remote User Access 4-11
    4.2.3 Access Security Management 4-12
      4.2.3.1 Access Attempt Recording 4-12
      4.2.3.2 Access Attempt Alerting 4-13
    4.2.4 Operating Permissions & Areas of Responsibility 4-13
  4.3 Alarm, Event or Off-Normal Processing 4-14
    4.3.1 Alarm Priority 4-16
    4.3.2 Alarm Class and Alarm Presentation...4-16
    4.3.3 Alarm Messages 4-17
    4.3.4 Alarm Window...4-18
    4.3.5 Alarm, Event and Off-Normal Summary Displays.......................................4-19
      4.3.5.1 Alarm Summary 4-19
      4.3.5.2 Event Summary 4-20
      4.3.5.3 Off-Normal Summary...4-21
    4.3.6 Alarm Acknowledgement 4-22
    4.3.7 Alarm Deletion 4-23

Table of Contents

4.3.8 Alarm Inhibit and Enable 4-24
4.3.9 Alarm Audible Silencing and Suppression 4-24
4.3.10 Alarm Help 4-25
4.3.11 Complex Alarming Functions 4-26
4.3.12 Enhanced Alarm Management 4-26
4.4 Trending 4-27
4.5 User Interface Development 4-28
4.5.1 Display Style 4-28
4.5.2 Display Elements 4-29
4.5.2.1 Data Presentation 4-29
4.5.2.2 Quality Code and Safety Tag Presentation 4-31
4.5.2.3 Data Sets 4-32
4.5.2.4 Display Layers 4-33
4.5.2.5 User Interaction 4-34
4.6 AE-Provided Displays 4-35
4.7 Vendor-Provided Displays 4-36

4. User Interface

R[1] The principal interface between the user and the ADMS-SCADA will be a single HMI client.

R[2] Printing devices will be part of the interface between the users and the ADMS-SCADA.

R[3] The ADMS-SCADA shall be fully compatible with the Primate Video Wall software.

R[4] Additional User Interface requirements to support the distribution system operations are defined in Section 13.1.

R[5] Austin Energy requires a User Interface that limits the number of steps that the Operator will be required to execute to achieve the desired results.

R[6] An informative context sensitive help system shall be available to be used by new dispatchers or when performing infrequent operations.

R[7] It is desirable that no single action take more than 3 (three) mouse clicks.

R[8] AE requires that the ADMS-SCADA have a single HMI, presenting a common appearance and consistent functionality to the user for all functions to be performed.

R[9] AE requires that the user will have the ability to access any of the ADMS-SCADA Systems (ECS Prod 1 or Prod 2, QAS, PDS, OTS from any AMDS workstation.

R[10] AE requires that all ADMS-SCADA workstations shall be able to accommodate MS Office applications in addition to their ADMS-SCADA responsibilities.

R[11] However, MS Outlook will not be installed on the ADMS-SCADA workstations.

R[12] The ADMS-SCADA shall have the ability to export results into Excel spreadsheets and XML-CIM files.

R[13] Ability to cut an paste numerical information into a spreadsheet to perform calculations in order to verify ADMS-SCADA results.

R[14] Support Data Engineering and Display Engineering activities.

R[15] Support CIM.

4.1 User Interface General Features

R[1] The following features shall be included in the ADMS-SCADA user interface.

R[2] Alternatives may be offered, but must be functionally equivalent to the features specified.

R[3] The user interface shall include the following common elements on each workstation, screen, or display (as required).

R[4] The user interface shall be capable of displaying alarms in in accordance with priority and group of responsibility.

R[5] The user interface hall be able to display alarm colors and to produce alarm associated sounds.

R[6] Alarms system shall allow for sorting and filtering alarms by any of its attributes. The results of such actions shall be capable of been saved in an Excel spreadsheet.

R[7] The user interface shall conform to MS Windows standards for the presentation of content. The Vendors shall include additionally the following:

R[7.A] A heading at the top of each user-defined window consisting of the unabbreviated name of the display, the abbreviated display call-up name, and, on multi-page displays, a page number in the form Page N of M.

R[7.B] A navigation aid for each display that is larger than the window in which it is presented.

R[7.B.i] The navigation aid shall be a condensed map of the full display. Highlighting within the condensed display shall indicate the portion of the display that is currently presented.

R[7.B.ii] The user shall be able to move, resize, and close the navigation aid.

R[7.C] Provide context sensitive user help.

R[7.D] An indication of the ADMS-SCADA component system the user is connected to (e.g., QAS, OTS, PPS, SPS) and the application being viewed (e.g., real-time SCADA, other application).

4.1.1 Display Selection

R[1] Rapid, convenient, and reliable selection of displays shall be provided using the following methods:

R[1.A] From a menu display.

R[1.B] Cursor target operation on any menu, graphic, or tabular display.

R[1.C] Selection of an alarm on an alarm summary or the alarm window followed by a display request command.

R[1.D] Entry of an alphanumeric display name or display number in a display select field.

R[1.D.i] The ADMS-SCADA shall provide the capability for a User to type in a partial name, including wild card characters, and shall show a list of displays meeting the criteria for selection.

R[1.D.ii] This predictive menu feature shall show those options that match the characters typed by the user, narrowing the set of matching displays as more characters are entered.

R[1.D.iii] Character matching shall not be case sensitive.

R[1.E] Forward and reverse paging through a series of displays.

R[1.E.i] Paging forward from a display's last page of a series shall present the display's first page.

R[1.E.ii] Paging backward from a display's first page of a series shall present the display's last page.

R[1.F] Operating a display recall cursor target in a window.

R[1.G] Selection of a manual refresh target/softkey to recall a display with current values

R[1.H] Selection of an analog or status point device number/name to be presented with a menu of displays that contain the point, for further selection and navigation to the desired display

R[1.I] Selection of a historical data display to present historian data on an ADMS-SCADA display (Section 7.1.5)

R[2] The user shall be provided with window selection techniques to independently direct a display to any window of the workstation.

4.1.2 List Displays

R[1] Certain displays will present data in a tabular format consisting largely of rows of similar entries.

R[2] The ADMS-SCADA shall support the following techniques for moving through the data presented on list displays:

R[2.A] Scrolling via slider bars.

R[2.B] Page up and down

R[2.C] Entry of a page number.

R[2.D] Entry of an alphanumeric search string

R[3] Paged displays shall include a “page N of M” message on each page of the display.

R[4] Empty pages – pages with no entries – shall be removed from the paging sequence.

4.1.3 Scaling and Translation

R[1] The user shall be able to scale (zoom) the image of a world coordinate space or other display in a smooth fashion.

R[2] The scale factors shall allow the presentation of an entire world coordinate space or other display on the full screen or a window.

R[3] Static and dynamic data shall be displayed and updated during a scaling operation, and display text shall be scaled to be consistent with the scaled image.

R[4] At defined scale factors, levels of declutter shall be invoked.

R[5] The user shall be able to select an area of a world coordinate display by cursor manipulation (“rubber-banding”) and cause the display to be redrawn with the selected area centered in the display and with the selected area magnified to best fit the full window.

R[6] The user shall be able to translate (pan) the display image to permit the observation of other portions of a display within a selected window.

R[7] Static and dynamic data shall be displayed and updated during a translation operation.

R[8] The user shall be able to define a display with a name and a particular focus area for initial call up of a world coordinate display, such that the focus will define the zoom level and translation area to be initially displayed.

R[9] This function shall allow multiple displays with unique names, each with a different initial focus area.

4.1.4 Supervisory Control Initiation

R[1] Any telemetry controlled object can be operated from any appearance of the object, including lists, tabular, schematic, graphical, etc.

R[2] Supervisory control actions shall be initiated through dialog that shall pop-up in the active window on the same screen and present commands dependent on the type of element to be controlled.

R[3] The dialog box to exert telemetry control shall display the Object ID of the data item selected and have a distinct presentation to distinguish it from non-telemetry control type boxes.

R[4] As the final step of the supervisory control process, the selected device shall be highlighted on the display and the user shall be presented with a clear description of the device to be controlled and the specific command to be issued and shall be required to confirm the command (“execute”) or terminate the command (“cancel”).

R[5] If the user does not complete or cancel the operation within a configurable time period, the ADMS-SCADA shall perform an Inactivity Timeout (4.1.9).

R[6] The ADMS-SCADA shall issue the command to the end device only after the user confirms the operation.

R[7] The supervisory control procedure shall support the control permissive check and other control interlock requirements described.

R[8] The supervisory control dialog box shall not cover the area of the display showing the data point selected for control.

R[9] A log shall be kept including all supervisory control operations performed by individual dispatchers, including alarm acknowledgement.

4.1.5 Data Entry

R[1] User entry of data shall be facilitated by simple procedures to select the point or points to be entered, enter the value or values, validate the changes, and to confirm or cancel the entry.

R[2] Data entry may use full window or single point techniques as appropriate. Data entry shall support multi-state devices as defined in Section 6.5.

R[3] The ADMS-SCADA shall perform any validity checks appropriate to the affected points. If there are no invalid entries, the new values shall be written to the database.

R[4] The ADMS-SCADA shall retain a copy of all changed data (e.g., safety tags, manually replaced, etc.) so that the data can be retained on a cold start or incorporated into a new database, at the option of the user.

R[5] If there are invalid entries, the invalid entries shall be highlighted and the user presented with the option of correcting the entries or accepting only the valid entries.

R[6] Single-point data entry shall be initiated by selecting the point to be entered and commanding the data entry mode.

R[7] The selected device shall be highlighted on the display.

R[8] Only the selected point shall be placed in the data entry mode.

R[9] The user interface shall allow the data entry to be confirmed using the enter key on the keyboard.

R[10] If the user does not complete or cancel the operation within a configurable time period, the ADMS-SCADA shall perform an Inactivity Timeout (Section 4.1.9).

R[11] The data entry dialog box shall not cover the area of the display showing the data point selected for data entry.

R[12] The dialog box shall display the Object ID.

R[13] A log shall be kept including all data entry performed by individual dispatchers.

4.1.6 User Control Action and Operator Action Recording

R[1] All user actions that change ADMS-SCADA data or operating conditions (e.g., data entries, alarm actions, data-source actions) shall be recorded as events.

R[2] Actions that request displays or modify their presentation, such as scaling, translation, paging, scrolling, relocating windows, and resizing windows do not need to be recorded as events.

R[3] Events shall include execution of distribution system network analysis functions in the study mode, including data setup, execution setup, and actual execution.

R[4] In addition, safety tagging entry and modification shall record all information changed or entered.

R[5] Each event record shall include the following information:

R[5.A] the login identity (user) and workstation of the user

R[5.B] the time and date of the action

R[5.C] a complete identification of the database point affected

R[5.D] a clear (non-coded) description of the action and the value, state, or condition of the item changed before and after the action

R[5.E] A log shall be kept including all control actions performed by individual dispatchers.

4.1.7 Interlocks

R[1] Data entry for an object shall be restricted so that multiple users will not produce conflicting actions on a given value. If an object is under the control of one user, an attempt to initiate the data entry function for that object by another user shall result in rejection of the second attempt to enter the data entry mode and the second user shall be informed of the conflict.

R[2] Similarly, control of a power system device, management of a single point, and data entry shall only be allowed from one window at one workstation at a time.

4.1.8 Sticky Notes

R[1] Users shall be able to define and place sticky notes that contain free-form text and graphics in a map window.

R[2] A unique icon or indicator shall be provided that will visually highlight to the user that a sticky note has been placed and shall be visible at defined declutter levels.

4.1.9 Inactivity Timeout

R[1] If a user does not complete a step within a multi-step operation within a pre-defined time, the process shall reset, and the user shall be informed of the reset.

R[2] User timeouts shall be configurable by type of user operation.

4.1.10 User Guidance

R[1] The ADMS-SCADA shall respond to all user actions indicating whether the action was accepted, was not accepted, or is pending.

R[2] For multi-step procedures, the ADMS-SCADA shall provide feedback at each step. Indications such as text messages, color changes, and blinking shall provide this feedback.

4.1.11 User Help

R[1] General and specific context-sensitive on-line help shall be available to the ADMS-SCADA user. Access to user help shall be available by:

R[1.A] A Help command on the window menu bar.

R[1.B] A Help button in a dialog box.

R[1.C] Topics from a Help menu.

R[2] The Help menu shall present a list of topics available for reference.

R[3] The topics shall refer to the ADMS-SCADA user documents.

R[4] The ability to scroll through the topic's explanatory text shall be supported.

R[5] The Help button in a dialog box shall present the text of the ADMS-SCADA user documents where use of the dialog box is explained.

R[6] The user shall be able to scroll through this text. Exit from the help facility shall return the user to the same point in the sequence for which help was requested.

R[7] Context-sensitive help facilities shall be provided for each application software package and the database fields.

R[8] The capability to easily edit or add additional help facilities in the future shall be provided.

R[9] Access to areas of User help shall be restricted by display permission.

R[10] User help files shall not be altered or lost when the ADMS-SCADA, or any portion of the ADMS-SCADA, is upgraded.

4.1.12 Display Hardcopy

R[1] The ADMS-SCADA shall print a copy of a window or the entire visible monitor view on any workstation when commanded by a user.

R[2] The output shall be directed to a printer of the user's choice.

R[3] Color displays shall be translated to gray scale for black and white printers using a mapping table (or other, similar technique) that can be changed by the user.

R[4] The ADMS-SCADA shall include a user selectable option to print with inverse colors, for printing of displays with dark backgrounds.

R[5] The display output shall be sized to fit on a single page and shall include the date and time of the display printout.

R[6] The display hardcopy function shall not inhibit the workstation from normal operation after a copy is requested, even when multiple users issue simultaneous hardcopy requests.

R[7] The ADMS-SCADA shall also include a user selectable option to print the entire contents of a multi-page display.

R[8] Also, the ability to redirect the printout to an electronic form/copy shall be provided in standard file types (e.g., gif, pdf), to allow display contents to be saved, distributed to others (outbound email only), and used for after-the-fact analysis.

4.2 ADMS-SCADA Access Security

R[1] A mechanism for defining and controlling user access to the ADMS-SCADA shall be provided.

R[2] Even though a user has logged onto the ADMS-SCADA network or a processor, access to the ADMS-SCADA functionality shall be subject to these additional security checks.

4.2.1 User Login

R[1] Password security shall be provided for access to the ADMS-SCADA.

R[2] The ADMS-SCADA shall include a redundant pair of LDAP servers at both ECS locations with Active Directory single sign-on capability to simplify the AE password maintenance and control process and user sign-on process across the full suite of ADMS-SCADA applications and servers.

R[3] This facility shall allow the administrator to request a report of users, to be used to periodically compare to the AE corporate users/employee information.

R[4] The report shall include, as a minimum: employee name, an invariant key to uniquely identify each user, employee ID, freeform text and other user permission information.

R[5] Users shall log in by entering a user ID and a password.

R[6] Each password shall be validated against the corresponding user information stored in the database.

R[7] A procedure shall be provided for users to log off.

R[8] ADMS-SCADA user IDs and passwords shall be encrypted at the workstations and transmitted over the network using secure communications techniques (e.g., ssh or ssl) and stored in encrypted form.

R[9] The ADMS-SCADA shall enforce configurable password construction rules as defined in Section 12.17, Authentication Methods and Password Construction.

R[10] Each of the password rules shall be configurable by AE, including the ability to enable or disable each rule individually.

R[11] Users shall be able to change their own passwords.

R[12] Changed passwords shall be propagated throughout the ADMS-SCADA as necessary and without additional user intervention.

4.2.2 Remote User Access

R[1] AE currently does not intend to provide remote web-based user access to the ADMS-SCADA.

R[2] However, AE is interested to see what capabilities the Vendors offer.

4.2.3 Access Security Management

R[1] The cyber security features shall be consistent across all ADMS-SCADA applications and services and security shall be managed as a single service for all component systems of the ADMS-SCADA, including the ECS Prod 1, ECS Prod 2, IS&R system, OTS, PDS, and QAS.

R[2] The use of generic accounts shall be minimized.

R[3] All accounts shall require an interactive login.

R[4] The login for Operators shall prevent access to operating systems in all UNIX-based servers.

R[5] For Windows-based processors, the Operators shall not be able to modify the UI environment and associated directories.

4.2.3.1 Access Attempt Recording

R[1] The ADMS-SCADA shall log all attempts to access the ADMS-SCADA with all pertinent information such as IP address, workstation identifier, etc., both at the application level and at the "infrastructure" (operating system and application support software) level including:

R[1.A] All attempts to log on, whether successful or unsuccessful. A user shall be allowed to login at multiple workstation locations simultaneously

R[1.B] All changes to privileges assigned to users.

R[1.C] All user actions affecting security, such as changing passwords.

R[1.D] Attempts to access a file for which the user has no access privileges.

R[1.E] Attempts to perform an action not authorized by the security scheme.

R[2] The log entries shall also be written to AE's existing RSA Envision log server.

4.2.3.2 Access Attempt Alerting

R[1] The ADMS-SCADA shall generate an alarm when access activity may be indicative of attempts to obtain unauthorized access to system services or data.

R[2] A simple method shall be provided for the user to view and to change the rules for generating alarms.

R[3] Initially, an alarm shall be generated when the system detects any of the following activities:

R[3.A] Repeated attempts to log in from a specific workstation or external port.

R[3.A.i] Multiple unsuccessful attempts to login shall be detected and the ADMS-SCADA shall include a configurable option to lock out a user when this is detected.

R[3.B] Repeated failed attempts at file access.

R[3.C] Port scans (attempts to access closed ports or services).

R[3.D] Unusual levels of traffic on the local area network.

4.2.4 Operating Permissions & Areas of Responsibility

R[1] Once logged on, access to the ADMS-SCADA capabilities shall be managed by assigning a set of Areas of Responsibilities (AORs) to individual user accounts.

R[2] There shall be no restrictions on the assignment of multiple AORs to a user or the assignment of an AOR to multiple multiple users.

R[3] User Permissions shall be created by assignment of AORs to a user and definition of the level of permission as either read-only, read/write, super-user (controlling program tuning and execution parameters), or maintenance permission level.

R[4] Read-only access shall preclude user interaction with the display other than to request another display.

R[5] Read/write access shall allow full interaction with the display, subject to function, database, and supervisory control jurisdiction assignments.

R[6] Access to a display, function, data item, or control data item shall be determined by the user permissions to obtain the allowed permission levels that are allowed for a particular user instance.

R[7] Management of User Permissions and AORs shall be a function subject to AOR validation.

R[8] A set of displays shall be provided to allow the authorized individual (e.g., supervisor) to control the AOR assignments and to make adjustments as operating conditions change. For example, these displays shall allow the supervisor to redistribute assigned AORs due to a storm situation, where additional staff are used and responsibilities are shifted (e.g., during evenings, when an Operator might assume responsibility for multiple areas due to decreased staffing during night-time shifts).

R[9] The access security function shall ensure that each AOR is at all times assigned to at least one user.

R[10] If a workstation failure or manual reassignment of AOR results in one or more AORs not being assigned to at least one user, the unassigned AORs shall be automatically assigned to a user assigned to an adjacent AOR. The newly assigned user will be notified and suitable alarms shall be generated.

4.3 Alarm, Event or Off-Normal Processing

R[1] Alarms may be generated by any ADMS-SCADA function, including the processor and device failure detection functions.

R[2] Alarms, when initially detected, shall be marked as “unacknowledged”.

R[3] Users will indicate that they have taken action on the alarm by acknowledging the alarm.

R[4] Events are conditions that are to be recorded by the ADMS-SCADA, but that do not require annunciation to or action by users.

R[5] Events may be generated by the same functions as alarms.

R[6] All alarms shall also be included on the event summary display for record keeping purposes.

R[7] The system Alarm facility shall be implemented using techniques to ensure the high performance characteristics required of this key feature

R[8] The Off-Normal condition represents devices that are in a state other than their defined normal state.

R[9] The ADMS-SCADA shall provide that ability to define a normal state for each device in the system (not all devices will have a normal state defined).

R[10] Based on that definition, the ADMS-SCADA will determine when a device is in an Off-Normal state.

R[11] Alarms shall be subjected to a series of alarm processing actions and user interactions.

R[12] Those actions to be executed shall be determined by the jurisdiction assigned to that database item that is exhibiting the alarm condition, the alarm priority, and by the alarm class also assigned to the database item.

R[13] Each database item may be associated with several alarms.

R[14] For example, a telemetered analog point will include operating limit alarms, reasonability limit alarms, and telemetry failure alarms.

R[15] Each alarm of each point shall be individually assigned to an AOR and to an alarm class.

R[16] Each database item shall also allow multiple alarms to be issued to other AORs (e.g., via the capability to assign a data item to a composite AOR that can issue multiple alarms based on a single event or via the capability to assign a data item to multiple AORs).

R[17] When selected for multiple alarms, the database item shall allow entry of other alarm classes and alarm priorities.

R[18] When a point selected for this feature changes state multiple alarms shall be issued, displayed, and managed independently.

R[19] This shall include generation of independent alarms for each AOR, event messages for each AOR, separate event messages for operator actions on the alarms (acknowledge, delete, alarm inhibit/enable, etc.) and separate storage of these messages in IS&R.

R[20] One alarm shall be issued to the base AOR assigned to the point and other alarms to the other assigned AORs.

4.3.1 Alarm Priority

R[1] Each alarm shall be assigned an alarm priority.

R[2] This alarm priority shall be used by the ADMS-SCADA to determine the content of the Alarm Window and Alarm Summary display viewed by the Operator.

4.3.2 Alarm Class and Alarm Presentation

R[1] Each alarm shall be assigned to a single alarm class that determines how the following alarm presentation and management characteristics are to be employed:

R[1.A] Audible annunciation – no audible alarm, single stroke or repeating, and which tone is to be sounded.

R[1.A.i] Use of standard sound files shall be supported (e.g., .wav, .mpg, etc.).

R[1.A.ii] The tones shall be configurable with options including: sound once, sound 2-3 times then stop, continuous sound until acknowledged/silenced, unique sounds for specific workstations, option for audible independent of AOR assignment, etc.

R[1.B] Display presentation:

R[1.B.i] For one-line and tabular displays diagrams – symbol change, color change, or no change, and flash/no flash for both unacknowledged and acknowledged alarms

R[1.B.ii] For message displays (such as an alarm summary) – message color and flash/no flash with support for a different message color for normal or abnormal states.

R[1.B.iii] Please note that an indicator in the alarm message, not the entire alarm message, shall flash to allow the Operator to read the content of the alarm message

R[1.C] Inclusion on or exclusion from the alarm window

R[1.D] Inclusion on or exclusion from the alarm summary

R[1.E] Alarm management (acknowledge and delete):

R[1.E.i] None required (for events).

R[1.E.ii] Acknowledgement is required before deletion.

R[1.E.ii.a] Manual deletion (user action) is required.

or

R[1.E.ii.b] The alarms are deleted when the return-to-normal alarm for the point is acknowledged.

or

R[1.E.ii.c] The alarms are deleted when the alarm is acknowledged.

R[1.E.iii] Acknowledgement is not required before deletion. Unacknowledged alarms may be deleted.

R[1.E.iii.a] Manual deletion (user action) is required.

or

R[1.E.iii.b] The alarms are deleted when the return-to-normal alarm for the point is acknowledged.

R[1.E.iv] Deletion is not allowed when the point is in an abnormal state (configurable on a per point basis)

4.3.3 Alarm Messages

R[1] Alarm messages shall be a single line of text describing the alarm that has occurred. Each alarm message shall include:

R[1.A] The time and date of the alarm. (Alarms from previous days shall be clearly identified).

R[1.B] A complete identification of the database point.

R[1.C] A clear (non-coded) description of the alarm.

R[1.D] The state of the item after the alarm detection.

R[1.E] The limit value and the data value at the time of the alarm detection, for analog data.

R[2] The alarm message shall be unabbreviated English text and shall not require the use of a reference document for interpretation.

R[3] Any alarm message components that are abbreviated shall be subject to approval by AE. AE shall be able to modify alarm message formats and define new formats.

4.3.4 Alarm Window

R[1] The alarm window shall provide a visual indication of alarm conditions in every AOR assigned to the workstation.

R[2] The alarm window shall contain an indicator for each data source and ADMS-SCADA function. When an unacknowledged alarm is present in any data source or function, the indicator shall be displayed and flashing, color, or other highlighting shall be used to draw the user's attention to the indicator.

R[3] Acknowledgement of the alarm shall modify the attributes of the indicator to indicate the presence of only unacknowledged alarms.

R[4] If the number of indicators exceeds the capacity of the alarm window, the user shall be notified of the overflow condition.

R[5] The Operator shall select the indicator to display the appropriate alarm summary page that contains the data point in alarm.

R[6] The Alarm Window and Alarm Summary shall be configurable to allow different characteristics of the Window and Summary, such as: the number of alarms displayed in the window, the size of the window, the display order (forward or reverse chronological order), the alarm displayed in the window (newest, oldest unacknowledged), and other key characteristics.

4.3.5 Alarm, Event and Off-Normal Summary Displays

R[1] The ADMS-SCADA shall include alarm and event summary displays.

R[2] These displays shall exhibit all of the general summary display characteristics described in Section 4.7, Vendor Provided Displays; Summary Displays and shall function as described below.

4.3.5.1 Alarm Summary

R[1] The ADMS-SCADA shall include Alarm Summary displays that operate as follows:

R[1.A] A single user action shall be used to call an alarm summary that presents only those alarms for the AORs assigned to the workstation from which the display is called.

R[1.A.i] All alarms in all classes shall be presented.

R[1.A.ii] The ADMS-SCADA shall also include facilities to call a general alarm summary that will present all alarms in all AORs.

R[1.B] The ADMS-SCADA shall also support alarm summary displays that show a distinct set of AORs.

R[1.B.i] The AORs assigned to an alarm summary display are distinct and may allow a user alarm and event access different than a user's other permitted AOR's. In addition, the ADMS-SCADA shall support an alarm summary that shows all AORs, all alarms regardless of AOR.

R[1.B.ii] The Operator shall be able to use filtering on this display to select specific AOR's based on alarms assigned to the Operator.

R[1.C] The summary shall have a system configurable option to display the alarms in chronological or reverse-chronological order.

R[1.D] Alarm summaries shall show power system and ADMS-SCADA alarms.

R[1.D.i] The user shall be able to acknowledge and delete messages on the display.

R[1.D.ii] Flashing shall identify unacknowledged alarms.

R[1.E] If the capacity of the alarm summaries is limited and an alarm summary display becomes full, the oldest messages shall be automatically deleted and the newest messages shall be added.

R[1.E.i] It shall be possible to perform any alarm interaction from the alarm summary displays.

R[1.E.ii] This condition shall be annunciated to the Operator as this limit is being approached (i.e., configurable percentage of total amount allowed).

R[1.F] The Alarm Summary display shall have the capability to filter and sort the contents based on the alarm priority and all other alarm message fields.

R[1.F.i]The Operator shall be able to select one, multiple, or all priorities for viewing.

R[1.F.ii] The Operator shall be able to define default views that use the filter and sort capabilities to quickly access a preferred priority based summary view, showing the hierarchy of priorities.

R[1.F.iii] When performing a filter or sort, the display shall keep a selected point visible in the same relative position in the window.

4.3.5.2 Event Summary

R[1] The event summary shall have the same functionality as the alarm summary with the exception that all alarms and events shall be listed.

R[2] The oldest events shall be removed from the event summary only when the capacity of the display is exceeded.

R[3] The Event Summary displays shall operate as follows:

R[3.A] A single user action shall be used to call an event summary that presents only those alarms for the AORs assigned to the workstation from which the display is called.

R[3.A.i] All events in all classes shall be presented.

R[3.B] The ADMS-SCADA shall also support event summary displays that show a distinct set of AORs.

R[3.B.i] The AORs assigned to an event summary display are distinct and may allow a user alarm and event access different than a user's other permitted AOR's.

R[3.C] The summary shall have a system configurable option to display the events in chronological or reverse-chronological order.

R[3.D] If the capacity of the event summaries is limited and an event summary display becomes full, the oldest messages shall be automatically deleted and the newest messages shall be added.

R[3.E] The Event Summary display shall have the capability to filter and sort the contents based on the various component fields of the event or alarm messages (e.g., user name, alarm priority, user id, workstation, etc.).

R[3.E.i] The Operator shall be able to define default views that use the filter and sort capabilities to quickly access a preferred summary view.

4.3.5.3 Off-Normal Summary

R[1] The ADMS-SCADA will provide a display that shows all devices in the Off-Normal state.

R[2] Devices shall be removed from the list when those devices are returned to normal.

R[3] In a case when the capacity of the display is exceeded, the oldest Off-Normal devices shall be removed from the Off-Normal Summary.

R[4] The Off-Normal Summary displays shall operate as follows:

R[4.A] A single user action shall be used to call an off-normal summary that presents only those off normal devices for the AORs assigned to the user. All off-normal devices shall be presented.

R[4.B] The ADMS-SCADA shall also support off-normal summary displays that show a distinct set of AORs.

R[4.B.i] The AORs assigned to an off-normal summary display are distinct and may allow a user off-normal access, different than a user's other permitted AOR's.

R[4.C] The summary shall have a system configurable option to display the off-normal in chronological or reverse-chronological order of when the devices were placed off-normal.

R[4.D] If the capacity of the off-normal summaries is limited and an off-normal summary display becomes full, the oldest messages shall be automatically deleted and the newest messages shall be added.

R[5] The Off-Normal Summary display shall have the capability to filter and sort the contents based on the various component fields of the off-normal device record (e.g., user name, device ID, device name, user id, etc.).

R[6] The Operator shall be able to define default views that use the filter and sort capabilities to quickly access a preferred summary view.

4.3.6 Alarm Acknowledgement

R[1] Alarms for any database item or application function condition shall be acknowledged by user action on any display presenting the alarm.

R[2] When an alarm is acknowledged, the unacknowledged condition shall be reset in the database and all display attributes for the point shall be reset to their acknowledged state (for the associated AOR).

R[3] Alarms shall be acknowledged both individually and as multiple alarms. Individual alarm acknowledgement shall require selection of a specific alarm before the acknowledgement is commanded.

R[4] If an individual point in alarm is selected on the alarm summary display, the acknowledge action shall affect only that message. If an individual point in alarm is selected on any other display, the acknowledge action shall affect all alarms for that point.

R[5] Multiple-alarm acknowledgement shall function as individual-alarm acknowledgement, except that the user interface shall include features to select multiple alarm messages for acknowledgement.

R[6] Multiple-alarm acknowledgement shall also allow the Operator to “rubber-band” an area of a one-line or other display using the mouse, and thereby select all points enclosed by the area for acknowledgement.

R[7] Note that the acknowledgement function shall support the independent acknowledgement of alarms from the same database item but for different AORs and the flashing on one-lines and displays shall reflect the AORs assigned to the user.

R[8] Page acknowledgement shall be supported on the alarm summary display and other page oriented displays and shall affect only those alarms visible within the window at the time the acknowledge action is commanded.

R[9] Acknowledged alarms shall generate an event message indicating the workstation and user that acknowledged the alarm.

4.3.7 Alarm Deletion

R[1] Alarms for any database item or application function condition shall be deleted by user action on any display presenting the alarm and programmatically based on pre-defined conditions.

R[2] When an alarm is deleted, the unacknowledged condition shall be reset in the database and the alarm message(s) shall be removed from the alarm summary display.

R[3] However, all other alarm attributes shall remain as before the delete action and the alarm conditions shall continue to be shown on displays other than the alarm summary.

R[4] Alarms shall be deleted both individually and as multiple alarms that the UI shall include features to select multiple alarm messages for deletion (e.g., rubber-banding, etc.).

R[5] The ADMS-SCADA shall operate successively on each message selected for multiple deletion.

R[6] Page deletion shall be supported on the alarm summary display and page based displays and shall affect only those alarms visible within the window at the time the deletion action is commanded.

R[7] Deleted alarms shall generate an event message indicating the workstation and user that deleted the alarm.

4.3.8 Alarm Inhibit and Enable

R[1] Alarm annunciation for any RTU, substation, and point shall be inhibited and enabled by user command.

R[2] When inhibiting alarms for an entire data source, each individual point associated with the source shall be marked as inhibited.

R[3] Alarm inhibit and enable operations shall be reported as events. When inhibited, alarms for the point shall be detected and processed and the database attributes for the alarm condition shall be set.

R[4] However, the point in alarm shall be marked as unacknowledged and any alarms detected shall not be annunciated nor presented on the alarm summary.

R[5] Alarm conditions and messages existing at the time of an inhibit action shall remain as before the action.

R[6] Alarms detected subsequent to an inhibit action shall not be annunciated when alarming is enabled.

R[7] The ADMS-SCADA shall include the capability to inhibit and enable alarms on a substation and RTU basis.

4.3.9 Alarm Audible Silencing and Suppression

R[1] Audible alarm annunciation shall be silenced, suppressed, and enabled by user command.

R[2] Alarm audible silencing and enable operations shall be reported as events.

R[3] Audible alarm silencing shall stop ongoing audible annunciation at the workstation issuing the silence command. New alarms shall again sound the audible alarm.

R[4] Audible alarm suppression silences audible annunciation and suppresses audible annunciation for new alarms at the workstation issuing the silence command until audible annunciation is enabled.

R[5] An indication of the suppression shall be presented as a common feature on the workstation so that the user is clearly informed of the condition.

R[6] A user's alarm suppression shall be disabled each time a user logs into the ADMS-SCADA, so that audible alarms will be annunciated after login, unless the user enables suppression for the new session.

4.3.10 Alarm Help

R[1] Each alarm message shall have an operator help window associated with it.

R[2] There shall be a help indicator displayed for each alarm that has help associated with it (e.g., ***, Help, etc.).

R[3] The alarm help window shall display the following information when the help indicator is selected for each database item and alarm:

R[3.A] The alarm message text;

R[3.B] The point name;

R[3.C] Station name;

R[3.D] Alarm description;

R[3.E] Description of cause and/or concern to the operator;

R[3.F] Description of operator action.

R[4] Displays shall be provided to allow operators to maintain the alarm help database.

R[5] Utilities shall be provided to allow bulk update of the alarm help database.

4.3.11 Complex Alarming Functions

R[1] The ADMS-SCADA shall have the capability to generate alarms based on complex comparisons of any data or events within the system.

R[2] Some of the features available shall be:

R[2.A] Comparisons of analog and digital (status) values (e.g., IF MW>100 and BKR OPEN or if a generator is on-line and generating VARs, the bus voltage should be held to a certain level, otherwise an alarm is generated)

R[2.B] Time-dependent alarms to delay the alarm generation for a configurable (time or number of scans) time before the alarm is generated (if point is still in alarm after the time, then issue the alarm).

R[2.C] Reissue times (i.e., reissue alarm periodically - configurable duration in minutes – initially 15 - based on alarm class - as long as condition persists)

R[2.D] Ability to let the operator initiate automatic notifications (i.e., outbound-only text messaging and e-mails) for certain alarms and to inhibit automated notification of alarms.

4.3.12 Enhanced Alarm Management

R[1] Enhanced alarm management functions required by AE include:

R[1.A] Minimization of nuisance alarm messages (for example, repetitive alarms for the same alarm condition).

R[1.B] Combining of related alarm messages.

R[1.C] Highlighting of the most urgent messages.

R[1.D] Suppression of alarms based on related alarm conditions.

R[1.E] Evaluation of related alarm conditions to determine the true alarm condition.

4.4 Trending

R[1] The ADMS-SCADA shall include facilities to generate plots of database values against time—“trends” or “trend displays”.

R[2] Trends shall be constructed as a set of “plot points” connected into a “curve” of the scaled value of selected database items on the vertical axis versus time on the horizontal axis. The trend shall include a minimum of 1000 “x-t” plot points for each database value presented on the display.

R[3] The Operator shall be able to configure trends by selecting points on display using a point and click user interface.

R[4] Data presented on each trend display shall include historical values, values acquired previous in time to the current time and stored in the IS&R function, and real-time values.

R[5] The trend presentation shall include features to scroll through time.

R[6] When a trend display shows only historical values, the trend display shall not update. The trend display shall also present the following information:

R[6.A] The name of each value trended.

R[6.B] Curve values at any point in time selected by the user.

R[6.C] The quality codes for the data at any point in time selected by the user.

R[6.D] A scale for the value axis of the trend.

R[6.E] The time scale.

R[7] Users shall be able to configure the trend display by adjusting the following parameters:

R[7.A] Range – the intercept and maximum (full range) values for each curve in engineering values. The default range shall be set by the reasonability limits for the value.

R[7.B] Trend update rate.

R[7.C] Trend start time.

R[8] The user shall determine the color of each curve. Violations of alarm limits shall be highlighted.

R[9] AE shall also be able to build trends into displays during display generation time to allow the trend to be present at display call-up time.

R[10] The Trending subsystem shall allow system data to be output to AE-provided video chart recorders.

R[11] The ADMS-SCADA shall allow the Operator to assign data points to the trend outputs and to define all the parameters to control and scale the output.

R[12] The Trend shall be output as an analog output.

4.5 User Interface Development

R[1] Tools to define and maintain displays shall be provided with the ADMS-SCADA.

R[2] The display "editor" shall support the definition of all of the displays in the ADMS-SCADA and shall be the same tool used by the Vendor to develop displays provided by the Vendor.

R[3] AE shall build a display only once, after which it shall operate on any workstation. AE shall not have to develop multiple versions of displays for each type of workstations or for different GUI products included with the ADMS-SCADA.

4.5.1 Display Style

R[1] All displays provided by the Vendor shall have a consistent "look and feel" and be consistent in its use of graphics, commands, menus, colors, poke procedures, and data entry such that data similar in appearance shall have a consistent meaning throughout the ADMS-SCADA.

R[2] This requirement shall apply to displays provided from the Vendor's standard offering and displays developed specifically for AE.

R[3] The Vendor shall submit to AE a display style guide for displays produced by the Vendor.

R[4] Any displays produced by the Vendor as part of their standard product shall comply with this display style guide.

R[5] AE will develop a style guide for displays produced by AE.

R[6] Any displays produced by the Vendor for this project, excluding displays to be incorporated into the Vendor's standard product, shall be produced in compliance with this style guide.

4.5.2 Display Elements

R[1] Displays elements shall be based on the GIS symbology and exhibit similar behavior as that within the GIS, plus additional functionality required by ADMS-SCADA.

R[2] A method of linking raster images; vector design files; jpeg, bitmap or gif files; operating procedures, and other documents to specific objects shall be included to allow an operator to select the object to display the associated document, image or file.

4.5.2.1 Data Presentation

R[1] The user shall logically identify individual dynamic data fields and data arrays in defined displays.

R[2] All linkages to the database necessary for ensuring the proper retrieval and output of the dynamic data or data arrays during actual use of the display shall be automatically established according to this identification.

R[3] The linkages between the displays and the database shall be by logical identification and shall be designed such that any database modifications do not require redefinition of existing displays.

R[4] Displays shall include a time tag indicating the time of last update of data on the display.

R[5] Data fields shall reference all supported formats.

R[6] These formats shall include programming language-equivalent data-to-ASCII conversions, plus all general GUI style elements (for example, radio boxes, menus, and sliders) and a special set of formats appropriate to the ADMS-SCADA context.

R[7] Formats shall be conveniently definable and modifiable.

R[8] It shall be possible to present any item in the database on any display.

R[9] Database items shall be displayable anywhere on the screen, excluding dedicated screen areas such as the display heading.

R[10] There shall be no limitation on the number of data items presented on any display, up to the physical limitations of the window or screen.

R[11] Similarly, screen locations for cursor targets shall be unrestricted.

R[12] The User Interface shall be designed to allow data stored in the historian to be displayed on ADMS-SCADA workstations and integrated into any ADMS-SCADA display.

R[13] Easy to use user interface techniques such as pop-up menus with default data request values shall be provided to make it simple to display historical data on ADMS-SCADA displays.

R[14] The ADMS-SCADA shall allow the operator to call up historical data with these techniques from on-line displays without having to predefine the historical data request at display build time.

R[15] Database items shall be presented in the following formats as appropriate:

R[15.A] Numerical text that presents analog and accumulator values; the format definition of the text shall include the number of characters, number of decimal places, and the use of sign or flow direction arrows.

R[15.B] Symbols, including alphanumeric text strings for a single item, based upon the item's state for all defined states.

R[15.C] Symbols, including alphanumeric text strings for multi-state items, based on flag fields where each flag represents a condition or a state and where multiple states may be true at any time; for example, data quality flag fields for both telemetry failure and alarm inhibit may be simultaneously set for an item.

R[15.D] X-Y and X-t point relationships with vectors connecting the points; for example trending and Kiviat plots.

R[15.E] Bar charts – display of value in a bar showing alarm conditions with changes in bar color.

R[15.F] Filled polygons (x or y axis inside the polygon showing the percent of full scale of the variable); for example, bar charts.

R[15.G] Filled arcs; for example, pie charts or simulations of meter movements.

R[15.H] Colors, textures, and blink conditions based upon state or value changes or a change of data quality, for example, alarm limits.

R[15.I] Combinations of the actions listed above; for example, change a bar chart color when the data value exceeds the limit.

4.5.2.2 Quality Code and Safety Tag Presentation

R[1] When more than one quality-code condition applies to the data (refer to Section 6.3.1), the highest priority condition, as determined by an AE-defined priority sequence shall be displayed.

R[2] AE shall determine the presentation of each quality code. Color, flash, appended symbols, and other display features shall be selectable during display build time.

R[3] It shall be possible to construct multiple representations for a data item and its quality codes such that the presentation of data may be optimized for a particular display and to define different representations on a per point basis.

R[4] A separate indicator shall be used to reflect the safety tag status of a database point.

R[5] When more than one safety tag applies to a point, the highest priority safety tag, as determined by an AE defined priority sequence, shall be displayed.

R[6] AE shall determine the presentation of each safety tag.

R[7] Color, appended symbols, and other display features shall be selectable for safety tag presentation.

R[8] It shall be possible to construct multiple representations for a data item and its safety tags such that the presentation of data may be optimized for a particular display.

R[9] Please refer to Section 6.4 for a complete description of the safety tag capability.

4.5.2.3 Data Sets

R[1] Selected displays will be defined with the intent of presenting data from different "data sets" defined as a collection of data produced by an application representing the state of the power system. It shall also be possible to simultaneously display data from the real-time data set and data from any of the other data sets on the same display.

R[2] Data sets from different applications include data for the same power system devices. For example, the ADMS-SCADA includes the following applications that will each produce a data set for the power system:

R[2.A] Data acquisition and processing (the real-time data set).

R[2.B] Distribution state estimator (the current solution).

R[2.C] Distribution system network analysis save cases and working areas.

R[2.C.i] Where save-case data is presented on a display, it shall be possible to present the save-case identification on the same display.

R[2.C.ii] It shall be possible to change the save case presented by entering a new save-case identification.

R[2.D] Unbalanced load flow results

R[2.E] OM function

R[2.F] AE shall be not required to create multiple displays to allow data from multiple data sets to be viewed.

R[2.G] AE shall be able to define each display once and to link the data elements to the real-time data set. All other processing necessary to link to other data sets shall be transparent to the display developer and to users.

R[2.H] At AE's discretion, they might create individual displays that show only a particular set of data.

R[2.I] The user interface shall include features such that data presented on displays can be highlighted to indicate the data set presented. It shall be possible to uniquely highlight data items for data generated by real-time state estimator solution and data from a network analysis save cases and working areas.

R[2.J] Called displays shall default to the real-time data set.

R[2.K] However, the display request mechanisms shall include features to facilitate the immediate presentation of other data sets when the display is called and to change datasets after the display has been presented.

R[2.L] Displays defined to present multiple data sets shall clearly indicate the data being presented (e.g., different background color of data).

R[2.M] Data set identification shall be unambiguous, obvious, and visible at all times.

4.5.2.4 Display Layers

R[1] World coordinate displays shall be constructed in layers.

R[2] Each layer shall be a self-contained world co-ordinate space onto which display elements, including data, shall be placed.

R[3] Layers shall be displayed in a defined order, with higher-order layers overlaying lower-order layers.

R[4] Where displayable elements of a multiple layers occupy the same space, the higher-order layer elements shall be displayed.

R[5] The selective presentation of layers – "decluttering" – shall be controlled by the scale (zoom) level and by user selection.

R[6] Each layer shall be visible over a range of scale level set defined as the display is built.

R[7] It shall also be possible for the user to override the automatic selection of layers and to select those layers presented at any time.

R[8] This layer capability shall be used to support the display of the geographic background for Distribution Circuit Displays.

4.5.2.5 User Interaction

R[1] Cursor targets shall send a message to an application or issue a command when events occur. The ADMS-SCADA shall support the following commands via user interaction:

R[1.A] Call a display. Page forward and backward commands shall be considered special cases of display call interaction, where the sequence of displays shall be part of the display definition.

R[1.B] Initiate a program. (Programs may be either an ADMS-SCADA application, operating system, utility, or third party program.)

R[2] Such commands shall convey both fixed and contextual data. As a minimum, supported contextual information shall include:

R[2.A] Record identities linked to the cursor target.

R[2.B] Cursor position on the screen and within the display.

R[2.C] Database, application, and application system associated with the display.

R[2.D] List position (for lists).

R[2.E] Workstation identification and any associated parameters, such as permissions.

R[3] Conditional attribute values shall be attached to any display element, primitive, or macro and shall be able to make a particular display item valid or invalid depending on whether the referenced data or display context is in a specified state.

R[4] Multiple cases shall be supported so that, for example, a data item may appear in one color if it is in range, another color if it is below range, and a third color if it is above range.

R[5] The ADMS-SCADA shall support "pop-up" and "pull-down" menus for user interaction.

R[6] Those menus supplied with the ADMS-SCADA shall be extensible by AE to incorporate new features and applications developed by AE.

R[7] It shall be possible to add additional items to existing menus, to define entirely new menus, and to link the call-up of new menus to specific user actions.

R[8] The menu items, when selected, shall pass messages to applications including fixed and contextual data as described above.

4.6 AE-Provided Displays

R[1] AE will provide the displays described below. Initially, the Vendor will assist AE in the creation of these displays. Once proficient, AE will take over the creation of these displays.

R[1.A] **Substation One-Lines** – These displays show the interconnected elements of individual substations including buses, incoming and outgoing lines, transformer banks, circuit breakers, capacitor banks, and disconnects.

R[1.A.i] The displays shall present telemetered, manual, and calculated data, including all alarm conditions.

R[1.A.ii] Highlighting and colors shall be used to distinguish the operating states of the different substation elements and shall be consistent with all other one-line displays.

R[1.A.iii] The user shall be able to interact with the substation one-line displays to perform any associated user interactions such as data entry and supervisory control.

R[1.B] **Tabular Displays** – These displays will contain telemetered data and calculated data.

R[1.B.i] They may be associated with either Vendor-provided application programs or AE-provided application programs.

R[1.B.ii] The user shall be able to interact with these tabular displays to perform user interactions such as data entry, application function execution, and display call-up.

R[1.C] **One-Line Menu** – These displays shall provide one-line menus for substations.

R[1.C.i] Each entry in these lists shall allow selection of the associated one-line diagram.

4.7 Vendor-Provided Displays

R[1] The Vendor shall provide the displays described below. All Vendor-provided displays shall present data using data names defined by AE.

R[1.A] **Access Control Display** – This display shall allow a designated authority to control user access to the ADMS-SCADA. The display shall enable the designated authority to enter, modify, and delete user IDs and passwords and to assign workstation jurisdiction and operating modes.

R[1.B] **Menu Directory Display** – This display shall list all menu displays in alphanumeric order. Each entry in the list shall have a cursor target for menu selection.

R[1.C] **Hierarchical Display Menu Directory** – This display shall list all displays in a hierarchical order based on the structure and organization of the display library, by application category, transmission, distribution, voltage level and display type (e.g., control input, output results). This display shall be generated automatically on call-up. Each entry in the list shall have a cursor target for display selection.

R[1.D] **ADMS-SCADA Directory Display** – This display shall list all ADMS-SCADA displays in alphanumeric order. Each entry in the list shall have a cursor target for display selection.

R[1.E] **Distribution Circuit Display** – These displays shall be generated from the data imported from AE's GIS and show the Distribution Circuits overlaid on the geographic background for the service area. Please refer to Section 13.2.1.1 for additional details.

R[1.F] **ADMS-SCADA Auto-Schematic Displays** – These displays shall show the distribution circuits in a pseudo -geographic form that maintains the relative geographic orientation of devices but compresses the distance between devices to show a schematic view of the circuits. Please refer to Section 13.2.1.3 for additional details.

R[1.G] **RTU Menu Display** – This display shall list all RTUs (including devices that provide RTU like functions) in the ADMS-SCADA in logical groupings/front-end order or alphanumeric order, selectable by the user. Each entry in the list shall have a cursor target to access an RTU detailed display, showing the configuration and composition of the selected RTU.

R[1.H] **ADMS-SCADA Configuration Monitoring and Control** – These displays shall allow the user to monitor and control the ADMS-SCADA configuration. The displays shall:

R[1.H.i] Present all equipment status and associated equipment alarms.

R[1.H.ii] Provide menus or cursor targets for performing actions such as failover, switching local and remote devices (such as workstations, servers, and RTUs), switching communication channels, controlling the ADMS-SCADA resource monitoring function.

R[1.H.iii] Present processor and communication channel loading and error statistics.

R[1.H.iv] These displays shall graphically show the interconnected elements of the ADMS-SCADA including communication paths and Vendor-provided channel interface equipment such as modems, transceivers, and multiplexors.

R[1.H.iv.a] The data sources communicating over each path shall be shown.

R[1.H.v] An RTU In/Out of Service display shall be provided to show the state of the RTUs in the system

R[1.I] **RTU Tabular** – These displays list the value of telemetered and calculated data associated with each RTU as well as related information such as alarm limits.

R[1.I.i] The user shall be able to interact with the RTU tabular displays to perform any associated user interactions such as data entry and supervisory control.

R[1.I.ii] The user shall be able to call-up the associated substation one-line display from a poke point located on the tabular display.

R[1.J] These displays shall be generated automatically by the ADMS-SCADA upon call up and shall be based on the current contents of the database.

R[1.J.i] AE shall have approval over the format of these displays.

R[1.J.ii] Points displayed shall be all database points within the substation:

R[1.J.ii.a] *For status points* – The information displayed for each point shall include: name descriptors, all data attributes, current status, normal status, quality codes and safety tags.

R[1.J.ii.b] *For analog points* – Information displayed for each point shall include: name descriptors, all data attributes, current value, all limit values, quality codes.

R[1.J.ii.c] *For accumulator points* – Information displayed for each point shall include: name descriptors, all data attributes, current value, quality codes.

R[1.J.ii.d] *For control points* – The information displayed for each point shall include: name descriptors, all data attributes, type of control point, current status, normal status, quality codes and safety tags.

(a) The types of points shall be displayed separately (i.e., using separate pages) from each other and telemetered data displayed separately from calculated data.

(b) As many display pages as needed to show all points at a substation shall be provided.

(c) For substations with multiple data sources, the points shall be ordered according to data source. It shall be possible to perform any allowed point function from the station tabular page.

R[1.K] **Device Information Displays** – Single displays shall be provided that will display all of the attributes for an individual data item on a per point basis, current state, alarm condition, all active quality codes, etc., when the data item is selected on another display.

R[1.K.i] These displays shall be provided for all telemetered (analog, status, SOE, accumulator, ICCP), calculated, control, pseudo/manual, distribution system devices (transformers, lines, etc.), substations, RTUs and other ADMS-SCADA devices.

R[1.K.ii] These displays shall be generated automatically by the ADMS-SCADA upon call up and shall be based on the current contents of the database. AE shall have approval over the format of these displays.

R[1.K.iii] The types of devices shall be displayed separately (e,g., using separate pages) from each other. As many display pages as needed to show all devices shall be provided.

R[1.L] **Summary Displays** – Summary displays are list displays presenting power system and ADMS-SCADA conditions to the users.

R[1.L.i] These displays shall be automatically dynamically updated when on view on a workstation.

R[1.L.ii] User interaction with the displays shall include filtering and sorting of the data presented in the displays, including defining a primary and secondary sort key.

R[1.L.iii] The ADMS-SCADA shall support sorting and filtering by:

R[1.L.iii.a] AOR.

R[1.L.iii.b] Location (substation, generating plant).

R[1.L.iii.c] RTU.

R[1.L.iii.d] Point name.

R[1.L.iii.e] Alarm class.

R[1.L.iii.f] Date and time.

R[1.L.iv] It shall be possible to define default filters and sorting for each summary, to be applied when the display is called to view:

R[1.L.iv.a] *Alarm, event, and SOE summaries* – sorted by date and time, with the most recent entries in view when the display is called. The summaries shall be filtered to present only those entries of those AORs assigned to the calling workstation.

R[1.L.iv.b] *All other summaries* – sorted by date and time and then location (alphanumeric). No filter shall be applied at call up; however, the summaries shall be filtered to present only those entries of those jurisdictions assigned to the calling workstation and be selectable by RTU.

R[1.L.v] Summary Displays shall support the export of their contents (e.g., memos, manual entries, safety tags, etc.) to external files (Excel, Access, Word) for external processing and reports.

R[1.L.vi] Summary displays shall include:

R[1.L.vi.a] *Alarm Summary* – (refer to Section 4.3.5.1)

R[1.L.vi.b] *Event Summary* – (refer to Section 4.3.5.2)

R[1.L.vi.c] *Off-Normal Summary* – This display shall list devices and values that are not in their normal state.

(a) Telemetered, calculated, and manually entered status, analog, and accumulator data points shall be included.

(b) For analog points, this summary shall provide information representing the overloaded equipment.

R[1.L.vi.d] *Off-Scan Summary* – This display shall list all points that have been suspended from acquisition.

R[1.L.vi.e] *SOE Summary* – This display shall list SOE information.

R[1.L.vi.f] *Alarm Inhibit* – This display shall list devices and data values for which the user has inhibited alarm processing.

(a) Controls to enable sorting by substation and by date and time of the entry of the inhibit shall be included on the display.

R[1.L.vi.g] *Limit Override Summary* – This display shall list devices and data values for which the user has overridden limits.

(a) The entries for overridden limits shall show the database (non-overridden) value of the limit as well as the overriding value.

(b) Controls to enable sorting by substation and by date and time of the entry override shall be included on the display.

R[1.L.vi.h] *Safety Tag Summary* – This display shall list and describe all active safety tags for all devices.

(a) The user shall be able to place and remove safety tags from this summary. Information on this display shall list each device safety tagged and shall include: date and time of safety tag placement, user who placed the safety tag, safety tag level, station identifier, device identifier, and comment field.

(b) The display shall include the ability to sort the safety tag information according to safety tag type.

R[1.L.vi.i] *Manual Replace Summary* – This display shall list all points that have been replaced by manual entries.

(a) Separate displays shall be provided for telemetered and manual/pseudo points for SCADA data.

(b) For each point, there shall be facilities for fast access to the display containing the point, such that the user can further modify the value or return the point to automatic data acquisition.

R[1.M] **Communication Maintenance Displays** – Communications with data sources and other computer systems shall be managed via these displays.

R[1.M.i] Communications management displays shall show the current status of the communication channels.

R[1.M.ii] Communication error counts, and tabulations of all types of errors and shall enable control and diagnosis of communications devices.

R[1.N] **Areas of Responsibility Management Displays** – The ADMS-SCADA shall include displays to allow the supervisor or administrator to manage and assign AORs/permissions based on current user responsibilities.

R[1.N.i] The responsibility (and access to) for this function shall be configurable to divide this function among the AE Operating regions (based on AORs) between users (refer to Section 4.2.4).

R[1.O] **Application Program Displays** – The Vendor shall provide all displays associated with all specified application programs and functions.

R[1.O.i] Displays that allow the user to interact with ADMS-SCADA application programs shall use a common look-and-feel approach.

R[1.P] **Other Displays** – Specific display requirements for other ADMS-SCADA functions are described throughout this RFP.

R[1.P.i] The Vendor shall be responsible for the supply of all displays necessary to support the specified functions, in addition to any other ADMS-SCADA displays required to control and monitor the ADMS-SCADA itself.

Table of Contents

5. Hardware Requirements 5-1
    5.1 Optional Maintenance Agreement 5-1
    5.2 Processors and Auxiliary Memory 5-1
    5.3 Archive Storage 5-2
    5.4 Local and Wide Area Networks 5-2
        5.4.1 ADMS-SCADA Network 5-2
        5.4.2 Firewalls and Routers 5-3
        5.4.3 Time Facility 5-3
    5.5 User Interface 5-3
        5.5.1 Workstations 5-3
            5.5.1.1 Monitors 5-4
            5.5.1.2 Processing Capability 5-4
            5.5.1.3 Keyboard and Cursor Control 5-4
            5.5.1.4 Audible Alarm 5-4
        5.5.2 Printers and Video Hardcopy 5-4
    5.6 Other Peripheral Devices 5-5
    5.7 Operating and Construction Requirements 5-5
        5.7.1 Power Distribution and Protection 5-5
        5.7.2 Environment 5-5
        5.7.3 Equipment Noise 5-6
        5.7.4 Enclosures 5-6
        5.7.5 Assembly and Component Identification 5-6
        5.7.6 Enclosure Grounding 5-7
        5.7.7 Interconnections 5-7

5. Hardware Requirements

R[1] All hardware will be purchased, installed, and configured by AE.

R[2] The Vendor shall specify the hardware, configuration, system software, and communication/network facilities required to meet the requirements of this Specification.

R[3] The Vendor shall also define the schedule requirements for having the various elements and configurations available for use in developing, configuring, integrating, and testing the ADMS-SCADA as required in this Specification, as well as the locations (e.g., Vendor site or AE site) where the hardware should be installed.

R[4] The hardware specified by the Vendor shall be complete including all elements defined herein.

R[5] Characteristics are provided to help convey AE's requirements and preferences.

5.1 Optional Maintenance Agreement

R[1] AE requests the vendor submit with their proposal their available maintenance agreements.

R[2] This option will include the associated rates, conditions and service level agreements.

5.2 Processors and Auxiliary Memory

R[1] All processors (servers, client PCs, etc.) shall be reasonably current models selected for efficient operation of a real-time system.

R[2] AE shall be able to replace or upgrade the processors with future compatible processor offerings to obtain increased computational power and system expansion with no required system or application software changes.

R[3] All processors shall be equipped with dual power supplies that automatically backup each other to provide a highly fault tolerant system design.

R[4] All processors shall be equipped with dual network interface cards (NICs) that shall be configured as a functional team. All component functionality shall be maintained if either or both NICs are connected to the network.

5.3 Archive Storage

R[1] All archive hardware will be purchased, installed, and configured by AE.

R[2] The Vendor shall specify the hardware, configuration, system software, and communication/network facilities required to meet the requirements of this Specification.

5.4 Local and Wide Area Networks

R[1] AE is responsible for implementing all connections to LANs and WANs,

R[2] AE uses Cisco networking and switching equipment as its corporate standard.

5.4.1 ADMS-SCADA Network

R[1] AE operates a converged data network. VLANs for control systems are highly fragmented with firewall service modules and extensive firewall rules.

R[2] Certain "commonly allowed" network commands are expressly denied over AE control system networks including but not limited to:

- R[2.A] Ping
- R[2.B] FTP (TCP port 21)

R[3] ALL network IP connections (regardless of port number or purpose) that go unused for 1 hour shall be torn down by the AE network equipment. ALL ADMS-SCADA system components shall gracefully and automatically re-establish required IP connections as needed.

R[4] AE will configure the VLANs interconnecting the ADMS-SCADA components to allow traffic through only those ports required for operation. Communication through ALL other ports shall be denied by firewalls.

R[5] AE will specify information for use in establishing network connectivity such as:

- R[5.A] Host names
- R[5.B] Host addresses (NIC and NIC team)
- R[5.C] Host subnet masks
- R[5.D] All ADMS-SCADA network devices shall support the necessary throughput and redundancy to meet overall system performance requirements

R[6] The Vendor shall assist AE representatives in establishing NERC CIP compliant connectivity to the AE network Corporate WAN.

R[1] The ADMS-SCADA shall interface to AE's Corporate LAN through firewalls at both Control Centers.

5.4.2 Firewalls and Routers

R[1] Firewalls (Cisco PIX 515E and PIX 525E) or equivalent will be provided by AE to limit access to the ADMS-SCADA to authorized users.

R[2] The Vendor shall supply a list, in Microsoft Excel form, detailing the ports and services required for full functionality of the ADMS-SCADA as defined herein. This list shall include all information required to define the firewall rules including source, destination, protocol, port number, associated service, etc. for each network connection.

R[3] AE will supply all network equipment (except individual machine NICs) including routers, switches and firewalls to implement the ADMS-SCADA network

R[4] The Vendor shall design the ADMS-SCADA to communicate properly in the network environment described here.

5.4.3 Time Facility

R[1] Two network time source appliances (one for each ECS cluster) shall be supplied by the vendor. Theses shall provide the time reference for all ADMS components.

5.5 User Interface

R[1] The user interface shall include all hardware necessary to facilitate optimum user communication with the ADMS-SCADA and to provide efficient operational control and monitoring of the power system.

5.5.1 Workstations

R[1] All workstations consist of the following equipment:

5.5.1.1 Monitors

R[1] The monitors shall be of LCD or LED technology and shall have a minimum screen size (diagonal) of 24 inches with a video resolution of 1920 x 1200 (minimum).

5.5.1.2 Processing Capability

R[1] The workstation shall be configured with sufficient processing speed, memory and graphics capability to support the performance requirements specified in the Capacity and Performance section of this RFP.

5.5.1.3 Keyboard and Cursor Control

R[1] One keyboard shall be provided at each console.

R[2] The keyboard shall include an alphanumeric keyboard, numeric keyboard, four-key cursor control, twelve function keys and a minimum three button mouse with a scroll wheel.

R[3] The cursor control device shall incorporate all console monitors without switching by the user. Keyboard output shall be directed to the active viewport (as determined by the user interface techniques).

5.5.1.4 Audible Alarm

R[1] Each workstation shall be equipped with an audible alarm tone generator that is capable of producing many different distinct sounds to distinguish between each alarm class and alarm priority, based on the audible alarming parameters (e.g., priority).

R[2] Volume shall be adjustable by the user.

R[3] The Vendor shall have the capability to interface to the Primate Video Wall software.

5.5.2 Printers and Video Hardcopy

R[1] All printers on the system shall adhere to AE standards as follows:

R[1.A] Black and White Printers: HP LaserJet 4250 dtn or its successor

R[1.B] Color Printers: HP Color LaserJet 5550 dtn or its successor.

R[2] Printers shall be separated from the ADMS-SCADA LAN in a DMZ to provide a level of isolation from the critical ADMS-SCADA processing resources.

R[3] Parallel or serial port connections to a processor are not acceptable.

5.6 Other Peripheral Devices

The Vendor shall supply any other peripheral devices or equipment normally provided for operation, software support, and maintenance of the ADMS-SCADA.

5.7 Operating and Construction Requirements

R[1] All ADMS-SCADA equipment shall operate and be constructed in accordance with the following requirements.

5.7.1 Power Distribution and Protection

R[1] Power will normally be supplied from a redundant, uninterruptible, conditioned sources

R[2] At times, power may be supplied directly from the utility lines.

R[3] All server equipment shall have redundant power supplies.

R[4] No single point of failure in power related hardware shall cause the component to disfunction.

R[5] AE will supply dual power sources to each enclosure as required.

R[6] The Vendor shall distribute power within the system enclosures, workstations, peripherals, and other components of the system.

5.7.2 Environment

R[1] Equipment located in the computer room shall operate over an ambient temperature range of 15 to 32°C (60 to 90°F), with a maximum rate of change of 8°C (15°F) per hour.

R[2] Relative humidity will range from 40% to 80% non-condensing.

R[3] Equipment located outside of the computer room shall operate over an ambient temperature range 10 to 38°C (50 to 100°F), with a maximum rate of change of 8°C (15°F) per hour.

R[4] Relative humidity will range from 30 to 95% non-condensing.

R[5] Note the printers specified in Section 5.5.3 are not subject to this requirement.

5.7.3 Equipment Noise

R[1] The noise generated by the equipment in any enclosure, including desktop equipment, located in the computer room shall not exceed 60 dbA 1 meter (3 feet) from the enclosure.

R[2] The noise generated by the equipment in any enclosure, including desktop equipment, located outside the computer room shall not exceed 50 dbA 1 meter (3 feet) from the enclosure.

R[3] Sound-deadening enclosures shall be provided where necessary to meet these requirements.

5.7.4 Enclosures

R[1] Except for workstations, monitors, keyboards, cursor positioning devices, printers, and processor terminals, all equipment shall be mounted in enclosures.

R[2] Equipment identified as redundant devices or components in this SOW shall be delivered with each component of a redundant pair being installed in physically separated enclosures with doors and locks.

5.7.5 Assembly and Component Identification

R[1] Each assembly in the system, to the level of printed circuit cards, shall be clearly marked with the manufacturer's part number, serial number, and the revision level.

R[2] All printed circuit card cages and all slots within the cages shall be clearly labeled.

R[3] Printed circuit cards shall be keyed for proper insertion orientation.

5.7.6 Enclosure Grounding

R[1] A safety ground in accordance with the National Electrical code shall be provided within each enclosure.

R[2] The grounding shall be designed to provide RF noise suppression, using many stranded ground cables.

5.7.7 Interconnections

R[1] The Vendor shall supply all cabling between component units of the ADMS-SCADA within each facility.

Table of Contents

6. Data Acquisition, Processing, and Control 6-1
6.1 Data Acquisition 6-1
6.1.1 Data Acquisition Protocols 6-2
6.1.2 Scan Group 6-2
6.1.3 Data Acquisition 6-3
6.1.3.1 Data Acquisition Via Polling 6-3
6.1.3.2 Spontaneous Reporting 6-3
6.1.3.3 Demand, Programmatic, and Integrity Scans 6-3
6.1.3.4 Full Report and Report by Exception 6-4
6.1.4 Enabling and Suspending Data Acquisition and Supervisory Control Permission 6-4
6.1.5 Telemetry Failure and Manual Substitution 6-5
6.1.6 Sequence-of-Events Collection 6-7
6.1.7 Monitor and Control of Data Acquisition Components 6-8
6.2 TASE.2 Data Exchange 6-10
6.2.1 TASE.2 User Interface Requirements 6-11
6.2.1.1 Database Maintenance - Bilateral Table Creation and Editing 6-11
6.2.1.2 Database Maintenance - Data Set Creation and Editing 6-12
6.2.1.3 Operational Monitoring and Control - Connection and Association Control 6-13
6.2.1.4 Maintenance and Support Tools 6-15
6.2.1.5 Performance Monitoring 6-17
6.3 Data Processing 6-17
6.3.1 Data Quality 6-18
6.3.2 Analog Data 6-20
6.3.2.1 Overload Monitor and Timer-Based Alarm Limits 6-21
6.3.2.1.1 Timer-Based Alarm Limits 6-22
6.3.2.1.2 Seasonal Limits for Overload Monitored Data 6-23
6.3.2.2 Alternate Limit Sets 6-24
6.3.2.3 Limit Manager 6-25
6.3.2.3.1 Line Ratings Display 6-25
6.3.2.4 ADMS-SCADA Sign Convention 6-27

Table of Contents

6.3.3 Status Data 6-27
6.3.3.1 State Conversion 6-27
6.3.3.2 Normal State Processing 6-28
6.3.3.3 State Change Detection 6-29
6.3.4 Accumulator Data 6-29
6.3.5 Sequence of Events Data 6-30
6.3.6 Non-Telemetered Data 6-31
6.3.7 Calculated Data 6-31
6.3.7.1 Generalized Calculations..6-32
6.3.7.2 Integration...6-32
6.3.7.3 Processing of Calculated Data 6-33
6.3.7.4 Nth Generation Programming Language...6-33
6.3.8 Data and Test Quality Code 6-35
6.4 Safety Tagging 6-36
6.4.1 Safety Tag Types and Supervisory Control Inhibit 6-36
6.5 Supervisory Control 6-37
6.5.1 Single State Control Devices (Relay Reset) 6-38
6.5.2 Two- and Three-State Control (Switching Devices)..................................6-38
6.5.3 Two- and Three-State Control – Delayed Close (Capacitor and Reactor Switching) 6-39
6.5.4 Incremental Control (Tap-Changing Transformers)...................................6-39
6.5.5 Setpoint Control 6-40
6.5.6 Control Completion Check 6-40
6.5.7 Control Permissive...6-41

List of Exhibits:

Exhibit 6-1: Quality Codes 6-19

6. Data Acquisition, Processing, and Control

R[1] The Supervisory Control and Data Acquisition (SCADA), data exchange, and data processing requirements of the ADMS-SCADA presented in this section shall apply equally to all data acquisition, supervisory control, data exchange, and processing, regardless of the data source or the communications protocol used between the ADMS-SCADA and the data source.

R[2] Conceptually, the ADMS-SCADA consists of a host system interacting with remote devices (RTUs) using DNP protocol.

R[3] For the purposes of this specification the term “RTU” shall be interpreted as any processor based device that acts as a DNP slave.

R[4] This may include, but is not limited to, traditional RTUs, data concentrators, IEDs (relays, meters, etc.) that can be addressed as a DNP “slave”.

R[4.A] AE anticipates using DNP 3.0 level 2 as the default host-slave protocol.

6.1 Data Acquisition

R[1] Telemetered data shall be collected from the following data sources:

R[1.A] Remote terminal units and Data concentrators, located at substations, equipment on distribution lines, and other facilities throughout AE’s electrical power system.

R[1.B] Substation SCADA and substation automation systems located throughout the power system.

R[1.C] Other external interfaces defined within this RFP (Section 2.1.7).

R[2] The ADMS-SCADA shall support all features of all specified protocols unless specifically stated otherwise.

R[3] In addition to telemetered data, the ADMS-SCADA shall support the following types of data:

R[3.A] Non-telemetered data entered by the user

R[3.B] Calculated data generated by the data processing function

R[3.C] Calculated data generated by applications.

R[4] This data may be of any type specified in Section 6.3, Data Processing.

R[5] All requirements in this and other sections pertaining to telemetered data, such as limit monitoring, state change detection, enabling and inhibiting alarms, and quality codes, shall also apply to non-telemetered and calculated data.

6.1.1 Data Acquisition Protocols

R[1] AE anticipates using DNP 3.0.

R[2] The vendor will be able to support industry standard protocols:

R[2.A] IEC 61970 and IEC 61968: Providing a Common Information Model (CIM), necessary for exchanges of data between devices and networks, primarily in the transmission (IEC

R[2.B] 61970) and distribution (IEC 61968) domains. IEC 61850: Facilitating substation automation and communication as well as interoperability through a common data format.

R[2.C] IEC 60870-6: Facilitating exchanges of information between control centers.

R[2.D] IEC 62351: Addressing the cyber security of the communication protocols defined by the preceding IEC standards.

R[3] The ADMS-SCADA shall support the following protocols:

6.1.2 Scan Group

R[1] A “scan group” is an addressable unit of data to be retrieved from a data source and may include one or more items of data, as defined by the protocol used by the data source and its configuration.

R[2] Each item of data available from each source shall be assigned to one or more scan groups, definable by AE, in accord with the capabilities of the source and the protocol used by the source.

R[3] Each data source may include any number of scan groups with any number of points, up to the limits of the protocol.

R[4] The ADMS-SCADA shall support all data address capabilities of each data source and shall specifically not be limited to retrieving only all data or all data of a specific type (status, analog, or accumulator) in a single scan.

6.1.3 Data Acquisition

R[1] The ADMS-SCADA shall acquire data by polling (master/slave relationship between the ADMS-SCADA and the data source) and by spontaneous reporting (peer-to-peer).

R[2] Data may be transmitted by the source as a full report or by exception.

6.1.3.1 Data Acquisition Via Polling

R[1] The ADMS-SCADA vendor shall be certified DNP 3.0 compliant and adhere to those Data Acquisition and polling requirements.

6.1.3.2 Spontaneous Reporting

R[1] Unsolicited data acquisition is spontaneously initiated by data sources, typically when changes in input data are detected or when processes within the data source determine that data should be reported.

R[2] The ADMS-SCADA shall accept data transmitted from the spontaneously reporting data sources at any time, and shall acknowledge the receipt of the data as required by the protocol.

6.1.3.3 Demand, Programmatic, and Integrity Scans

R[1] In addition to periodic and spontaneous data acquisition, the ADMS-SCADA shall acquire data from sources under the following conditions:

R[1.A] When requested by a user (demand scan).

R[1.B] When initiated by an application.

R[1.C] Integrity scan – periodically for all scan groups where the data is acquired by report by exception or by unsolicited reporting.

R[1.C.i] Report by exception processing and integrity scans shall be configurable to enable the functions and adjust the frequency of the integrity scans.

R[1.D] Integrity scan when an RTU is brought on-line, prior to marking the RTU up.

6.1.3.4 Full Report and Report by Exception

R[1] The ADMS-SCADA shall accept data reported in full and by exception.

R[2] Data reported in full is transmitted as the current value of every item in the scan group requested (polling) or transmitted (spontaneous reporting), even where the value has not changed since it was last reported.

R[3] The ADMS-SCADA shall also accept data reported by exception, both in response to polls or spontaneously reported.

R[4] Data reported by exception is transmitted by the source when the value of the data has fulfilled some condition at the source, typically when it has changed.

R[5] If supported by the protocol and for those data sources so configured by AE, the ADMS-SCADA shall store a deadband value for each value reported by exception.

R[6] This deadband shall be adjustable by ADMS-SCADA users and shall be downloaded to the data source upon change of the deadband and whenever the data source is brought on-line.

6.1.4 Enabling and Suspending Data Acquisition and Supervisory Control Permission

R[1] Users shall be able to suspend (deactivate) acquisition of (“remove from scan”) any individual point, scan group, entire data source (e.g., RTU) or station (refer to Exhibit 6-1).

R[2] Suspended points, scan groups, and data sources shall not be processed nor stored in the database.

R[3] The ADMS-SCADA shall set an “acquisition suspended” quality code for all suspended points and shall make an entry for the points on the off-scan summary.

R[4] The acquisition suspended quality code shall be distinct from the ‘telemetry failure’ quality code.

R[5] When the user enables (“restores”) the point, scan group, or data source, the ADMS-SCADA shall resume polling the data and updating the database with the data.

R[6] Users shall also be able to suspend Supervisory Control Permission on any individual point, scan group, entire data source (e.g., RTU) or station.

R[7] The suspension of Control Permission shall disallow any control operation to the suspended device.

6.1.5 Telemetry Failure and Manual Substitution

R[1] “Telemetry failure” is defined as any of the following conditions:

R[1.A] The inability of the ADMS-SCADA to complete a scan group data collection within a timeout period defined for the scan group in a particular RTU.

R[1.A.i] The timeout period for each scan group in a particular RTU shall be set between 0.1 and 60 seconds to a resolution of 0.1 second.

R[1.B] The inability of the ADMS-SCADA to complete a scan group data collection due to errors in the communications with the data source.

R[1.C] The inability of the ADMS-SCADA to complete a scan group data collection prior to the next scan request addressed to the same scan group.

R[1.C.i] In the event that the ADMS-SCADA fails to complete scans before the next scan request is due, the ADMS-SCADA scan process shall degrade gracefully to allow scanning of all available data but at slower rates commensurate with the loading level being experienced.

R[1.C.ii] This feature shall be configurable on a per channel basis and RTU basis.

R[1.D] The ADMS-SCADA shall increment the retry count (configurable) for each erroneous transmission from a spontaneously reporting scan group.

R[1.E] The retry count and other error counts shall be maintained until manually reset or periodically reset (configurable).

R[1.F] When the retry count exceeds a retry limit set for each scan group, a telemetry failure shall be declared.

R[1.G] Scans subsequent to a telemetry failure shall occur at the normal time.

R[1.H] If a new transmission is received from a spontaneously reporting scan group before the previous transmission has been processed and acknowledged, the ADMS-SCADA shall attempt to process the incoming data.

R[1.I] If a spontaneously reporting data source continues to report data at a rate faster than the ADMS-SCADA can process the data ("data overrun"), the ADMS-SCADA shall log and indicate a scan overrun and declare a telemetry failure for the source.

R[1.J] The telemetry failure condition shall be removed by the ADMS-SCADA after a time specified for all spontaneously reporting sources (initially 30 minutes).

R[1.K] The user shall be able to inhibit this failure restoration procedure (for all sources, not individually).

R[1.L] Upon declaring telemetry failure, the ADMS-SCADA shall set a "telemetry failure" quality code for all affected points and shall make an entry for the points on the off-scan summary.

R[1.M] The ADMS-SCADA shall generate an alarm when a telemetry failure occurs.

R[1.N] The alarm shall describe the data source or scan group failing; the individual points of the scan group or data source shall not be listed.

R[1.O] The ADMS-SCADA shall issue an alarm when a communications "slow-down" occurs. This shall not cause the data sources or circuit to fail, for non-failed devices.

R[1.P] The last good value of a point in telemetry failure (that value stored in the database immediately prior to the detection of the telemetry failure) shall be retained in the database.

R[1.Q] Upon failure of a FEP, the ADMS-SCADA shall alarm the failure and mark all associated RTUs and data points as failed until successfully scanned on a redundant FEP.

R[1.R] The ADMS-SCADA shall support user entry of a substitute value for any point and shall set a “manual substitution” quality code and shall suspend data acquisition for the point.

R[1.S] If the data acquisition is suspended by entry of a manual entry without first placing the point out of scan and when the point is next successfully (without error) acquired and processed, the value shall be overwritten and the manually substituted quality code shall be reset.

R[1.T] If the Operator suspends data acquisition for a data point before performing a manual replace, data acquisition shall not overwrite the suspended data point until the point is unsuspended.

R[1.U] The feature to disable data acquisition for manually entered data shall be configurable and shall initially be configured to block the scan process and attach the manually entered quality code.

R[1.V] The ADMS-SCADA shall collect hourly communication error statistics and calculate RTU availabilities.

R[1.W] These statistics shall be tracked on an RTU and communications channel basis and shall be retained in the IS&R Historian.

6.1.6 Sequence-of-Events Collection

R[1] Sequence-of-events (SOE) data, time-stamped reports of status changes, shall be collected from appropriately configured data sources including support for all DNP SOE formats and event reporting.

R[2] A subset of the data sources reporting SOE data (periodic) will include time stamp to a millisecond resolution with each status change indication.

R[3] The status change shall be processed as any other status change, including the value of the local GPS time stamp, for those RTUs that are so equipped.

R[4] Other data sources report the availability of SOE data (report-by-exception), typically by setting a flag in the header of a reply to a scan request.

R[5] The ADMS-SCADA shall issue a scan request for the appropriate SOE scan groups.

R[6] Where the data source and the communications protocol support SOE buffer 'near-full' and 'overflow' conditions, the SOE collection process shall give priority to retrieving SOE data from those sources reporting the 'near-full' or 'overflow' condition.

R[7] The ADMS-SCADA shall have a GPS interface to time ADMS-SCADA events.

R[8] All RTUs that support time synchronization shall be synchronized either from the ADMS-SCADA time source or be GPS time–synched at the source.

R[9] The ADMS-SCADA shall convert the Universal Time format to current legal time in Austin. It shall have the ability to automatically change between CT and CSLT and vice-versa as required by law. The list of dates on which those changes occur shall be programmatically updateable.

R[10] The ADMS-SCADA shall provide the capability for selection, at RTU configuration time, of a GPS source at the data source or a centralized GPS source (at the ADMS-SCADA) that shall synchronize the clock at the data source, on a data source basis.

R[11] The ADMS-SCADA reports shall include either the locally GPS time synched or the centralized time synched sequence-of-events data in chronological order.

6.1.7 Monitor and Control of Data Acquisition Components

R[1] The ADMS-SCADA shall include the displays to monitor and control the data acquisition components, as described below:

R[1.A] FEP Control Display - shall have the following features:

R[1.A.i] FEP's listed by region.

R[1.A.ii] Poke point to go to comm. lines display for each FEP.

R[1.A.iii] Poke point to place FEP offline.

R[1.A.iv] Poke point to restart FEP.

R[1.A.v] FEP status listed by text and number.

R[1.A.vi] FEP status shall indicate when there is a loss of communications

R[1.B] Comm. Lines Control Display for FEP's - shall have the following features:

R[1.B.i] Logical Grouping of Like Communications (e.g., Whole T-1 per screen – 24 channels/lines, etc.).

R[1.B.ii] Status listed for each comm. line.

R[1.B.iii] Poke point to place the comm. line offline.

R[1.B.iv] Poke point to restart the comm. line.

R[1.B.v] Comm. Line transaction and error counts for the hour.

R[1.B.vi] A group select poke point for failing groups of circuits between front-ends, alternate paths, etc.

R[1.B.vii] Individual poke points for failing single comm. lines and groups of circuits between front-ends, alternate paths, etc.

R[1.B.viii] Status point to indicate which front-end is active for each comm. line.

R[1.B.ix] I.P. address for each comm. line.

R[1.C] RTU Displays - shall have the following features:

R[1.C.i] RTU's listed in alphanumeric order.

R[1.C.ii] Poke points for listing "all" or just "operational" RTU's.

R[1.C.iii] Poke points to sort RTU's by FEP line address – all FEP's or one at a time.

R[1.C.iv] Poke points to sort by status – offline RTU's at the top. RTU's are then sorted by address.

R[1.C.v] Poke point to bring up the RTU station schematic.

R[1.C.vi] If RTU is operational.

R[1.C.vii] Protocol Definition.

R[1.C.viii] Poke point to allow a URL link to a document providing RTU specific data.

R[1.C.ix] Indication point to show if the RTU has SOE.

R[1.C.x] FEP/FEP comm. Line and RTU address listed with ability to change them.

R[1.C.xi] Offline/online poke point next to RTU status.

R[1.C.xii] Comm. line transaction and error counts for the hour.

R[2] This facility shall interface to the IS&R Historian to save hourly RTU communications statistics and calculated RTU availability.

6.2 TASE.2 Data Exchange

R[1] The ADMS-SCADA shall support the Telecontrol Application Service Element (TASE.2) protocol, also known as the Inter-Control Center Communications Protocol (ICCP) to exchange data and information messages with other AE-owned systems.

R[2] The secure version of ICCP (which includes the capability for simultaneous secure and non-secure associations) must be provided.

R[3] The ADMS-SCADA shall be fully compliant with the IEC 870-6-503 Version 1996-08, TASE.2 Services and Protocol, and IEC 870-6-802 Version 1996-08, TASE.2 Object Models, Conformance Blocks 1, 2, 3, 4, 5, 7, and the basic structures of Block 8.

R[4] A programming interface, for use by user-written applications, shall be provided to accept information messages into Block 4 messages and subsequent transmission of the messages.

R[5] The programming interface shall also include features to notify recipient applications of arriving messages and to transfer the contents of the message to the applications.

R[6] Selected messages, configurable by AE, shall be transferred to the ADMS-SCADA System Alarm and Event logs.

R[7] The ADMS-SCADA shall provide the capability to monitor TASE.2 connections and traffic for the purposes of diagnosing problems and verifying configuration.

R[8] The ADMS-SCADA shall also provide the ability to alarm failures at both association and dataset levels.

6.2.1 TASE.2 User Interface Requirements

R[1] A User Interface (UI) shall be provided with operational tools to enable the user to maintain the TASE.2 database and monitor TASE.2 link performance.

R[2] Displays shall also be provided to enable the Operator to view availability of TASE.2 systems and the status of each TASE.2 connection.

R[3] The user shall be able to access the TASE.2 system remotely, with required access security controls, for problem determination and resolution.

6.2.1.1 Database Maintenance - Bilateral Table Creation and Editing

R[1] The ICCP data definitions shall be maintained with tools that integrate with and interact with the ADMS-SCADA database maintenance tools (Section 2.2.5.1) and that maintain the ICCP data definitions in the same logical database as the ADMS-SCADA data.

R[2] A user interface shall be supplied to facilitate entry and modification of the Bilateral Table data.

R[3] The interface shall be designed to lead the user in a stepwise fashion to perform the desired editing or data entry function and to prevent accidental or intentional changes to the Bilateral Table data by unauthorized personnel.

R[4] It shall be possible to create or edit a Bilateral Table while the system is on-line and operating and to create a Bilateral Table by making a copy of existing data.

R[5] The user shall be able to edit a Bilateral Table by entering data into a temporary area that is not activated until a specific command is issued. It shall be possible, by user command, to revert to a previous Bilateral Table.

R[6] TASE.2 database configuration (Data Engineering) shall be done using the Database and Display Construction utility.

R[7] Consistency checks and data type validation shall be performed.

R[8] The ADMS-SCADA database maintenance tools shall include a feature that coordinates the usage of data by ICCP and the ADMS-SCADA database.

R[9] If a data point is deleted or changed in the ADMS-SCADA database such that the internal reference is no longer valid, the tools shall enumerate all uses of the data in ICCP data Bilateral Tables and Datasets.

6.2.1.2 Database Maintenance - Data Set Creation and Editing

R[1] The ADMS-SCADA shall include displays facilitating the creation and editing of data sets.

R[2] The interface shall be designed to lead the user in a stepwise and logical fashion to perform the desired editing or data entry function and to prevent accidental or intentional changes to data sets by unauthorized personnel.

R[3] Displays shall be provided to permit creation and editing of Transfer Account objects.

R[4] Displays shall be provided wherein a TASE.2 client can view the Bilateral Table of a compliant server to determine what objects the client is permitted to access.

R[5] The capability shall be provided via point–and-click to select desired data objects and create data sets for Block 1 data without having to manually enter the selected point information.

R[6] Changes to the Bilateral Table shall be highlighted to aid the client in determining what objects have changed (i.e., been added, deleted, or modified) since the last update.

R[7] Messages that automatically and dynamically define datasets shall be sent when transfers are started.

R[8] This ensures that the remote systems definition of the dataset matches the local definition.

R[9] TASE.2 shall also support incoming Dataset Creation and Deletion requests and shall dynamically create server datasets as necessary.

R[10] It shall be possible for the client to create and delete Data Sets in the server, and to restart individual associations without restarting TASE.2.

R[11] TASE.2 shall support collection of a data item under one Object ID and sending the same data item under another Object ID.

R[12] Data set creation shall validate all model changes (data items and connection) before TASE.2 model deployment.

R[13] Data set creation shall support creating partial data sets.

R[14] A display facility that can show the actual data in each dataset that is available to each external entity that is data from AE via TASE.2 is required to check the functionality of the process.

6.2.1.3 Operational Monitoring and Control - Connection and Association Control

R[1] The ADMS-SCADA software shall include displays that enable a user to exercise control over TASE.2 data link software and manage Associations (e.g., Associate, Conclude, and Abort).

R[2] TASE.2 functionality shall include the following display features:

R[2.A] An overview display shall be provided which shows the roles and availability of primary and backup TASE.2 systems.

R[2.A.i] This display shall include pages to show the roles and availability in both a tabular and graphical format.

R[2.A.ii] The graphical display shall use full graphics capabilities and color to visually diagram the TASE.2 connections and indicate TASE.2 system status (e.g., primary, backup) and availability (e.g., available, off-line).

R[2.A.iii] Both the status of ADMS-SCADA systems and other remote computer systems that are active shall be shown.

R[2.A.iv] The ADMS-SCADA shall save the site status information to allow this data to be transmitted to other sites over the TASE.2 link.

R[2.B] An overview display shall be provided which shows the status of each connection (e.g., active, available, off-line, or error).

R[2.B.i] On a connection basis, controls shall be provided for: separate bilateral agreement, bilateral agreement number, and retry connection rate.

R[2.B.ii] The User shall be able to control permissions on a point-by-point basis (both for Domain and VMD data) per connection.

R[2.B.iii] This display shall include pages to show the connection status in both a tabular and graphical format. The graphical display shall use full graphics capabilities and color to visually diagram the TASE.2 connections and indicate their status.

R[2.B.iv] The connection status shall include status of ADMS-SCADA systems and other computer systems at the remote end.

R[2.B.v] The connection status shall also be available for alarming.

R[2.C] Displays shall be provided which allows the Operator or user to view and control configured Associations and Dataset.

R[2.C.i] This display shall include the Association/Dataset name, type, state, date and time of transmit, Master slave attribute, and all parameters related to the Association/Dataset.

R[2.C.ii] Color shall be used to distinguish active and inactive Associations.

R[2.C.iii] The time of creation and end time of each Association shall be shown.

R[2.C.iv] This display shall show a list of the TASE.2 systems and connections for user selection.

R[2.C.v] The display shall provide the capability for a user to disable Associations. Disabling Associations implies a graceful close of any existing Associations.

R[2.C.vi] Entry capability shall be provided for the Operator or user to enter the In-service or Out-of-service status tag for each Association/Dataset or possible Association./Dataset.

R[2.C.vii] For example, TASE.2 systems in alternate control centers will be placed out-of-service until needed.

R[2.C.viii] TASE.2 shall dynamically control each Association based on the user–entered in or out of service tag.

R[2.D] Displays shall be provided which allow the Operator or user to view the contents of Datasets.

R[2.D.i] This display shall allow the user to view any dataset either locally created or created by one of the attached remotes.

R[2.D.ii] This display shall include a list of all the data items contained within the Dataset.

R[2.D.iii] In addition to the data item name, the display shall list, for each data item the following information: the value/state, sign, time tag (last received), last time of change, ICCP quality code, AE quality code and the Object ID.

6.2.1.4 Maintenance and Support Tools

R[1] The TASE.2 system shall provide tools to allow the user to view and maintain the TASE.2 system and database.

R[2] These tools shall allow the user to select a particular data set, connection, or association (or all) to view and modify the selection.

R[3] The maintenance tools shall provide the following features:

R[3.A] Display parameters of data set objects (created by both sides of a connection) including: descriptions, triggers, transmit, and time of creation.

R[3.A.i] The tools shall allow the user to perform the following operations for manipulating Data Set objects: Create Data Set, Delete Data Set, Get Data Set Element Values, Set Data Set Element Values, Get Data Set Names, and Get Data Set Element Names. In addition, the tools shall have the ability to monitor iccp traffic in real time.

R[3.B] The ADMS-SCADA shall provide a mechanism (e.g., via system parameters, etc.) to coordinate the mapping of ADMS-SCADA quality codes to ICCP quality codes, to allow AE to define which codes are received and passed to/from ICCP.

R[3.C] Display the contents of a dataset and each data point value, sign, time tagged (time last received), last time of change, and quality code (both ADMS-SCADA and TASE.2 quality codes).

R[3.C.i] The tools shall allow the user to perform the following operations for manipulating Data Value objects: Get Data Value, Set Data Value, Get Data Value Names, and Get Data Value Type.

R[3.D] Display all data items by data set (Block 1 & 2) including: Object ID (including Indication Point or Control Point), the attributes Point Value/Sign, TASE.2 Quality, Select-Before-Operate (if applicable), and Time Stamp and Change of Value counter (when available).

R[3.E] Display the complete contents of Block 4 and Block 8 messages.

R[3.F] Display all data items Source and Source Object ID along with Consumers Object IDs.

R[3.G] Maintain a log of all ICCP messages and data transferred.

R[3.G.i] These log files shall be sized to retain a minimum of 4 days of data.

R[3.G.ii] The log files shall include the date and time of creation, and shall allow AE to archive or save a specific day’s log files if additional investigation is required.

R[3.G.iii] The log facility shall include a UI to allow AE to review specific stored content and the ongoing data transfers as they occur.

R[3.G.iv] Also, the UI shall allow the user to filter and search for specific data, associations, sites, etc. and, at Operator request, to freeze the data being viewed when current incoming data is being observed.

R[3.H] Provide an interface to the MMS-EASE debug facility, which can be activated or deactivated on user command.

R[3.H.i] The MMS_EASE debug tool shall provide the user with tools to help solve TASE.2 problems.

R[3.I] Provide tools to perform IP pinging of any connection.

6.2.1.5 Performance Monitoring

R[1] The TASE.2 Quality of Service (QOS) attribute shall provide the user with performance statistics on a connection and association basis (e.g., uptime, disconnects, etc.).

R[2] Performance statistics shall include: throughput, residual error rate, priority, transit delay, and protection.

R[3] Displays shall be provided to allow the user to select the connection, association, or all connections or associations and view the performance statistics for the selection.

6.3 Data Processing

R[1] The ADMS-SCADA shall support the following types of data processing:

R[1.A] Data quality

R[1.B] Analog data

R[1.C] Status data

R[1.D] Accumulator data

R[1.E] Sequence of Events data

R[1.F] Non-Telemetered data

R[1.G] Calculated data

R[1.H] Non-Commissioned data

R[1.I] Redundant data

6.3.1 Data Quality

R[1] Quality codes that apply to a point shall be maintained in the database for that point and shall be accessible for display, inclusion in reports, and use by ADMS-SCADA functions.

R[2] Typically, only the highest priority will be presented on a display or report.

R[3] However, it shall be possible to access and present the most severe code and all codes individually.

R[4] Please refer to Section 4.5.2.2 for a description of the display capabilities for quality codes and Section 4.7 for a description of the Device Information Displays.

R[5] For calculated data, the presence of a quality code on any of its arguments shall not disrupt the calculation using that value.

R[6] The propagation of quality codes in calculations shall be selectable on an individual calculation basis, defined when the calculation is created.

R[7] When selected for propagation, the quality code of the calculated value shall be the highest priority quality code of the arguments.

R[8] Results of calculations that are manually overridden by users shall be denoted with a quality code that can be differentiated from the propagation of a "manual substitution" quality code from one its arguments.

R[9] Quality codes included with data from data sources using standard protocols such as DNP 3.0 and TASE.2 shall be mapped to the ADMS-SCADA's quality codes.

R[10] Similarly, data transmitted from the ADMS-SCADA to other computer systems using the TASE.2 protocol shall map ADMS-SCADA quality codes to TASE.2 quality codes.

R[11] A preliminary mapping in presented in Exhibit 6-1: Quality Codes.

R[12] The mapping of quality codes shall be determined during project implementation.

R[13] Exhibit 6-1: Quality Codes presents the required minimum set of data quality codes defined in this RFP, mappings for protocol quality codes, and the propagation of the quality code to the result of a calculation.

R[14] The table is ordered in the priority order (highest priority first) preferred by AE.

R[15] The priority order shall be defined by AE during the project implementation and shall be adjustable.

Exhibit 6-1: Quality Codes

Quality Code	Protocol Quality Code Mapping			Propagate input point to calculated point result?
	DNP 3.0	TASE.2		
		To ADMS-SCADA	From ADMS-SCADA	
1) Implemented				No
2) Non-commissioned data				Yes
3) Test Mode				Yes
4) Unacknowledged Alarm				No
5) Persistent Alarm				No
6) Remote Manual Entry	Local forced data, remote forced data	Valid & Entered*	Valid & Entered	No
7) Manual Entry	Local forced data, remote forced data		Valid & Entered	No
8) Updated (opposite of Telemetry Failure)		Valid	Valid	No
9) Control Blocked				
10) Invalid				Yes
11) Alarm Inhibit				No
12) Secondary Source				No
13) Control Pending				No
14) Deactivated/Out of Scan			Suspect	Yes
15) Abnormal/Off-Normal				Yes
16) Suspect (e.g., ADC error)				Yes
17) Calculation Failure				Yes

Quality Code	Protocol Quality Code Mapping			Propagate input point to calculated point result?
	DNP 3.0	TASE.2		
		To ADMS-SCADA	From ADMS-SCADA	
18) Telemetry Failure (opposite of updated)	Off-line, communication lost	Held, Suspect, Not valid	Not Valid	Yes

6.3.2 Analog Data

R[1] Prior to storage in the ADMS-SCADA database, analog data shall be processed as follows:

R[1.A] *ADC accuracy monitoring* – Selected data sources will report one or two reference points for each analog-to-digital (ADC) converter in the source. These reference points shall be scanned as part of the normal data acquisition process and compared against high and low limits. The ADMS-SCADA shall provide the capability to associate telemetered data points to an ADC, and if points are not associated in this manner, the ADC accuracy checking shall not affect the quality of the data.

R[1.B] *Reasonability checking* – All analog points shall be compared against high and low reasonability limits each time they are processed.

R[1.C] *Conversion to engineering units* – Analog points shall be converted to engineering units by assuming a linear characteristic of the form:

$$Converted\_value = (a * Telemetered\_value) + b$$

or using 'expanded scale' transducers'

$$\begin{aligned}
&if\ (Telemetered_value \geq z) \\
&Converted_value = (a * Telemetered_value) + b \\
&else \\
&Converted_value = 0
\end{aligned}$$

where a and b are as above and z is a positive value defining the lower limit of the transducer.

R[1.D] *Limit checking* – All analog points shall be compared against operating limits (5 pair) that define various operating ranges for the point. Pairs of high and low limits shall be supported for each point.

R[1.D.i] Limit checking shall include features to provide timer-based alarms for bulk power system equipment data points as Overload Monitor limits and for other analog data points as a basic time delayed alarming feature, configurable on a group/point type basis and on an individual point basis.

R[1.E] A *deadband* shall be applied to each of the limits to derive the return-to-normal level, so that repeated alarming does not occur when the value of a point repeatedly crosses a limit. A return to normal deadband shall be defined to make sure analog values returning back to their normal state come out of the limit violation alarm.

R[1.E.i] It shall be possible to specify a unique deadband for each analog point.

R[1.F] *Sudden Deviation/Rate-of-change checking* – An alarm shall be generated when the change in the value of the analog point over a user-defined time interval for each point (multiple of the scan rate, in the range of 2 seconds to 5 minutes) exceeds the point's rate-of-change limit.

R[1.F.i]Default values shall be established based on point device types.

R[1.G] Periodic average/hourly average – the ADMS-SCADA shall calculate periodic averages (configurable duration, initially 15 minutes) and hourly averages for all analog points.

R[1.G.i] These averages shall be available via pop-up window on one-line or other displays that show the base point, when selected by the Operator.

R[2] The ADMS-SCADA shall support operating limit sets (refer to Section 6.3.2.2). Each operating limit set shall include an entry for each operating limit in the database.

6.3.2.1 Overload Monitor and Timer-Based Alarm Limits

R[1] The ADMS-SCADA shall include the capability for Overload Monitor alarm processing and timer-based alarm limits.

R[2] The details of these functions are described in the subsections below.

R[3] For Overload Monitor alarm processing, every 10 seconds, up to 5000 AE-specified measurements shall be checked for overload (or potential overload) conditions by comparing a telemetered or calculated MVA value against a set of four Engineer/Programmer-changeable overload limits.

R[4] The limits shall represent increasing levels of concern and be named “Normal (NOR)” “Long Time Emergency (LTE)”, “Short Time Emergency (STE)”, and “Drastic Action Limit (DAL)”.

6.3.2.1.1 Timer-Based Alarm Limits

R[1] The ADMS-SCADA shall include Timer-Based Alarm processing that provides Operators with automated notification when a point value violates alarm limits over a period of time.

R[2] This feature shall be configurable on a per-point basis.

R[3] Analog points shall have the ability to assign a general timer-based alarm to the first three (3) limit pairs.

R[4] These timers shall be referred to by their associated limit pair number (i.e. limit pair 1 timer, limit pair 2 timer, etc.)

R[5] Specific features of the timer-based alarms are as follows:

R[5.A] A different time value can be assigned to each timer defined for an analog point.

R[5.B] Once a limit is violated (and the initial alarm is generated) and a timer is activated, the timer shall start to decrement from its initial value.

R[5.C] If more than 1 limit is violated, the system shall maintain and initiate additional timers for each violated point limit.

R[5.D] An alarm shall be generated indicating that the timer has expired whenever a timer reaches zero.

R[5.E] If an analog point with an active timer returns to a value within the limits associated with the timer before the timer has expired, then that particular timer shall be deactivated.

R[5.E.i] If any other limits are still being violated for that specific point when this occurs, those timers shall remain active.

R[5.F] Initial timer values shall be editable using the standard database editing tools, including system-wide default timer values.

R[5.G] The display editing subsystem shall support the capability of linking timers to displays.

R[5.G.i] The display shall show the time remaining for an active timer. If a point has more than one (1) active timer, the display shall reflect the timer with the earliest expiration.

R[5.H] Deactivated timers shall be removed from all displays.

6.3.2.1.2 Seasonal Limits for Overload Monitored Data

R[1] Each monitored point shall have one summer, one winter, one Spring/Fall and one manual set of limits associated with it.

R[2] The change of limits from one season to the next shall be scheduled to occur automatically at 00:01 on the respective season transition date.

R[3] The Operator shall also have the ability to designate which of the sets will become the active set.

R[4] The current season shall be determined by Engineer/Programmer-changeable season demarcation dates.

R[5] Two sets of summer/winter start dates shall be provided, one set for overhead lines and one set for underground lines.

R[6] Summer ratings are typically in effect from April 1 through October 31. Winter ratings are typically in effect from November 1 through March 31.

R[7] The Operator shall be able to override the current season and select a set of limits from the alternate season to accommodate atypical weather conditions.

R[8] This override shall be in effect for the current day, after which the previously selected limit set shall be reinstated.

R[9] The Operator shall also be able to change the limit set on a per point basis, as well as for all monitored elements.

R[10] These limits shall be used as the active limits until reset by the Operator or reset automatically by the season change.

R[11] The manual set may not contain values for all limits, but will only contain those that have been normally entered by the Operator.

R[12] When the manual set is selected, only those valid limits, which have been entered by the Operator, shall be copied into the active set.

R[13] The Operator shall also be able to manually enter a limit. It shall be retained in the manual limit set, and may be selected individually or as a group (for those points which have had manual limits entered) to become part of the active set.

R[14] The Operator shall be able to disable the automatic seasonal limit switchover for points that have been manually entered.

R[15] The Operator shall be able to select to override manually-entered limits either individually or as a group by reloading default limits from the summer or winter set.

R[16] Overridden manual limits shall be retained in the manual limit set for future use.

6.3.2.2 Alternate Limit Sets

R[1] The ADMS-SCADA shall include the different sets of operating limits, such as seasonal Summer Ratings, Winter Ratings, and Spring/Fall Ratings in different modalities like day and night or normal and emergency.

R[2] The ADMS-SCADA shall have the ability to switch the sets of operating limits based on dates of the year, time of the day, temperature and system status, i.e. normal or emergency, as determined by the dispatcher.

R[3] Only one set of seasonal ratings shall be active at any given time.

R[4] Each set of seasonal ratings shall include an entry for the defined normal and overload monitor limits for each analog point.

R[5] The ADMS-SCADA shall allow the user to overwrite the current operating ratings for all the monitoring facilities with another alternative operating limit set. (e.g. from Summer to Spring/Fall

R[6] The switch of operating limits shall be documented with an event message which shall include the identifier of the workstation which made the switch.

R[7] If a rating does not exist for a particular point, the existing rating will not be changed when the set changes.

R[8] These seasonal operating limit sets shall consist of the most recent values of those limits in the ADMS-SCADA database for the limit set currently in effect.

R[9] Ability to dynamically change the sets of operating limits based on weather conditions, mostly temperature, shall be available.

R[10] Ability to dynamically change individual limits based on local weather conditions, temperature, wind velocity and direction, and other parameters such as conductor tension, or sag shall be provided.

6.3.2.3 Limit Manager

R[1] A Limit Manager function shall control the current operational set of limits (both normal and overload monitor limits), switching the Summer, Winter, Spring, or Fall set into the current set and managing manual limit entries to the current set.

R[2] The Limit Manager function shall include a Line Ratings Display to assist AE in maintaining these operational parameters.

6.3.2.3.1 Line Ratings Display

R[1] The ADMS-SCADA shall include a Line Ratings display that presents the following information for each monitored facility:

R[1.A] The name of the monitored facility;

R[1.B] The current value and measurement units of the telemetry value;

R[1.C] The 3 or 4 ratings currently in effect (NOR, LTE, STE, DAL)

R[1.D] The dead band to be applied to the telemetry value for this monitored facility;

R[1.E] A place to inhibit the alarm;

R[1.F] An indication of which set or ratings (Summer or Winter) is effect;

R[1.G] A place to change from Summer to Winter and back again.

R[2] When a facility is selected for dynamic rating a new display shall be presented that allows the user to enter a dynamic rating.

R[3] A display shall also be provided to allow the user to change the Summer and Winter seasonal ratings. The display shall contain the following information:

R[3.A] The name of the monitored facility;

R[3.B] The current value and measurement units of the telemetry value;

R[3.C] The full scale value of the telemetry point;

R[3.D] The three/four Summer and three/four Winter seasonal ratings.

R[4] The Line Ratings Display shall provide the following additional functionality:

R[4.A] Ability to link 3 Ampere measurements to a MW measurement and automatically rate (and derate) the MVA, MW and Ampere ratings (configurable) from the MW rating.

R[4.B] Ability to sort list by:

R[4.B.i.a] Alphanumerically

R[4.B.i.b] Closest to Normal Limit (calculated by the ADMS-SCADA)

R[4.B.i.c] Points that have full-scale problems

R[4.C] Ability to identify MW values (i.e. by color coding) that have rating limits that are greater than the full scale of the data point)

R[4.D] Ability to issue a message when a MW value is at full scale

R[4.E] Ability to toggle between Ampere values and their associated MW values

R[4.F] Display the current telemetry value along with the limits

6.3.2.4 ADMS-SCADA Sign Convention

R[1] The ADMS-SCADA shall be designed to be easily configurable to support various sign convention schemes.

R[2] The sign convention is a function of the metering point of the element being monitored.

R[3] For points whose metering causes reversal of sign, the point's conversion factors shall be used to adjust the sign.

R[4] A database flag shall exist on a per point basis, so that the sign may be reversed in different applications subsystems (e.g., SCADA, Network Analysis).

6.3.3 Status Data

R[1] Status data shall be processed to convert the input data to a meaningful state and to identify and report changes in state.

R[2] Status data shall be used to represent breakers, substation alarm points, etc.

R[3] A listing of all status points shall be presented on an automatically generated station tabular.

6.3.3.1 State Conversion

R[1] The ADMS-SCADA shall include the following state data conversions.

R[1.A] *Two-state points*, typically reported as a single bit, that represent one of two possible states of a power system device or other equipment or process:

R[1.B] *Three-state points*, typically reported as two bits, which represent one of three possible states of a power system device or other equipment or process:

R[1.C] *Multi-state points*, typically reported as two bits, which represent one of four possible states of a power system device or other equipment or process:

R[1.D] *Momentary change detection (MCD)* – two-state points that may incur multiple operations between scans: Typically, such points are identified with circuit breakers with high-speed reclosers. The ADMS-SCADA shall scan MCD points immediately after a control operation, to detect any rapid subsequent state change in order to correctly alarm if the control operated successfully but changed state again after the control.

R[2] Some protocols may report multiple operations of any device as a series of operations of the same device all transmitted in the same message.

R[3] The ADMS-SCADA shall process all reported changes of any device within a message.

R[4] The ADMS-SCADA shall also process all indication status bits returned by an RTU for each data point, reflecting the state of the reported status measurement.

R[5] For manual status points (not telemetered or control points), the ADMS-SCADA shall allow the Operator to manually substitute a state value for multiple points by selecting (e.g., windows multi-point select, rubber-banding) multiple manual points and selecting data entry for the points.

R[6] The ADMS-SCADA shall include a state-table to allow AE to associate the various state conditions with different textual representations of the states of the data point (e.g., open-closed, trip-close, raise-lower).

R[7] Data point processing shall also include the ability to invert the state of the data point before data processing is performed.

6.3.3.2 Normal State Processing

R[1] One of the states of each status point shall be designated as its “normal” state.

R[2] The designation shall be made individually for each point. It shall also be possible to define a point as having no normal state.

R[3] Users shall be able to override the normal state definition and to remove the override.

R[4] Overriding the normal state designation shall establish a normal state override quality code on the point in the ADMS-SCADA.

R[5] Removal of the normal state override shall remove the normal state override quality code.

R[6] All points with an overridden normal state shall be listed on the off-normal summary display.

6.3.3.3 State Change Detection

R[1] Each time a status value is acquired, its state shall be compared to the state currently resident in the database and any change of state shall be reported.

R[2] Changes in state that are the direct result of a supervisory control action initiated within the ADMS-SCADA shall be reported as events.

R[3] Spontaneous changes in state shall be reported as alarms.

6.3.4 Accumulator Data

R[1] Prior to storage in the ADMS-SCADA database, accumulator data shall be processed as follows:

R[1.A] *Conversion to engineering units* – Data sources will report accumulator points in two forms, as a continuous count value and as a resetting value.

R[1.A.i] Data reported in continuous (non-resetting) count form shall be converted using the following linear conversion algorithm:

$$Converted\_value = a * (Raw\_value_n - Raw\_value_{n-1})$$

R[1.A.ii] Note: The above conversion algorithm shall accommodate the rollover of the accumulator to zero when the accumulator reaches the maximum value for the accumulator, configurable on a per point basis.

R[1.A.iii] Data reported in resetting count form shall be converted using the following linear conversion algorithm:

$$Converted\_value = a * (Raw\_value_n)$$

R[1.B] *Reasonability checking* – All converted accumulator values shall be compared against high and low reasonability limits. The reasonability limits shall represent the extremes of valid measurements for the point's value.

R[1.C] *Limit checking* – All accumulator points shall be compared against high and low operating limit pairs.

R[1.D] *Accumulator Comparison* – The ADMS-SCADA shall support the comparison of other data for invalid accumulator values. The comparison shall be triggered by any of the following conditions:

R[1.D.i] Telemetry failure of an accumulator point

R[1.D.ii] An accumulator point with a long value quality code

R[1.D.iii] When the difference between the accumulator value and another analog or accumulator value (typically a calculated analog value) exceeds a predefined value (a "meter error").

R[1.E] *Suspect Accumulator Values* – When an RTU reports a powerfail or reboot, any accumulators associated with the RTU shall be marked as suspect.

6.3.5 Sequence of Events Data

R[1] SOE data shall be stored in the IS&R function for presentation on displays and reports. SOE data shall also be transferred to the Historian as soon as it is received to allow users rapid access to sequence of events data.

R[2] The ADMS-SCADA shall include an SOE Event List Summary to show SOE event data, in addition to the system event list.

R[3] This Event List Summary shall allow the user to sort and filter SOE events to display areas of interest (e.g., sort and filter by specific points, RTU, substation, area, voltage level).

R[4] All SOE data shall be stored with one millisecond resolution.

6.3.6 Non-Telemetered Data

R[1] Certain data in the database will be manually entered by the users.

R[2] These data points shall include analog, accumulator, and status points.

R[3] Event messages shall be generated for each change made to a non-telemetered value. Non-telemetered points shall be shown as implemented points that are processed as updated, but as a default not displayed with a ‘telemetry failure’ quality code or a ‘manual entry’ quality code.

R[4] The display generation utility shall allow the user to select to show these quality codes.

6.3.7 Calculated Data

R[1] Calculated points shall be derived from AE-defined algorithms (generalized calculations) and pre-defined algorithms supplied with the ADMS-SCADA (such as MVA calculations and analog value integration).

R[2] This RFP assumes that calculations will be performed periodically and that the periodicity of calculations shall be assigned on a per-point basis, or where a calculation is triggered whenever any of the arguments of the calculation change is also acceptable.

R[3] The ADMS-SCADA shall allow the user to enable/disable quality code propagation for individual calculations.

R[4] It shall be possible to suspend and enable the calculation of any calculated data point.

R[5] It shall be possible to use any value of any type from the database for arguments of the calculation, including other calculated points and values produced by ADMS-SCADA functions.

R[6] The calculation function shall detect arithmetic exceptions such as division by zero and over-range results and shall place a “calculation failure” quality code on the resultant calculated point.

R[7] Any calculation failure shall be able to generate an alarm to annunciate the failure. If an input or output point shall become undefined, an alarm shall be generated.

R[8] This failure shall not impact other calculations execution.

6.3.7.1 Generalized Calculations

R[1] Generalized calculations shall be defined from the following operators and rules:

R[1.A] *Mathematical operators* – addition, subtraction, multiplication, division, square root extraction, exponentiation, and logarithmic functions

R[1.B] *Trigonometric functions* – including sin, cos, tan, and inverse functions

R[1.C] *Min/max functions* – selection of the minimum and maximum value from a set of arguments

R[1.D] *Logical operators* – including AND, OR, NOT, and XOR

R[1.E] *Comparative operators* – including greater and less than, equal to, and combinations thereof

R[1.F] *Conditional execution operators* – including if-then-else statements.

R[2] Each calculation may consist of multiple arguments.

R[3] Multi-level parenthesis shall be supported. It shall be possible to use the quality codes of database values for use as arguments.

R[4] The Vendor shall propose an option to allow the user to display multi-level calculations (that interact and call each other) by drilling down through the multiple levels of calculation definitions.

6.3.7.2 Integration

R[1] The integration calculation will typically be used to produce MWh and Mvarh values from MW and Mvar inputs respectively.

R[2] The integration period shall be defined for each point and the result for the current period stored and a new integration started at the end of each period.

R[3] Two values shall be maintained in the database as analog values for each integration point:

R[3.A] *The current value* – the value for the current (in-progress) period

R[3.B] *The previous value* – the result for the previous (completed) period.

R[4] Failovers and Switchover shall not diminish the accuracy of the integration calculation.

6.3.7.3 Processing of Calculated Data

R[1] After a data item is calculated, it shall be processed as follows:

R[1.A] Analog value

R[1.A.i] Reasonability limit checking

R[1.A.ii] Operating limit checking

R[1.A.iii] Rate-of-change checking

R[1.B] Status value:

R[1.B.i] Normal state checking

R[1.B.ii] Change checking

R[1.C] Accumulator value:

R[1.C.i] Reasonability limit checking

R[1.C.ii] Operating limit checking

6.3.7.4 Nth Generation Programming Language

R[1] The ADMS-SCADA shall include an advanced Nth Generation Programming Language to allow AE to create advanced control and automation schemes.

R[2] This facility will allow a programmer/controls engineer to create independent control sequences that will utilize permissives (from ADMS-SCADA data), advanced calculations, all types of control outputs, control feedback, and other additional features.

R[3] This facility shall include an advanced control, scheduling, and display facility to enable development and monitoring of the control sequences created

R[4] This facility shall permit multiple supervisory control commands to be programmed for automatic execution in a predefined sequence.

R[5] Commands to be supported shall include:

- R[5.A] All supervisory control commands
- R[5.B] Pause execution for a given time delay
- R[5.C] Stop execution until an user commanded restart or continue
- R[5.D] Conditional check before execution
- R[5.E] Jump (pass control to another sequence)
- R[5.F] Manual Entry.

R[6] After executing a supervisory control action, the facility shall support a function to pause to obtain an indication of a successful control completion check.

R[7] If the control completion check is not received, or does not have the expected value, the ADMS-SCADA shall terminate the execution of the sequence and shall declare an alarm.

R[8] Apart from waiting for control completion checks, and unless there is an explicit command for a delay, such as a “Pause” or “Stop” command, the ADMS-SCADA shall not introduce any artificial delays in the execution of an command sequence.

R[9] The control completion check pause shall be configurable to allow no pause in circumstances where a feedback is not available or the control sequence author does not want to delay the rapid output of a set of controls.

R[10] No limit shall be placed on the number of command sequences, which may execute in parallel.

R[11] The following manipulation of lists shall be possible:

R[11.A] Display a catalog of the lists

R[11.B] Display, build, copy, edit, and delete a list

R[11.C] Name the list and enter a description

R[11.D] Store the list

R[11.E] Select the list for execution

R[11.F] Execute the list.

R[12] At any time during the execution of a list, the user shall be able to stop further execution via a cancel feature.

R[13] In addition, telemetry and control permissive checks shall be incorporated in the sequence with user override capability.

R[14] Upon failure of the telemetry and control permissive checks, the sequence shall pause and require user interaction.

R[15] Resumption of the sequence at any point shall be provided.

R[16] Initiation of any list shall be recorded as events, and events shall also be recorded noting the time of any “stop”, “continue”, or “cancel” command. All control malfunctions and control commands successfully.

6.3.8 Data and Test Quality Code

R[1] The non-commissioned attribute is used to indicate equipment that is being commissioned into service and is not currently being scanned or processed.

R[2] A unique quality code shall identify all such equipment on any ADMS-SCADA display or report and this quality code shall be applied/removed by the user.

R[3] It shall be possible to declare individual data points as non-commissioned.

R[4] It shall also be possible to declare a data source as non-commissioned in which case all data points within that data source shall have the non-commissioned attribute applied.

R[5] The Test Quality code is manually set by the Operator/user and is used to indicate that the data point is undergoing test.

R[6] The test tag or quality code shall allow the point to be scanned, but prevent generation of alarms or events in the system.

R[7] Control shall also be permissible for points with the test tag/quality code.

R[8] The intent is to allow for basic SCADA testing without interfering with normal operations or applications that could potentially pick-up these changes for reporting purposes.

R[9] Additionally, the test tag/quality code shall be used to differentiate points that have not been tested and released from points that are simply "alarm inhibited".

R[10] The ADMS-SCADA shall include a feature to create a summary of points with the Test quality code set.

6.4 Safety Tagging

R[1] Safety tags are conditions applied to database values in order to call the users' attention to exception conditions for field devices and to inhibit supervisory control actions.

6.4.1 Safety Tag Types and Supervisory Control Inhibit

R[1] The ADMS-SCADA shall support 32 safety tag types and 16 safety tags to be set on an individual point.

R[2] The safety tag types shall be ordered by AE to indicate its relative priority to other types.

R[3] The safety tag types and all of their characteristics shall be defined by AE to correspond with the field device-safety tagging scheme.

R[4] Examples of AE safety tag names are as follows:

R[4.A] Danger/ Hold (do not operate),

R[4.B] Information

R[4.C] Damaged

R[4.D] Ground

R[5] AE General Tag Characteristics

R[6] The definition shall include the safety tag type name , priority, its supervisory control inhibit properties, and the safety tag symbol, definable by AE.

R[7] The control-inhibit properties shall be selected by AE for each safety tag type from the following:

R[7.A] All control allowed

R[7.B] Control inhibited in one direction, such as close

R[7.C] Control inhibited in the other direction, such as trip

R[7.D] All control inhibited

R[8] The supervisory control function shall check for the presence of a control-inhibit tag as part of the control permissive scheme defined.

R[9] The ADMS-SCADA shall include an API to allow access to the Safety Tag function database, to allow AE to develop interfaces to other internal applications.

6.5 Supervisory Control

R[1] The ADMS-SCADA shall issue supervisory control commands to field devices when directed by a user or an application program.

R[2] Output of Control commands shall take priority over other ADMS-SCADA data acquisition tasks to ensure that these operations can be completed during periods of heavy system load and stress.

R[3] Control actions requested by a user shall include a confirmation step subsequent to selection of the field devices to be controlled and the control action to be commanded.

R[4] After the user confirms the control action, the supervisory control message exchange process shall be initiated.

R[5] The message exchange with the field devices shall use a select-checkback-execute command sequence if available in the protocol.

R[6] The execute command shall be issued only if select and checkback messages are exchanged without error and if the checkback message indicates that the correct field device and control action have been selected.

R[7] The select and execute messages shall not be retried. Any errors in the control command exchange shall be reported as alarms to the user and the command shall be cancelled.

R[8] If, after selecting a field device and control action, the user does not execute the control action within 20 seconds (a programmable interval) or if the user performs any action on the workstation other than executing the control action, the selection shall be cancelled and the user informed.

R[9] The user shall not be prevented from requesting other displays, performing a different supervisory control action, or performing any other operation while the ADMS-SCADA waits for a report-back on previously executed control actions.

6.5.1 Single State Control Devices (Relay Reset)

R[1] The ADMS-SCADA shall support the supervisory control of devices, such as underfrequency reset relays, that can only be commanded to one state.

R[2] It shall not be possible to select a command into the second state for these devices.

6.5.2 Two- and Three-State Control (Switching Devices)

R[1] Controllable switching devices include circuit breakers, reclosing relays, line reclosers, circuit switchers, and motor-operated disconnect switches.

R[2] Three-state points may also be commanded only into one of two states. It shall not be possible to select a command to a third or fourth state for three-state points.

R[3] Capability shall be provided to issue an open command to an open device (also a close command to a closed device).

6.5.3 Two- and Three-State Control – Delayed Close (Capacitor and Reactor Switching)

R[1] Selected two- and three-state control points shall be designated as “delayed close” points.

R[2] The procedure for controlling these devices shall be the same as that of a switching device except that any supervisory control action shall be inhibited for a specified interval after the switch has been opened.

R[3] The interval shall be determined by AE, and specified individually for every device subject to delayed close restrictions.

6.5.4 Incremental Control (Tap-Changing Transformers)

R[1] Incremental control is typically used to raise and lower the tap position of Load Tap Changing (LTC) transformers and the control settings of similar devices such as voltage regulators.

R[2] The initial selection and control of the device for a raise/lower operation shall follow a select-checkback-execute process.

R[3] For additional raise/lower operations, the user shall only have to repeat the desired number of raise/lower execute commands, which shall be performed immediately.

R[4] The user shall be able to cancel the operation at any time.

R[5] The ADMS-SCADA shall cancel the operation 20 seconds (initial value, timer shall be adjustable) after the most recent control execute has been issued or if the user performs any action on the workstation other than the control execute command.

R[6] The data acquisition function shall not be suspended between the times that repeated raise/lower execute commands are issued.

R[7] Control actions that would result in movement of the device beyond its defined operating range shall be rejected.

R[8] The ADMS-SCADA shall support display of the current tap setting as a set of text string identifiers (4 characters) that represent the current tap position of the LTC transformer.

R[9] This shall be accomplished by using "translation tables" which specify an analog telemetry point that represents tap position feedback from the field.

R[10] The analog telemetry value shall be used to locate an entry in a tap position/text string identifier table and display the appropriate text string to the Operator.

R[11] A tap translation table shall be definable for each transformer that AE wants to represent.

6.5.5 Setpoint Control

R[1] The ADMS-SCADA shall provide the capability to issue setpoint control to field equipment and to other computer systems, to indicate the desired operational setting of the device.

6.5.6 Control Completion Check

R[1] The response to control actions shall be verified by monitoring a feedback variable designated individually for selected control points.

R[2] If a feedback point is not defined for a control point, the control completion check shall be deemed successful as long as the control command is successfully transmitted to the field device.

R[3] A report-back timer, independently defined for each device, shall be started when the execute command is issued.

R[4] Each delay time shall be adjustable from two seconds to at least ten minutes with a one second resolution.

R[5] If an Operator requests a control action to move a device to its current state (e.g., open to open, or close to close) the ADMS-SCADA shall issue a fail to operate message.

R[6] A control action shall be deemed successful if the appropriate success indication described below is recognized prior to expiration of the report-back timer:

R[6.A] *For single-state and two-state devices (including delayed close devices)* – the corresponding status feedback point of the device under control changes to the desired state.

R[6.B] *For incremental control devices* – the corresponding analog feedback point of the device under control changes to the desired value, within a tolerance.

R[6.C] *For setpoint outputs* – the corresponding analog feedback point of the output under control changes to the desired value, within a tolerance.

R[7] Successful controls shall be recorded as an event. If the control was unsuccessful, an alarm shall be generated.

R[8] For supervisory control commands issued as part of a group control or load shedding operation the successful completion of all control actions shall be reported via a single message.

R[9] If any operation is unsuccessful, the user shall be informed of those devices in the group that failed to operate by individual alarms.

R[10] Where a supervisory control action is initiated by an application, the interface shall include features to report the success or failure of the control action to the application.

6.5.7 Control Permissive

R[1] The supervisory control function shall perform a permissive check immediately after the user has selected the device for a control action.

R[2] As part of this check, the User Interface shall only display those commands that are allowed based on the point's condition/state.

R[3] The presence of any, or all, of the following conditions for the selected point shall be deemed as a failure of the check:

R[3.A] A status value from the ADMS-SCADA database, designated for each controllable point, evaluates as true

R[3.B] A safety tag with a supervisory control inhibit property is set.

R[3.C] Supervisory Control Permission is disabled.

R[4] If the permissive check does not permit the control action, the user shall be informed of the failure by a message that clearly indicates the permissive failure and that differentiates among the check types.

R[5] If the permissive check passes, the control sequence shall proceed to the execute step.

R[6] Where a supervisory control action is initiated by a Vendor- or AE-supplied application, the interface shall include features to report the presence of a control-inhibit tag.

Table of Contents

7. Information Storage and Retrieval 7-1
   7.1 General Capabilities 7-1
      7.1.1 Database Preferences and Licensing 7-3
      7.1.2 IS&R Data Definition 7-3
      7.1.3 Data Collection 7-4
      7.1.4 IS&R Data Calculation 7-5
      7.1.5 Data Display and Editing 7-6
      7.1.6 Reports 7-7
      7.1.7 Audit Trail 7-7
      7.1.8 Data Archiving 7-8
   7.2 Specific Applications 7-8
      7.2.1 Alarm and Event Storage and Retrieval 7-9
      7.2.2 Periodic Data Recording 7-9
      7.2.3 Continuous Data Recording 7-10
      7.2.4 Sequence of Events Storage and Retrieval 7-10
      7.2.5 Communication Error Statistics and Availability Calculations 7-11
      7.2.6 Application Generated Historical Data 7-11

7. Information Storage and Retrieval

R[1] The information storage and retrieval requirements are presented both as general capabilities and as specific applications using the general capabilities.

R[2] The specific applications include:

R[2.A] Alarm and event storage and retrieval.

R[2.B] Periodic data storage.

R[2.C] Continuous data recording

R[2.D] Sequence of events storage and retrieval

R[2.E] Trouble calls

R[2.F] Outage restoration history

R[2.G] Operator actions (events)

R[2.H] Abnormal device states

R[2.I] Topology such that the state of the system can be reconstructed

7.1 General Capabilities

R[1] Information Storage and Retrieval (IS&R) shall consist of a relational database management system (RDBMS) capable of supporting two-tier client/server and three-tier client/application/server architecture.

R[2] Functionality shall be provided to capture values from the ADMS-SCADA database, calculate and store additional values, present the information on displays and reports, and to transfer near real-time data to a vendor supplied Historian system (PI or similar).

R[3] The ADMS shall have the ability to capture and playback events advancing at real time and reduced speed and stopping at any point in time to obtain snapshots.

R[4] The interface shall be provided to transfer those captured events and snapshots to the OTS.

R[5] Interface shall be provided to transfer data to simulation software such as ASPEN, PSCAD, EMPTP and similar programs as requested by AE.

R[6] Vendor shall be able to support PI Historian as an option to AE including the CIM XML interface.

R[7] The interface to the Historian shall be designed to use the native Historian interface to support buffering of data to prevent data loss, in case the Historian server is temporarily down.

R[8] Additionally, the interface to the PI Historian shall be designed to transfer data to a cluster of redundant PI Historian servers in order to prevent data loss.

R[9] Users shall access the IS&R database by using all of the data retrieval capabilities of the RDBMS.

R[10] Data retrieval shall meet the latest Structured Query Language (SQL) standard. ODBC (Open Database Connectivity) is required, with proven compatibility for the Microsoft Office[1] productivity suite and other common front-end software.

R[11] The Vendor shall provide database client software and any additional Vendor-developed client software needed to use the IS&R capabilities.

R[12] For the purposes of this IS&R function, “on-line” data is defined as data available within IS&R without requiring mounting of archive (storage) media.

R[13] Data stored on such media is considered archived or “off-line” data.

R[14] For IS&R Data, the retention period of 2 years is the minimum length of time the data shall be kept on-line.

R[15] Data older than the retention period may be transferred to archival storage (refer to Section 7.1.8).

[1] Microsoft Office is a registered trademark of Microsoft Corporation.

7.1.1 Database Preferences and Licensing

R[1] AE prefers the Oracle® 11i or higher Enterprise Edition RDBMS for general use and Oracle products for IS&R functionality.

R[2] The Vendor shall provide pricing for the necessary Oracle licensing and AE will decide if it will acquire Oracle software under AE's existing licenses or have the Vendor supply the Oracle licenses.

R[3] In either case, the Vendor shall clearly define all Oracle products to be included with the ADMS-SCADA, including software required for development of the ADMS-SCADA.

R[4] AE will license the software specified by the Vendor.

R[5] All licenses for IS&R software shall allow for "full use" of the software.

R[6] That is, the licenses shall provide for use by AE of all databases and applications delivered with the ADMS-SCADA as well as permit AE to develop additional applications and databases for their own purposes.

R[7] Exhibit 3 1: Number of Users specifies the number of simultaneous users, maximum accounts, and development users:

R[7.A] The number of simultaneous users specifies the maximum quantity of human users who may be using IS&R resources at any one time.

R[7.B] The maximum number of accounts specifies the total quantity of human users who will use IS&R resources over any period of time.

R[7.C] The number of development users specifies the maximum quantity of human users who may be developing or maintaining functionality and databases provided by the Vendor or developed by AE.

7.1.2 IS&R Data Definition

R[1] All data values, alarm/events lists, communications statistics (RTU and ICCP), and results of all applications, in the ADMS-SCADA shall be available for collection and storage into IS&R.

R[2] Data points that are to be collected shall be defined in the ADMS-SCADA database and shall not require separate IS&R definition.

R[3] All IS&R data shall remain retrievable regardless of content or structure changes to the ADMS-SCADA or IS&R databases.

R[4] The ADMS-SCADA database process to define data to be stored within IS&R shall automatically handle any data point that is renamed in or deleted from the ADMS-SCADA database using techniques that allow the previously stored IS&R data to be retrieved and accessed, including any redefinition or renaming of the data in the IS&R or Historian databases that is required.

7.1.3 Data Collection

R[1] Any data written to IS&R shall include all of the quality codes associated with each point, as well as all supervisory control safety tags. In addition, a quality code shall be provided to denote that a correction has been made to a point's value while in the IS&R database.

R[2] The IS&R database shall accommodate Daylight Saving Time (DST), time zones, and leap year automatic changes.

R[3] Data presentation (displays and reports) shall be automatically adjusted to accommodate Daylight Saving Time and/or Standard Time based on a user-defined flag.

R[4] For Daylight Saving Time on a short day, only twenty-three (23) hours shall be shown; on a long day, twenty-five (25) hours shall be shown.

R[5] Calculation of totals and averages shall be such that no data is lost on either long or short days.

R[6] Data to be written to both IS&R and the historian shall be buffered such that data will not be lost if IS&R or the historian is not available at the time the data is collected.

R[7] The ADMS-SCADA shall be sized to buffer a minimum of 1 week of data to protect against data loss in case the historian is down.

R[8] Data passed to IS&R and the historian shall be removed from the buffer only after positive feedback of the successful storage of data into both IS&R and the historian has been received.

7.1.4 IS&R Data Calculation

R[1] It shall be possible to perform predefined calculations on any collected data value at specified periodicities, when requested by a user, and when triggered by an application program. It shall also be possible to perform further calculations on previously calculated data and on constants.

R[2] These calculations shall be definable by the users via the RDBMS.

R[3] Common mathematical calculations including carry-forward (with and without integer truncation and carryover of the fractional value to the next time period) within a data set (particular snapshot in time) shall be supported.

R[4] Calculations of multiple samples (over time) of the same data value shall be supported:

R[4.A] Statistical measures (e.g., minimum, maximum, average, and total) for the following time periods:

R[4.A.i] Fifteen-minute using real-time samples. Sample rates shall be configurable.

R[4.A.ii] Half hourly using real-time samples. Sample rates shall be configurable.

R[4.A.iii] Hourly using real-time samples. Sample rates shall be configurable.

R[4.A.iv] AM and PM periods, where AE defines the hours in each period.

R[4.A.v] Daily using fifteen-minute samples. Sample rates shall be configurable.

R[4.A.vi] Weekly using fifteen-minute samples. Sample rates shall be configurable.

R[4.A.vii] Monthly using daily and fifteen-minute samples.

R[4.A.vii.a] Capabilities to save ‘n’ values for a pre-defined period, for example, five maximum and five minimum values, shall be supported.

R[4.A.viii] Yearly using monthly samples.

R[5] All calculated data shall include a quality code derived from the highest ranking of the quality codes of the data used in the calculation.

7.1.5 Data Display and Editing

R[1] IS&R data shall be available for display in tabular and graphic form using all of the capabilities of the RDBMS, including an ad hoc query capability.

R[2] The IS&R user interface shall comply with the general user interface requirements specified in Sections 4.1 and 4.6.

R[3] The Vendor shall provide the display building tools that support ad hoc data retrieval display as well as pre-defined displays.

R[4] The tools shall be GUI and web-based, allowing the user to see representative output from the report during the building procedures.

R[5] The data display function shall incorporate the following features as a minimum:

R[5.A] Menu driven data selection process.

R[5.B] Pre-formatted sets of data retrieval request displays.

R[5.C] Selection of data based on:

R[5.C.i] Date and time of collection.

R[5.C.ii] Comparative operations (equal to, greater than, etc.) on the value of fields within each stored item

R[5.D] Sets of predefined, generic access routines (i.e., templates) for typical types of access, such as all analog points at a specific time, maximum, minimum, and average of a value over a specific time period, all status points at a specific time etc.

R[5.E] Capability to define ad hoc queries to call for any specific value(s).

R[5.F] Restrictions on access to confidential information based on user access control.

R[6] Sufficient relationships shall be maintained between the IS&R data and the ADMS-SCADA database to ensure that selections can be made based on comparison between stored IS&R values (such as a periodically saved bus voltage value) and any related, fixed ADMS-SCADA value (such as the bus voltage limit).

R[7] When a display is called, the calling process shall include triggers to calculate additional data (refer to Section 7.1.4 for details of the possible calculations).

R[8] The calculated values may be defined as either permanent values (stored in the IS&R database) or temporary values (created for display only and retained only as long as needed for the display).

R[9] The User Interface shall be designed to allow data stored in the Historian to be displayed on ADMS-SCADA workstations and integrated into any ADMS-SCADA display.

R[10] The ADMS-SCADA shall also support export of IS&R data to .csv and Excel data files.

7.1.6 Reports

R[1] The Vendor shall provide report building tools that support ad hoc data retrieval reports as well as periodic and on-demand reports.

R[2] The tools shall be GUI and web-based, allowing the user to see representative output from the report during the definition process.

R[3] The reporting software shall have full read-only access to the IS&R database and real-time database; and shall support grouping, algebraic, logical, and arithmetic functions such as spreadsheet calculations, to allow for creation of reports.

R[4] The software provided preferably shall be a commercially available package capable of generating complex reports.

7.1.7 Audit Trail

R[1] An audit trail of all changes made to the IS&R database shall be maintained and made available for display and printout.

R[2] This audit trail shall identify every change made to the IS&R database structure and content, the time and date of the change, and the user ID and workstation identifier of the party making the change.

R[3] The audit trail shall include both before and after values of all content changes.

R[4] Printouts and displays of the audit trail shall be available in formats sorted by:

R[4.A] Period (from date/time and to date/time).

R[4.B] Data identifiers (table/re.cord, value name, substation, RTU, etc.)

R[4.C] User ID.

7.1.8 Data Archiving

R[1] For IS&R Data, the retention period of 2 years is the minimum length of time the data shall be kept on-line.

R[2] Data older than the retention period shall be transferred automatically to the archival system.

R[3] It shall also be possible to manually archive any data.

R[4] IS&R shall include a directory listing all information that has been stored on archive media.

R[5] It shall be possible to reload any IS&R archival media and access the archived data without disturbing the collection, storage, and retrieval of IS&R data in real-time and without requiring that any current on-line archives be removed from the system.

R[6] This RFP assumes that archived data will be reloaded into a “working area” in order to satisfy this requirement.

7.2 Specific Applications

R[1] The following specific applications of the general features of IS&R shall be supported by the ADMS-SCADA.

R[2] Capacity and performance requirements for these specific applications are presented in Section 3.

7.2.1 Alarm and Event Storage and Retrieval

R[1] The alarm and event storage and retrieval function shall consist of a chronological listing of all ADMS-SCADA alarm messages and event messages.

R[2] Each entry shall consist of the same information that is displayed on the alarm summary and event summary described in Section 4, User Interface.

R[3] Alarms and events shall be stored, but not modified, in both the Vendor's IS&R function and in the Historian.

R[4] Facilities to sort, selectively display (filter), and print the contents of the alarm and event storage shall be provided through the IS&R user interface.

R[5] User access to view and/or print alarm and event messages shall be controlled by the assigned AORs in the ADMS-SCADA for both the IS&R and Historian applications.

R[6] A user shall be able to select the entries to be displayed or printed based on the following sort and filter parameters and any multiple combinations of data elements stored.

7.2.2 Periodic Data Recording

R[1] It shall be possible to capture any value defined in the ADMS-SCADA database periodically in sets of associated data ("collection sets"). The collection sets to be captured initially, the capture periodicity, the retention period are presented in Section 3. The periodicity of storage shall be set independently for each collection set over a range from 2 seconds to daily with the following resolutions:

R[1.A] For periodicities less than once an hour – 1 second time resolution.

R[1.B] For periodicities of once an hour or greater – 1 minute time resolution.

R[2] Periodic data storage shall include a programming interface to initiate data collection.

7.2.3 Continuous Data Recording

R[1] The ADMS-SCADA shall maintain a continuous record of power system operations by recording all telemetered, manually entered, and calculated data including all associated quality codes and supervisory control safety tags.

R[2] Continuous data recording information shall be stored, but not modified.

R[3] Data shall be recorded in such a manner that it is possible to retrieve a complete picture of the power system from any date and time specified by the user (a “snapshot”), assuming that the data recording function was active at that time.

R[4] This snapshot shall include power system measurements, derived measurements, statuses, and derived statuses, and also the results of some application programs, as well as alarms.

R[5] The user shall be able to view (“play back”) continuously recorded data, on any display containing real-time data.

R[6] Data values, control safety tags, and quality codes being updated during replay. Summary displays are specifically excluded from replay.

R[7] The playback refresh rate, the periodicity at which the data is advanced to the next time increment, shall be selected by the user, from scan rate to on-demand, with an incremental resolution of 4 seconds.

R[8] Procedures for selecting and sorting recorded data by time, variable, and combinations of these criteria shall be provided for displays, video trends, and reports.

7.2.4 Sequence of Events Storage and Retrieval

R[1] The sequence of events storage and retrieval function shall consist of a chronological listing of all SOE messages (refer to Section 6.1.6).

R[2] Facilities to sort and search and selectively display and print the contents of the SOE storage shall be provided through the IS&R user interface.

R[3] A user shall be able to select the display of events based on the following sort or search parameters and combinations of these parameters:

R[3.A] Substation

R[3.B] Device Type

R[3.C] Device

R[3.D] Time Period

7.2.5 Communication Error Statistics and Availability Calculations

R[1] Hourly communication error statistics for RTUs (reference Section 6.1.5) and ICCP links (reference Section 6.2.1.5) shall be collected by IS&R and shall also be stored and maintained in the Historian.

R[2] The communication error statistics shall be grouped by communication channel for viewing on ADMS-SCADA displays.

R[3] In addition to the communication error statistics, the ADMS-SCADA shall calculate and store hourly availability statistics for each RTU and ICCP communications channel both in IS&R and in the Historians.

7.2.6 Application Generated Historical Data

R[1] It shall be possible to capture any data value calculated by any ADMS-SCADA Application defined in the specification for storage in IS&R and storage in the Historian.

R[2] The data capture shall be performed after execution of each application or periodically, depending on the mode selected by AE when the system and database are configured.

Table of Contents

8. Documentation 8-1
  8.1 Document Format 8-1
  8.2 Document Review and Approval 8-3
    8.2.1 Document Review 8-4
    8.2.2 Document Approval 8-4
    8.2.3 Scope of Reviews and Approvals 8-6
  8.3 Deliverable Documentation 8-7
  8.4 Documentation Standards 8-8
  8.5 Hardware Documentation 8-8
    8.5.1 List of Required Hardware 8-9
    8.5.2 Equipment Configuration Diagram 8-9
    8.5.3 Network Configuration Diagram 8-9
    8.5.4 Interconnection List 8-9
    8.5.5 Site Installation Drawings and Procedures 8-9
  8.6 Software Documentation 8-10
    8.6.1 List of Deliverable Software 8-10
    8.6.2 Software Development Standards 8-11
    8.6.3 Database Definition 8-11
    8.6.4 Interface Requirements Document 8-12
    8.6.5 Software Functional Description 8-12
    8.6.6 Installation Images and Source Code 8-13
    8.6.7 Software Requirements Matrix 8-13
    8.6.8 Design Document 8-13
  8.7 System Maintenance Manual 8-14
  8.8 Display Style Guide 8-16
  8.9 Operating Manual 8-16
    8.9.1 User Guides 8-17
    8.9.2 Operator's Manual 8-17
    8.9.3 Database Editor's Manual 8-18
    8.9.4 Display Editor's Manual 8-18
  8.10 Simulator Instructor User's Guide 8-19
  8.11 Cutover/Transition Plan – ADMS-SCADA 8-19

Table of Contents

8.12 Transition/Integration Plan 8-19

List of Exhibits:

Exhibit 8-1: Deliverable Documentation 8-7

8. Documentation

R[1] Documentation shall be provided for all equipment and functions provided by the Vendor as part of this procurement.

R[2] All documentation shall be properly written in clear Standard English.

R[3] All documentation shall be written or prepared by, or under the supervision, of qualified technical writers and tested for readability. An effort shall be made to organize information in a logical and functional manner.

R[4] The training material described in section 10, shall also be developed in accordance to the guidelines provided in this section.

R[5] The documentation mentioned in this section, shall also be referred to and explained during the training described in section 10.

R[6] A list of acronyms shall be provided. Furthermore acronym definitions shall be retrievable by pointing the pointing on top of them.

R[7] A comprehensive permutable index shall be available.

R[8] Ability for the individual users to place book marks and notes shall be provided.

R[7] A diagnostic and trouble shooting section shall be provided.

R[8] The remainder of this section addresses the requirements for documents other than project documents, which are described in Section 11.3, Project Documents.

8.1 Document Format

R[1] Documents shall be delivered in two phases:

R[1.A] Approval documents, submitted for AE's review and approval

R[1.B] Final documents, reflecting installation of the final "as-built" software and databases on the ECS (Prod 1 and Prod 2), QAS (Test), OTS, and PDS "(Development) platforms.

R[2] AE prefers that approval documents be delivered as softcopy on magnetic media or by electronic transfer (SharePoint, email or ftp, as examples).

R[3] Final documents shall be delivered on-line on the Program Development System (PDS), and in softcopy on CD-ROM.

R[4] Any user shall be able to access on-line documentation including functional design documents, user guides, maintenance manuals, on-line help, and operating procedures via a simple procedure from any ADMS-SCADA workstation.

R[5] Documents, excluding third party documentation, shall be supplied in a format that can be searched and edited by AE.

R[6] Drawings and diagrams may be supplied embedded in the document files or may be supplied as separate files.

R[7] Documents delivered on softcopy media shall be formatted for printing on 8½" x 11" paper, except tables, drawings and diagrams, which shall be sized appropriately.

R[8] Each document shall include a title or information page showing the document number, title, and revision record.

R[9] The document number shall be a unique number assigned in accordance with the Vendor's standard practice.

R[10] The title page shall include a space into which AE may enter a document number assigned from the AE document management system.

R[11] The revision record shall describe each new version of the document since its original production.

R[12] The revision record shall include:

R[12.A] The date of the change

R[12.B] A brief description of the change

R[12.C] An indication that the change has been reviewed and approved in accordance with the Vendor's quality assurance procedure

R[13] Each document shall include a table of contents.

R[14] If a document is divided into several physical volumes, each volume shall contain the complete table of contents of the whole document.

R[15] Where the phrase "on-line documentation" is used in this Specification, it shall be interpreted to mean the ability to view the appropriate documents by user needs from any ADMS-SCADA workstation.

R[16] The Vendor shall provide all software necessary to provide this capability.

R[17] For non-OEM documentation (i.e., documentation produced by the Vendor), the Vendor shall also provide the capability to edit and annotate the document.

R[18] Vendor shall deliver documentation in Vendor's standard format that is editable and in both secure and unsecured PDF format for the given documentation type.

8.2 Document Review and Approval

R[1] All standard and OEM documents provided pursuant to this contract shall be subject to review by AE, as defined in Section 8.2.1.

R[2] Custom documents provided pursuant to this contract shall be subject to approval by AE, as defined in Section 8.2.2.

R[3] All features and functions newly developed by Vendor for the ADMS-SCADA project whether custom for AE or as an addition to Vendor's baseline software shall be considered custom software and the documents describing the software shall require AE's approval.

R[4] Vendor and AE shall identify the list of custom features during the implementation phase of the project and include them in the Documentation Plan.

R[5] All ADMS-SCADA Test Plans and Procedures (refer to Sections 9.4, 9.4.1, and 9.4.2) shall be considered custom documents for the AE project and all Test Plans and Procedures shall be subject to review and approval by AE.

R[6] AE will review documents within fifteen-business days or a time period mutually agreed to in writing at the time of their submittal.

R[7] If a document review takes longer than 30 business days from initial submittal, the project managers shall escalate the issue to expedite the review process.

R[8] If AE transmits comments on any documents, the Vendor shall respond to the comments within ten business days of receipt of the comments.

8.2.1 Document Review

R[1] AE's review of documents shall be limited to determining that:

R[1.A] The documents have been produced in accordance with the documentation standards of the Vendor or Subcontractors

R[1.B] All hardware and software is in full conformance with the contract

R[1.C] For software, that the software has been produced in accordance with the coding and display standards of the Vendor or Subcontractors

R[1.D] The documents clearly and accurately describe the features and options of the hardware and software that pertain to the ADMS-SCADA

R[1.E] The documents are written in English, and hard copies are printed legibly, and well bound.

R[2] AE will review documents within fifteen-business days of their submittal or a time period mutually agreed to in writing at the time of their submittal.

R[3] If AE transmits comments on any documents, Vendor shall respond to the comments within ten business days of receipt of the comments.

R[4] If the comments address OEM documents, Vendor shall act as an advocate of AE to initiate and facilitate resolution of the comments with the Subcontractor.

8.2.2 Document Approval

R[1] All custom documents shall be subject to a formal approval process. The approval process shall proceed as follows:

R[1.A] The Vendor shall transmit documents subject to the approval process to AE.

R[1.B] AE will return comments to the Vendor within the agreed time.

R[1.B.i] This time may be adjusted by mutual agreement in writing to accommodate the other activities of AE and the Vendor.

R[1.B.ii] Requests by either party to change the time shall be made within five-business days of receipt of the documents.

R[1.B.iii] The transmittal cover for the comments shall clearly indicate that the document is either:

R[1.B.iii.a] *Approved* – If approved, the Vendor may proceed with the work covered by the document. No further approval action is required.

R[1.B.iii.b] *Approved with Comments* – If approved with comments, the Vendor may proceed with the work covered by the document and the comments.

R[1.B.iii.c] *Not Approved* – If not approved, the Vendor may proceed with the work covered by the document and the comments only at their risk. No schedule or cost relief will be granted for any work undertaken prior to approval of the appropriate documents.

R[1.C] If desired by any party, the comments may be discussed to clarify AE intent.

R[1.D] The Vendor shall then revise and resubmit the documents within five-business days after receipt of the comments from AE.

R[1.D.i] This time may be adjusted by mutual agreement to accommodate the other activities of AE and the Vendor. Requests by either party to change the time shall be made within two-business days of receipt of the comments by the Vendor.

R[1.D.ii] All changes made to documents to reflect approval comments shall be clearly highlighted and the revision record shall be updated to reflect the changes.

R[1.D.iii] An automated revision tracking mechanism shall be used when documents are updated during the review process to simplify the review and approval process.

R[1.D.iv] The final approved documents shall have all tracked changes accepted so that the documents are “clean” and formatted correctly.

R[1.E] After the document has been updated by Vendor, AE will review the document to ensure that the comments have been incorporated correctly.

R[1.E.i] Any additional comments added following the initial comment submittal will be evaluated for inclusion by the project managers.

R[1.E.ii] The acceptance of the document or results of the review will be completed within five (5) business days after Vendor submittal (unless a different time is mutually agreed by the project managers).

R[1.E.iii] This review and comment process shall be continued until the document is approved.

R[1.E.iv] After a document is approved Vendor shall deliver a final version of the document free of any change tracking marks.

8.2.3 Scope of Reviews and Approvals

R[1] The acceptance or approval of any documents by AE shall not relieve the Vendor of the responsibility to meet all of the requirements of the contract or of the responsibility for the correction of the documents.

R[2] All deliverable documentation shall be revised by the Vendor to reflect the delivered system.

R[3] Any modifications to the ADMS-SCADA resulting from the factory and site acceptance tests shall be incorporated in this documentation.

R[4] All previously submitted documents that have been changed because of engineering changes, contract changes, or errors or omissions shall be resubmitted for review or approval as appropriate.

8.3 Deliverable Documentation

R[1] Exhibit 8-1: Deliverable Documentation lists the minimum documentation to be delivered for each ADMS-SCADA platform, quantities to be delivered, and the desirable delivery dates for the first submission review or approval copies.

R[2] Electronic or soft copies plus hard copies shall be supplied as shown below.

Exhibit 8-1: Deliverable Documentation

Document	Quantity		Delivery Date
	Review and Approval	Final	
Documentation standards	1 soft copy	1 soft copy	Per the Project Schedule
Basic hardware documents			
• Configuration diagram	1 soft copy	1 soft copy	Per the Project Schedule
• Network configuration, interconnection lists	1 soft copy	1 soft copy	Per the Project Schedule
• Site installation drawings and procedures	1 soft copy	1 soft copy	Per the Project Schedule
Software list of deliverables ADMS-SCADA	1 soft copy	1 soft copy	Per the Project Schedule
Software development standards	1 soft copy	1 soft copy	Per the Project Schedule
Database definition	1 soft copy	1 soft copy	Per the Project Schedule
Interface Requirements Document	1 soft copy	1 soft copy	Per the Project Schedule
Software functional description	1 soft copy	1 soft copy	Per the Project Schedule
Installation images	1 soft copy	1 soft copy	Per the Project Schedule
Design document	1 soft copy	1 soft copy	Per the Project Schedule
Test Plans and Procedures	1 soft copy	1 soft copy	Per the Project Schedule
System maintenance manual	1 soft copy	1 soft copy	Per the Project Schedule
Configuration Guidelines	1 soft Copy	1 soft copy	Per the Project Schedule

Document	Quantity		Delivery Date
	Review and Approval	Final	
Operating Manual	1 soft copy	1 soft copy	Per the Project Schedule
User Documentation	1 soft copy	1 soft copy	Per the Project Schedule
Display style guide	1 soft copy	1 soft copy	Per the Project Schedule
Simulation instructor user's guide	1 soft copy	1 soft copy	Per the Project Schedule
Cutover/Transition Plan	1 soft copy	1 soft copy	Per the Project Schedule
Change Management Processes	1 soft copy	1 soft copy	Per the Project Schedule

R[3] AE recognizes that the documentation scheme used by the Vendor may not match that described in this and other sections.

R[4] Therefore, the Vendor is not expected to supply the specific documents presented herein.

R[5] However, the documentation supplied shall provide all of the information described in the following sections.

8.4 Documentation Standards

R[9] The Vendor shall provide a document defining the standards used to create and maintain all documentation supplied by the Vendor.

R[10] The documentation standards shall include a document template so that AE can create additional documents in the same form as the standard documents.

8.5 Hardware Documentation

R[1] The following documentation shall be provided for all hardware provided pursuant to this contract:

R[1.A] List of required hardware

R[1.B] Equipment configuration diagram

R[1.C] Network configuration diagram

R[1.D] Interconnection list

R[1.E] Site installation drawings and procedures.

R[2] The other hardware documentation to be supplied shall be commensurate with the hardware maintenance philosophy to be employed by AE.

8.5.1 List of Required Hardware

R[1] The list shall itemize each hardware item and include equipment configuration information.

8.5.2 Equipment Configuration Diagram

R[1] The equipment configuration diagram shall depict the logical interconnection of all of the Vendor-supplied equipment and its connection to AE-supplied equipment.

8.5.3 Network Configuration Diagram

R[1] This document shall show the design of the local and wide area networks supplied by the Vendor as well as the communications network supplied by AE.

8.5.4 Interconnection List

R[1] The physical interconnections among the ADMS-SCADA components, other than those shown on the network configuration diagram, shall be depicted.

R[2] Each cable shall be identified, along with its terminations.

8.5.5 Site Installation Drawings and Procedures

R[1] The site drawings shall depict the physical arrangement of the ADMS-SCADA components.

R[2] These drawings shall show the separation of the equipment between the different control rooms and computer rooms at each AE location.

8.6 Software Documentation

R[1] The following documents shall be provided for all software:

R[1.A] List of Deliverable Software

R[1.B] Software Development Standards.

R[2] The Vendor or Subcontractors shall provide the following documents for all software that has been produced for the ADMS-SCADA.

R[3] This specifically includes the support software of Section 2, ADMS-SCADA Architecture, as well as all application software:

R[3.A] Database definition and data flow, along with an explanation of stored procedures

R[3.B] Interface Requirements Document

R[3.C] Software functional description

R[3.D] Installation images and source code, per the Terms and Conditions

R[3.E] Source code version control and revision control documentation.

R[4] The following documents shall be produced for all software produced specifically for this contract:

R[4.A] Software Requirements Matrix

R[4.B] Detailed design documents.

8.6.1 List of Deliverable Software

R[1] The list shall itemize each software item and include version and license information.

8.6.2 Software Development Standards

R[1] The Vendor shall document the development standards used to develop the ADMS-SCADA software.

R[2] AE reserves the right to reject software that does not conform to the development standards.

8.6.3 Database Definition

R[1] The database definition shall identify the characteristics of all ADMS-SCADA databases including the complete database schema, security provisions, and data definitions.

R[2] Database documentation shall include the following:

- R[2.A] Database Name(s)
- R[2.B] Version(s)
- R[2.C] Patches
- R[2.D] A description of the intended use of each database
- R[2.E] Database Schema, including
  - R[2.E.i] table names
  - R[2.E.ii] table extents
  - R[2.E.iii] description of the purpose of each table
  - R[2.E.iv] constraints
  - R[2.E.v] keys
  - R[2.E.vi] authorization levels
- R[2.F] Any application user ids and authorization

R[3] Documentation should be provided for database maintenance, including

R[3.A] Backup and restoration procedures and schedule

R[3.B] User Addition / Deletion procedures

R[3.C] Database extension procedures

8.6.4 Interface Requirements Document

R[1] The Interface Requirements Document shall describe in detail the interfaces between the ADMS-SCADA and AE-provided systems and networks.

R[2] The interface documentation shall include the following information for each interface:

R[2.A] Timing of anticipated exchange and/or download of data (frequency) and processes, if any, for initiating manual transfers

R[2.B] Anticipated volume of data exchange

R[2.C] Security implementation

R[2.D] Error processing, queuing, and timeout information

R[2.E] Definition of alarms or other logged events on interface failure

R[2.F] Description of failover process to use alternate interfaces

R[3] The Interface Requirements Document will be used by both the Vendor and AE as the definition of the interface between the ADMS-SCADA and all other systems, so that each system can be designed or modified to meet its requirements.

R[4] AE will provide all required information for the Vendor to prepare the document accordingly as required by the mutually agreed project schedule.

8.6.5 Software Functional Description

R[1] The intent of the software functional description shall be to describe the functions to be performed by each software module from the standpoint of a user.

R[2] The functional operation of the ADMS-SCADA shall be clearly described so that it can be understood without understanding the detailed operation of each software module.

R[3] The functional description shall also describe how the function will interact with the EMS/SCADA.

R[4] Software functional descriptions shall also be used as the first step in the design of custom software (for example, new functionality).

R[5] Thus it shall have sufficient information for AE to determine that the new functionality will meet the requirements of the contract.

8.6.6 Installation Images and Source Code

R[1] Please refer to section 0300 Standard Terms and Conditions

8.6.7 Software Requirements Matrix

R[1] The Vendor shall provide a list of all software requirements, cross-referenced to show where each requirement is discussed in the relevant software document.

R[2] The Software Requirements Matrix shall list each of the requirements for the ADMS-SCADA stated in this specification, in numerical order, referenced by chapter, section, and paragraph number.

R[3] This list of specified requirements shall be supplemented by a list of all functions provided by the Vendor's software system that go beyond the specified requirements.

8.6.8 Design Document

R[1] The design documents are intended as a second level of detail to the software functional descriptions. In general, a design document shall relate to a single software functional description.

R[2] It is expected that, for customized software, the Vendor will first deliver a software functional description for approval by AE. After approval, the Vendor will then produce a design document for review and comment.

R[3] The software design documentation shall include, but shall not be limited to, the design information for implementation of the software.

R[4] It shall show the divisions of the software design entities; a dependency description specifying the dependent entities, their coupling, and required resources, an interface description providing details of external and internal interfaces not provided in the software functional description; and a detailed design description containing the internal details of each design entity.

R[5] The software design documentation shall provide a description of how the software will support the functions described in the software functional description.

R[6] Software design documentation shall include a diagram of the software indicating major modules and an overview of the operation of each module.

R[7] It shall describe data structures and flow, and a diagram or description of the manner in which the modules interfaces with other modules.

R[8] Design document is provided for review.

R[9] Vendor does not differentiate between design documents and detailed design documents.

R[10] The Vendor-supplied design document will conform to Vendor's standard format.

R[11] Each program module, including subroutines, shall be sufficiently documented to allow an experienced programmer (with supervision of the designer) to perform the coding of the module, as well as allow AE personnel to maintain such software in the future.

R[12] All job control files (batch or make files) required for compilation, assembly, and linking of each program shall be documented in detail as part of the software design documentation.

8.7 System Maintenance Manual

R[1] The System Maintenance Manual shall describe all user procedures necessary to install and maintain the software system, from the delivered object code, of the ADMS-SCADA.

R[2] It shall include complete instructions on performing a system generation from sources for all processors. It shall provide information on optimizing system performance.

R[3] It shall describe the hierarchy of disk directories used by the ADMS-SCADA software system, and the location of all categories of files: including executable programs, displays, databases, sources, build files, etc.

R[4] It shall also describe the procedures to configure the ADMS-SCADA computer system.

R[5] The System Maintenance Manual shall also include documentation of the distributed system software supporting the configuration control function, data integrity, startup, restart, and the network management subsystem including all third-party software (e.g., OS, etc.) used and the appropriate version identifications, patch levels, and configuration files.

R[6] This document shall include Configuration Guides for each function that describes the configuration, setup, and all adjustable parameters for each function.

R[7] The manual shall provide a location for AE to enter the list of the Internet Protocol (IP) addresses of all devices in a manner compatible with AE security standards and shall describe the procedures for upgrading or adding additional workstations, loggers, storage devices, and other peripheral devices.

R[8] The System Maintenance Manual shall provide detailed information on troubleshooting all processors of the ADMS-SCADA.

R[9] It shall describe the use of error logs, the meaning of all program-generated error or informational messages, and the recommended response to these messages.

R[10] It shall explain what the user should do to save information after a processor failure, and shall describe the procedures to gather this information to allow the user to communicate in an informed manner with maintenance personnel.

R[11] It shall include a description of the procedures to restore normal operation after a failure of the ADMS-SCADA.

R[12] The maintenance manual shall detail the procedures to backup the ADMS-SCADA software, configuration data, and real-time/historical operating data, and shall present a schedule for periodic backup.

R[13] Directions to restore software, configuration data, and operating data for each server and workstation shall also be provided.

8.8 Display Style Guide

R[1] The Vendor shall furnish a Display Style Guide that describes the discretionary aspects of display design and implementation for the ADMS-SCADA.

R[2] This guide shall be used by the Vendor to develop all displays supplied with the system.

R[3] AE will also use this guide as input to the development of its display conventions and standards.

R[4] The objective of the display conventions and standards shall be to promote a consistent look and feel across all ADMS-SCADA displays.

8.9 Operating Manual

R[1] The Vendor shall submit, for review and approval operating manuals for all ADMS-SCADA functions as defined in Section 8.2.

R[2] The operating instructions associated with all features shall be incorporated into these manuals.

R[3] These manuals shall be incorporated into the on-line user HELP function and context sensitivity shall be used to go directly to the appropriate place in the manual.

R[4] The manuals shall be organized for quick access to each detailed description of the user procedures that are used to interact with the ADMS-SCADA functions.

R[5] The manuals shall present in a clear and concise manner all information that a user needs to know to understand and operate the ADMS-SCADA satisfactorily.

R[6] The manuals shall make abundant use of screen snapshots to illustrate the various procedures.

8.9.1 User Guides

R[1] The ADMS-SCADA shall include User Guides for each function in the system.

R[2] These guides shall describe all of the features and capabilities of the ADMS-SCADA function covered and describe how the User operates the function.

R[3] The User Guides shall be written to the appropriate level so that the user can understand and operate all features of the ADMS-SCADA function.

R[4] The User Guide shall describe the ADMS-SCADA in a manner and at a level of detail that allows the user to detect and isolate problems in the ADMS-SCADA.

R[5] All program-generated messages (such as, alarms, prompt messages, and error messages) shall be listed along with easily understood meanings and recommended remedial actions, where appropriate.

R[6] The User Guide shall be provided on-line.

R[7] The system operator shall be capable of accessing the User Guide from the operator workstation via the on-line Help function.

8.9.2 Operator's Manual

R[1] The Operator's Manual shall document all AE ADMS-SCADA functionality.

R[2] Vendor will deliver the Users Guides in an editable format (Microsoft Word) so that AE may edit and customize these documents to meet their needs.

R[3] The Operator's Manual shall be created for system operators, by AE from the User Guide, as the audience.

R[4] It shall be organized in a logical sequence and shall fully describe the user interface of all operational functions of the ADMS-SCADA.

R[5] Each step of a multi-step procedure shall be described, with a clear indication of which menu items are selected to proceed to the next step.

8.9.3 Database Editor's Manual

R[1] The ADMS-SCADA data shall be held in an Oracle database.

R[2] Oracle tools shall be used to create new database users, if required.

R[3] The ADMS-SCADA shall include utilities to define an empty Oracle database structure.

R[4] These utilities shall also have the ability to modify the Oracle database structure as needed to support upgrades or bug fixes to the ADMS-SCADA software.

R[5] AE shall use standard Oracle tools to backup and restore the Oracle database, such as recovery manager (RMAN).

R[6] The ADMS-SCADA shall include a Data Dictionary document that lists each Oracle database table and a description of the table.

R[7] The Data Dictionary document shall also list each table column, its data type and a text description of that column.

8.9.4 Display Editor's Manual

R[1] The Display Editor's Manual shall describe and fully illustrate the capabilities of the Display Editor.

R[2] Procedures to auto-generate and edit single-line displays for the ADMS-SCADA and to link display fields with entities in the database of the ADMS-SCADA shall be included if this feature is include with the Display Editor.

R[3] It shall describe how to generate new device symbols and all ADMS-SCADA constraints in expanding the number of symbols, if any.

R[4] It shall present a clear description of the principles behind zooming and decluttering, and shall explain how the user can assign declutter levels to display elements in order to achieve a satisfactory decluttering upon zooming.

8.10 Simulator Instructor User's Guide

R[1] This document shall describe the instructor-oriented capabilities of the Simulator and how to use them.

8.11 Cutover/Transition Plan – ADMS-SCADA

R[1] This document shall describe the process to be used to commission the new ADMS-SCADA and cutover operations to the new ADMS-SCADA.

R[2] The cutover/transition plan shall be jointly developed by the Vendor and AE.

R[3] The Vendor shall provide its standard and recommended cutover procedures, adapted to reflect the AE configuration, ADMS-SCADA functions implemented, communications infrastructure, and operating environments.

R[4] AE shall review, comment, and provide additional information regarding its specific procedures and policies and additional cutover/transition details where required.

8.12 Transition/Integration Plan

R[1] This document shall describe the process to be used to integrate the EMS and the ADMS-SCADA.

R[2] The cutover/transition plan shall be jointly developed by the Vendor and AE.

R[3] The Vendor shall provide its standard and recommended cutover procedures, adapted to reflect the AE configuration, ADMS-SCADA functions implemented, communications infrastructure, and operating environments.

R[4] AE will review, comment, and provide additional information regarding its specific procedures and policies and additional cutover/transition details where required.

Table of Contents

9. Quality Assurance and Testing 9-1
9.1 Quality Assurance Program 9-1
9.2 Inspection 9-1
9.3 Test Responsibilities 9-1
9.4 Test Documents 9-2
9.4.1 Test Plans 9-2
9.4.2 Test Procedures 9-2
9.4.3 Test Records 9-3
9.5 Variance Recording and Resolution 9-3
9.5.1 Variance Records 9-4
9.5.2 Schedule for Variance Correction 9-5
9.5.3 Variance Resolution 9-6
9.6 Test Schedule 9-6
9.6.1 Test Initiation 9-6
9.6.2 Test Completion 9-7
9.6.3 Test Suspension 9-7
9.7 Modifications to the ADMS-SCADA During Testing 9-7
9.8 Preliminary Factory Testing 9-8
9.9 Factory Test 9-8
9.9.1 Equipment Test 9-8
9.9.2 Functional Test 9-9
9.9.3 Performance Test 9-10
9.9.4 Stability Test 9-11
9.9.5 Unstructured Test 9-12
9.9.6 Cyber Security Audit 9-13
9.10 Site Test 9-13
9.10.1 Installation Test 9-13
9.10.2 Functional and Performance Tests 9-13
9.10.3 Site Cyber Security Audit 9-14
9.11 Integration Testing 9-14
9.11.1 Factory Acceptance Testing 9-14
9.11.2 Site Acceptance Testing 9-14

Table of Contents

9.12 Availability Test....9-15
9.12.1 Test Activity....9-15
9.12.2 Test Definitions....9-15
9.12.3 Duration and Criteria for Passing....9-16
9.13 Acceptance Criteria....9-16

9. Quality Assurance and Testing

R[1] To ensure that the Vendor produces a well-engineered and contractually compliant ADMS-SCADA, a quality assurance program shall be followed, and both structured and unstructured tests shall be performed.

9.1 Quality Assurance Program

R[1] The Vendor shall employ documented Quality Assurance (QA) techniques and practices throughout this project.

9.2 Inspection

R[1] AE shall be allowed access to the Vendor's facilities during system design, development, and testing and to any facility where software is being produced.

R[2] The Vendor shall provide office facilities, equipment, and documentation necessary to complete all inspections and to verify that the ADMS-SCADA is being developed in accordance with this Contract.

9.3 Test Responsibilities

R[1] Prior to the start of the factory test, AE and the Vendor shall each designate a test coordinator, in writing.

R[2] Each test coordinator shall be responsible for ensuring that the tests are conducted in accordance with the requirements of the Contract.

R[3] Unless otherwise stated in this Specification, the Vendor shall be responsible for all factory tests.

R[4] This responsibility shall include the conduct of the tests and all record keeping and document production.

R[5] AE will support the factory testing by supplying staff to execute the test procedures under the Vendor's supervision.

R[6] Also, unless otherwise stated in this Specification, AE shall be responsible for all site tests.

R[7] This responsibility shall include the conduct of the tests and all record keeping and document production.

R[8] The Vendor shall support the site testing by supplying adequate staff to monitor the tests.

R[9] AE expects that at least one qualified Vendor representative will be on-site during these tests.

R[10] The Vendor shall provide remote support during availability testing.

9.4 Test Documents

R[1] Test plans, procedures, and records shall be provided by the Vendor for all tests (excluding inspections and software demonstrations pursuant to Section 9.2, Inspection) to ensure that each test is comprehensive and verifies the proper performance of the ADMS-SCADA elements under test including those functions integrated with the EMS.

R[2] All test plans and test procedures (standard, modified standard, and custom functions) shall be submitted to AE for approval and shall be subject to the approval process as defined in Section 8.2, Document Review and Approval.

9.4.1 Test Plans

R[1] The test plans shall describe the overall test process, including the responsibilities of individuals and the documentation of the test results.

R[2] Separate test plans shall be provided for the Factory Acceptance Test, Site Acceptance Test, and Availability Test.

9.4.2 Test Procedures

R[1] The test procedures shall describe the methods and processes to be followed in testing the ADMS-SCADA.

R[2] The test procedures shall be modularized, such that individual functions of the ADMS-SCADA can be independently tested and so that the testing proceeds in a logical manner.

R[3] This section uses the term segment to refer to a higher-level part of a test procedure and the term step to refer to the most detailed level of test instruction.

R[4] The Vendor shall note that AE will not accept any certified test data in lieu of testing except where specifically stated in the Contract.

9.4.3 Test Records

R[1] Complete records of all test results shall be maintained.

R[2] The records shall be keyed to the test procedures.

9.5 Variance Recording and Resolution

R[1] The Vendor shall establish a process to record and track variances for each ADMS-SCADA.

R[2] This process shall be initiated at a time to be determined by the Vendor but no later than the start of pre-FAT, and shall continue through the completion of the Warranty period.

R[3] Both the Vendor and AE may initiate variances at any time.

R[4] The variance process system shall produce reports of all variance information and shall produce reports of subsets of the variances based on searches of the variance parameters singly and in combination.

R[5] Variance reports shall be available to AE at all times.

R[6] The Vendor shall periodically distribute a variance summary that lists for each variance the report number, a brief overview of the variance, its category, and its severity, with the severity being determined by agreement between the AE Project Manager and the Vendor Project Manager.

R[7] The Vendor's variance recording process shall contain controls to limit access to any variances related to cyber security features and vulnerabilities.

R[8] Reporting and resolving variances for other Vendor clients shall be tightly controlled and shall not indicate in any way that the vulnerability was detected or related to AE.

R[9] The Vendor shall also provide variance reports that Vendor or other clients have detected against any elements of the Vendor's baseline system version (and higher) that is being used for the AE project.

R[10] All version release notes, plus the variance resolutions and reports related to the release, shall also be provided for AE's use.

R[11] This process shall become effective at the start of FAT.

9.5.1 Variance Records

R[1] The record of each variance shall include the following information:

R[1.A] The time and date of the initial discovery of the variance.

R[1.B] A variance number.

R[1.C] An identification of the person submitting the variance. Other witness names can be placed in a free-format comments field.

R[1.D] An identification of the ADMS-SCADA component, such as a hardware item or software function, against which the variance is being written.

R[1.E] An identification of the test plan and stage or step of the plan or procedure shall be identified. If problem is not part of a structured test, any applicable Contract document or operators manual (if applicable) reference shall be provided.

R[1.F] A detailed description of the variance including conditions and observed behavior.

R[1.G] A variance state (at a minimum):

R[1.G.i] Submitted

R[1.G.ii] Open

R[1.G.iii] Released

R[1.G.iv] Closed

R[1.G.v] Resolved

R[1.H] The date of assignment into each category.

R[1.H.i] A variance severity:

R[1.H.ii] *Critical* –Applies to variances that affect the whole system operation or a non-operational critical function.

R[1.H.iii] *Major* – Denotes the failure of the system to successfully perform a required function which delays further testing of the ADMS-SCADA.

R[1.H.iv] *Medium* – Denotes the failure of the ADMS-SCADA to perform one or more required features of a function or failure to produce accurate results.

R[1.H.v] *Low* – Denotes the failure of the ADMS-SCADA to perform a required feature in a manner that reduces the utility of the ADMS-SCADA only slightly. This variance usually is more of an inconvenience or annoyance or with a readily available workaround.

R[1.I] Estimated time to fix the variance

R[1.J] A description of the resolution.

R[1.K] A record of all testing performed.

R[1.L] Identification of AE PM accepting the resolution and the date of acceptance.

9.5.2 Schedule for Variance Correction

R[1] The Vendor and AE shall meet as necessary to review the variance list.

R[2] Each new variance opened since the previous meeting shall be scheduled for correction at the meeting.

9.5.3 Variance Resolution

R[1] A variance shall be deemed resolved only upon written acceptance of the correction by AE.

R[2] A variance shall be deemed accepted only after AE has tested the corrected variance to its satisfaction.

R[3] The Vendor shall support any and all testing deemed necessary by AE to verify the corrections.

R[4] The Vendor shall be responsible for installing all variance resolutions, as appropriate, in all instances of the ADMS-SCADA.

9.6 Test Schedule

R[1] The sequence of tests to be performed and their scheduling with respect to other activities are presented in Section 11.4, ADMS-SCADA Testing, Shipment and Commissioning.

9.6.1 Test Initiation

R[1] The following conditions must be satisfied before starting any test (exclusive of inspections or demonstrations pursuant to Section 9.2):

R[1.A] AE has:

R[1.A.i] approved all plans and procedures for the test.

R[1.A.ii] reviewed or approved all relevant documentation.

R[1.B] A copy of each relevant document, including as a minimum, Functional Documents, User Guides, Operator Documents, Test Plans and Procedures, and Design Documents has been placed on the test floor.

R[1.C] The software under test has undergone a complete regeneration to ensure no unexpected “post-generation” modifications have been made which might alter the validity of the test.

R[1.D] For the factory test, preliminary testing, as described in Section 11.8, Preliminary Factory Testing has been completed.

R[1.E] For the availability test, all variances have been corrected and verified to the satisfaction of AE.

R[1.E.i] The AE project manager shall have the authority to waive the requirement for resolution of any specific variances

9.6.2 Test Completion

R[1] A test shall be deemed to be successfully completed only when:

R[1.A] All critical and major variances have been resolved to the satisfaction of AE.

R[1.A.i] All medium variances have been resolved to the satisfaction of AE, unless mutually agreed upon by Vendor and AE.

R[1.A.ii] All remaining (deferred medium and low) variances shall have a plan for resolution and completion.

R[1.B] All test records have been transmitted to AE.

R[1.C] AE acknowledges, in writing, successful completion of the test.

9.6.3 Test Suspension

R[1] If AE believes, at any time, that the quantity or severity of variances warrants suspension of any or all testing, the test shall be halted, remedial work shall be performed, and the test shall be repeated.

9.7 Modifications to the ADMS-SCADA During Testing

R[1] No changes shall be made to the ADMS-SCADA after factory testing has started without the express written authorization of AE Project Manager or designee.

R[2] The Vendor shall make fix releases available during the testing as variances are discovered and resolved.

R[3] However, these fixes will not be rolled into the system during the testing without AE's written authorization.

R[4] Fixes shall be rolled into the system at the end of factory testing.

9.8 Preliminary Factory Testing

R[1] The pre-FAT shall be a complete dry run of the FAT, following the test plans and procedures.

R[2] The Vendor's project manager or designee shall sign off each test.

R[3] The completed test results shall be sent to AE for inspection before AE personnel travel to the Vendor's facilities for the FAT.

R[4] All tests shall be conducted using AE-specific databases unless AE authorizes the Vendor to use a test database.

R[5] The Vendor shall notify AE at least thirty calendar days prior to the start of the pre-FAT, and AE shall have the option to witness all or parts of it.

R[6] The Vendor shall notify AE when the pre-FAT has been successfully completed and the ADMS-SCADA is ready for FAT.

9.9 Factory Test

R[1] In parallel with the Factory Test, the Vendor shall place workstations at AE's facilities for AE Operators to review and test the system from AE's facilities while Factory Testing is being performed at the Vendor's facilities.

9.9.1 Equipment Test

R[1] The equipment test shall verify that the ADMS-SCADA includes all required equipment, that the equipment is properly configured, and that the equipment can successfully execute the diagnostic programs provided.

9.9.2 Functional Test

R[1] The functional test shall use an equipment configuration that may include an extension of the Vendor's deliverables as required to prove the correct functionality of the ADMS-SCADA.

R[2] The test procedures shall take into account all additional test equipment and shall ensure that the additional equipment does not create false test results.

R[3] The functional tests shall rigorously exercise all functions and devices, both individually and collectively, and shall verify the correct functional operation of all hardware and software.

R[4] These tests shall include the following, as may be applicable to the system under test:

R[4.A] Verification of all required functionality of the system.

R[4.B] Verification that all software has been correctly sized and meets AE capacity requirements.

R[4.C] Verification of proper acquisition, processing, and storage of data from appropriate sources, and verification of protocol and data exchanges with all external systems that will interface with the ADMS-SCADA.

R[4.D] Verification of all user interface functions and consistency of the user interface operations across all ADMS-SCADA applications.

R[4.E] Verification of the proper operation of local and wide area network devices.

R[4.F] Verification of the application program and system development capabilities.

R[4.G] Verification of communications maintenance capabilities.

R[4.H] Verification of the redundancy and failure recovery schemes of the ADMS-SCADA.

R[4.I] Verification of the proper response of the system to abnormal situations.

R[4.J] Demonstration of the security of the system from unauthorized access.

R[4.K] Verification that the system meets all NERC cyber security requirements.

R[4.L] Verification that changes of system time will not prevent the system from operating properly.

R[4.M] Documentation verification that will verify that all documentation to be delivered with the system is present and meets requirements.

R[4.N] Verification of the ADMS-SCADA Recovery Plan to confirm that backup and recovery procedures and tools function correctly.

R[4.O] Vendor and AE personnel will build and install the ADMS-SCADA software and databases from source code at the factory to verify the escrow build process.

9.9.3 Performance Test

R[1] The performance test shall verify that the performance requirements specified in Section 3, Capacity and Performance, are met.

R[2] Execution of the performance tests shall have all AE-approved anti-virus software and patches turned on and shall be automated as much as possible so that test runs can be reproduced.

R[3] All tools and simulations (including source code for these tools, scripts, etc.) used for the performance test shall be delivered to AE to allow the tests to be repeated in the field.

R[4] Data collection and change simulation shall be performed.

R[5] The performance test shall include simulation of the EMS interfaces and functions to verify the overall system capacity and performance requirements are satisfied.

R[6] The Vendor shall demonstrate, during the integrated performance test (refer to Section 3), that the ADMS-SCADA the following:

R[6.A] Computer redundancy check. Failing over of the ADMS-SCADA shall result in no impact on Computer functions during testing and successful switching/testing shall occur without equipment failure.

R[6.B] Computer Systems performance. Verify computer-processing capacity during blackout-like simulation or multiple status changes and heavy alarm activities such as in a major system disturbance or blackout.

R[6.B.i] A burst test shall be performed to simulate a major system disturbance by executing the following test scenario:

R[6.B.i.a] Toggle all telemetered status points (RTUs and ICCP) open in the first 10 seconds and have the points reclose in the subsequent 5-second period. Repeat the abnormal to normal state toggling every 30 seconds for a total of 10 state transitions.

R[6.B.i.b] Toggle all analogs (RTUs and ICCP) out of limits in the first 10 seconds and return back to normal within the next scan. Repeat the abnormal to normal state toggling every 6 seconds for a duration of 5 minutes.

R[6.B.ii] After the burst subsides, the ADMS-SCADA shall be fully operational.

R[6.B.iii] Also, verify the ADMS-SCADA correctly processed all state changes, the resultant alarms, the data transfers to IS&R and that ICCP transfers are working correctly.

R[6.B.iv] The ADMS-SCADA processor loading requirements can be exceeded during the above burst test scenario.

R[6.B.v] However, there shall be no loss of data and no degradation of operator interactions with the User Interface.

9.9.4 Stability Test

R[1] A 100-hour continuous run of the system shall be performed after successful completion of the functional and performance tests.

R[2] The stability test will be considered successful if no critical function is lost, no major hardware failure occurs, no unforced failover occurs, and no restarts occur within the test period.

R[3] Any operator initiated failover shall not cause a failure of the test.

R[3.A] During this test, the ADMS-SCADA shall be exercised (with simulated inputs, events, and conditions) in a manner that approximates an operational environment. AE will simulate unstructured user activity during this test.

R[3.B] The Vendor shall assist AE in this test as required by AE.

9.9.5 Unstructured Test

R[1] The test schedule shall allow time throughout the functional testing for unstructured testing by AE.

R[2] Time for unstructured testing shall be reserved at the rate of at least two hours of unstructured testing for each eight hours of structured testing during the structured test period.

R[3] In addition, no less than four days and no more than 10 days total shall be spent on unstructured testing after the completion of the structured test period.

R[4] The Vendor shall assist AE in this test as required by AE.

R[5] For any substantial unstructured test, AE shall provide the Vendor with unstructured test outlines for documentation and future retest.

R[6] The Vendor will assist AE to help define specific steps or processes to complete the unstructured tests.

R[7] The functions tested during the unstructured testing will be coordinated with the Vendor so as not to interfere with other testing and problem correction activities by the Vendor.

R[8] AE shall, during the unstructured portion of the Factory Test, compare the results obtained from the new DMS's power flow with the results from their existing system's power flow and investigate all results outside of 1% of the existing solutions.

R[9] The Vendor shall assist AE in assessing any differences in results detected and shall resolve any problems identified with the new DMS's functions.

9.9.6 Cyber Security Audit

R[1] The FAT shall include a Cyber Security Audit to ensure that the ADMS-SCADA meets the NERC CIP and other cyber security requirements in this specification. Please refer to Section 12.23, Cyber Security Audit, for the details of this test.

9.10 Site Test

R[1] The site test includes the installation test, the functional test, and the performance test that will be conducted at AE sites after shipment and installation of the each ADMS-SCADA.

9.10.1 Installation Test

R[1] The installation tests shall be conducted by the Vendor and shall, at a minimum, include:

R[1.A] A repetition of the equipment test of Section 9.9.1, Equipment Test.

R[1.B] Install the ADMS-SCADA software and starting the system.

R[1.C] In cooperation with AE, attachment of the ADMS-SCADA to communications facilities for all data sources and other systems that interface with the ADMS-SCADA, as appropriate prior to on-line operation.

R[1.D] Initialization and preliminary tuning of application software as needed.

9.10.2 Functional and Performance Tests

R[1] The site functional and performance tests shall comprise a subset of the functional and performance tests of Sections 9.9.2 Functional Test, and 9.9.3, Performance Test.

R[2] The tests to be performed shall be proposed by the Vendor and approved by AE.

R[3] These tests shall be extended as necessary to test functions simulated during the FAT, such as communications with all field devices and all other systems that interface with the ADMS-SCADA.

R[4] The extended tests shall be performed to a test procedure prepared by the Vendor and approved by AE.

R[5] Unstructured tests shall also be employed, as necessary, to verify overall operation of the ADMS-SCADA under actual field conditions.

9.10.3 Site Cyber Security Audit

R[1] The SAT shall include a Site Cyber Security Audit to ensure that the ADMS-SCADA meets the NERC CIP and other cyber security requirements in this Specification.

R[2] Please refer to Section 12.24, Site Cyber Security Audit, for the details of this test.

9.11 Integration Testing

9.11.1 Factory Acceptance Testing

R[1] The Integration Test shall consist of both functional and performance tests on the completely integrated ADMS-SCADA system in the factory as part of the FAT.

R[2] The tests shall consist of all DMS and OMS functions fully operational and may use the QAS system to perform the necessary performance testing per Section 3, Capacity and Performance.

9.11.2 Site Acceptance Testing

R[1] The site integrated test shall have interfaces to all external systems and data sources shall be fully operational or simulated at the required data transfer rates.

R[2] This test shall be performed after all systems have been delivered and have successfully completed their individual site acceptance testing.

R[3] As necessary, the QAS system may be used for testing that might interfere with systems that are already operating as an on-line Production System.

R[4] The tests shall consist of all DMS and OMS functions fully operational and may use the QAS systems to perform the necessary performance testing per Section 3, Capacity and Performance.

9.12 Availability Test

R[1] ADMS-SCADA and device availability in accordance with the criteria specified in Section 2.4, System Availability shall be demonstrated by the availability test.

9.12.1 Test Activity

R[1] The test activity shall consist of normal ADMS-SCADA operations with the system in commercial use.

9.12.2 Test Definitions

R[1] The definitions of the time periods used in determining the duration of the test and the success of the test shall be as follows:

R[1.A] **Downtime** – Downtime occurs whenever the criteria for successful operation defined in Volume II, Section 2.4, Availability Requirements – Core ADMS-SCADA, are not satisfied.

R[1.B] **Hold time** – Certain periods of time during which the ADMS-SCADA is down may be due to circumstances that are beyond the control of either party. Specific instances of hold time are:

R[1.B.i] Scheduled shutdown

R[1.B.ii] Power interruption and environmental excursion

R[1.B.iii] Intermittent failure

R[1.B.iv] Failure of AE software

R[1.B.v] Corrected design defect

R[1.B.vi] Logistics delays

R[1.B.vii] Service response time

R[1.C] **Total time** – The time elapsed from the start of the availability test until the end of the availability test

R[1.D] Test time – The time elapsed from the start of the availability test until the end of the availability test, excluding hold time. That is,

$$Test\_time = Total\_time - Hold\_time$$

9.12.3 Duration and Criteria for Passing

R[1] The minimum duration of the availability test shall be 2200 consecutive hours of test time.

R[2] After 2200 consecutive hours of test time have elapsed and contingent on the conditions of the above paragraph, system availability shall be computed using the following formula:

$$System\_Availability = \frac{Test\_time - Down\_time}{Test\_time} * 100\%$$

R[3] When it has been determined that the system availability requirement has been met, the availability of each system device shall be calculated and compared against the device availability requirements of Section 2.4, Availability Requirements – Core ADMS-SCADA.

9.13 Acceptance Criteria

R[1] Final acceptance of the ADMS-SCADA systems shall occur only after:

R[1.A] Successful completion by Vendor of all payment milestones, including the Availability Tests

R[1.B] The ADMS-SCADA satisfies all functional and performance requirements of the SOW document, including integrated testing with the EMS

R[1.C] All system variances are addressed to the satisfaction of AE

R[1.D] AE's receipt of all final documentation reflecting all changes and corrections, including those resulting from Site Acceptance Testing and Availability Testing

R[1.E] Successful completion of the Site Cyber Security Audits

R[1.F] Successful completion of the Integration Tests

R[2] Vendor shall request final acceptance in writing stipulating:

R[2.A] The Work is complete for all ADMS-SCADA systems

R[2.B] Final acceptance and payment does not constitute a waiver by AE of any rights with respect to Vendor's continuing obligations under the contractual Agreement.

Table of Contents

10. Training 10-1
10.1 Scope of Training 10-1
10.1.1 Training Location 10-1
10.1.2 Self-Study Courses 10-1
10.1.3 Recording of Courses 10-1
10.2 Training Documents 10-2
10.2.1 Training Plan 10-2
10.2.2 Course Descriptions 10-3
10.2.3 Course Material 10-3
10.3 Training Requirements and Instructor Qualifications 10-3
10.3.1 System Overview 10-3
10.3.2 Database and Display Building 10-4
10.3.3 Data Engineering Workshops 10-4
10.3.4 Information Management 10-4
10.3.5 Operating System Administration 10-5
10.3.6 System Programming Languages 10-5
10.3.7 Programming in the ADMS-SCADA Environment 10-5
10.3.8 Communications Software 10-5
10.3.9 System Administration 10-5
10.3.10 Application Software 10-6
10.3.11 Operator Training Simulator Trainer 10-6
10.3.12 On-Site Support 10-6
10.3.13 Operator Training 10-7
10.4 Location and Number of Students 10-7
10.5 Training Costs 10-8
10.6 No Additional Charges 10-8

List of Exhibits:

Exhibit 10-1: Course Attendance and Location 10-7

10. Training

R[1] The Vendor shall prepare and deliver a comprehensive training program on the operation and maintenance of the ADMS-SCADA.

R[2] The training program shall identify the different skill sets required by users in accordance to their areas of responsibility and include the sequence of courses required to achieve the required proficiency levels.

R[3] A train the trainer program shall also be defined for training new employees.

10.1 Scope of Training

R[1] The training curriculum shall comprehensively train AE staff on all Vendor-supplied software to be provided with the ADMS-SCADA.

R[2] For third-party products, Vendor shall provide training on how the product is configured and used in the ADMS-SCADA.

10.1.1 Training Location

R[1] AE prefers that the training be conducted at AE provided facilities.

R[2] Training may take place at the Vendor's site when approved by AE.

10.1.2 Self-Study Courses

R[1] AE prefers classroom-style courses for all training. Self-study training using books, computer-aided instruction (CAI) or computer-based training (CBT) may be used as supplementary training.

10.1.3 Recording of Courses

R[1] AE shall be permitted to make video and audio recordings of all Vendor-delivered and third party vendor training classes.

R[2] Recordings of training sessions shall be for AE. AE will only use recordings of training supplied by Vendor to support on-going training for AE internal requirements.

10.2 Training Documents

R[1] The Vendor shall prepare a training plan in cooperation with AE.

R[2] No training will be considered complete without AE's written acceptance.

R[3] All training material shall be written or prepared by, or under the supervision, of qualified technical writers and tested for readability. An effort shall be made to organize information in a logical and functional manner.

R[4] Where appropriate, the documentation described in Section 8 which includes the Design Document and the Maintenance and Operation's Manual shall be integrated into the training so that they can be used as learning and reference resources.

10.2.1 Training Plan

R[1] The training plan shall be included in the ADMS-SCADA approved project schedule.

R[2] A logical sequence of courses shall be arranged, so that training on base system elements (e.g., operating system, languages, database, and displays) is given before the training for specific ADMS-SCADA elements (e.g., applications).

R[3] The training plan shall list each course to be taken, the dates for the course, and the expected number of students to attend.

R[4] Vendor will schedule courses a minimum of one month prior to course date; final dates will require AE approval.

R[5] The plan shall include the pre-requirements needed to take each courses as well as the course outcomes. Where appropriate a final exam shall be developed by the Vendor and administered.

R[6]

10.2.2 Course Descriptions

R[1] Course descriptions shall be included with the training plan.

10.2.3 Course Material

R[1] The Vendor shall provide all necessary training materials, including course manuals and reference materials.

R[2] Each trainee shall receive individual copies of the training materials and one additional set shall be provided for AE archives in both hardcopy and electronic form.

10.3 Training Requirements and Instructor Qualifications

R[1] Course instructors shall have demonstrated technical competence in the subject and previous instructing experience.

R[2] Course instructors will be required to provide list of references and details of related experience using Vendor's product as submitted in the specification.

R[3] Course instructors shall have experience teaching at least 3 similar courses to other clients on the vendor's product required by this RFP.

R[4] Where practical, Subcontractors shall deliver training on their products directly.

R[5] However, the Vendor shall remain responsible for selecting these courses, coordinating their delivery, and ensuring that all training objectives are met.

R[6] Vendor will provide training using AE data.

R[7] As a minimum, the training shall consist of the following types of courses.

10.3.1 System Overview

R[1] The system overview course shall be the first course in the training sequence.

R[2] The course shall serve as an introductory class for AE personnel who are designated to attend additional training later.

R[3] It shall also provide each trainee with a general understanding of the ADMS-SCADA including those aspects of the ADMS-SCADA for which the trainee will not receive additional training.

10.3.2 Database and Display Building

R[1] The database and display building courses shall be scheduled to coincide with the delivery of the PDS.

R[2] The courses shall teach students how to prepare the input data to define the ADMS-SCADA operating environment, to build the ADMS-SCADA database and displays, and to prepare the database administrator to maintain and modify the database and its structures.

10.3.3 Data Engineering Workshops

R[1] The objectives of the workshops are to bridge the gap between the training on the mechanics of database and display building and understanding practical design and conceptual issues.

R[2] These workshops shall use AE actual data, displays, and models to ensure that AE is properly engaged in database and display building activities.

R[3] The workshops shall be scheduled after the databases and display building courses.

R[4] The workshops shall be centered on hands-on training using the PDS.

10.3.4 Information Management

R[1] The Information Management courses shall be designed to train AE personnel in the use of the Information Management capabilities of the ADMS-SCADA, including selections of items to be archived, calculations associated with historical data, and report building features.

R[2] These courses shall be especially oriented for those AE personnel who develop and maintain displays, reports, and calculations relating to Information Management data and for those AE personnel who maintain the ADMS-SCADA as an enterprise-wide resource.

10.3.5 Operating System Administration

R[1] The Operating System (OS) administration course shall be designed to train the students in managing and maintaining the ADMS-SCADA at the operating system level.

10.3.6 System Programming Languages

R[1] Courses shall be provided for each of the programming languages that are used in the ADMS-SCADA.

R[2] Although it is anticipated that the students may be experienced software engineers, the Vendor will provide training for students having minimum proficiency in the programming languages used in the ADMS-SCADA.

10.3.7 Programming in the ADMS-SCADA Environment

R[1] This course shall instruct the student on the skills needed to program in the ADMS-SCADA software environment and shall be designed for the software engineers responsible for maintaining, expanding, or adding new functions.

10.3.8 Communications Software

R[1] The Vendor shall provide training on the communications among data sources, communications network software used for the ADMS-SCADA local and wide area networks, and on the interfaces or communications links with the external subsystems and networks.

R[2] Training shall be provided for both Vendor and Subcontractor supplied software and communications products.

10.3.9 System Administration

R[1] The System administration course shall familiarize participants with the procedures necessary to operate the system as an integrated entity, to recognize and respond to malfunctions, and to perform maintenance functions.

R[2] The only prerequisite for this course shall be familiarity with the overall functionality and architecture of the ADMS-SCADA.

R[3] System and user security training shall be included in the System Administration course plus any other applicable courses to promote security awareness and provide an understanding of security policies, processes, and tools used with the ADMS-SCADA.

10.3.10 Application Software

R[1] The Vendor shall provide training on application software.

R[2] These shall cover all ADMS-SCADA applications other than those already covered in the database, display, and Information Management courses.

R[3] Each application course shall be organized to be responsive to AE specific requirements and shall be regarded as an extension to the standard courses that are provided.

R[4] The design specifications and the user manuals prepared for the each regional ADMS-SCADA shall be used as course text where applicable.

R[5] The Application Software training shall be conducted for all ADMS-SCADA applications in the Specification.

10.3.11 Operator Training Simulator Trainer

R[1] This course shall cover the operation of the OTS associated with the Option selected by AE (Section 14). The course will provide the instruction and skills necessary to set up and run training using the OTS and shall include at a minimum scenario building and maintenance.

10.3.12 On-Site Support

R[1] To supplement formal training and to assist the Vendor in developing customized application software, AE may provide staff at the Vendor's site for 3 to 6 month periods throughout the duration of the project.

R[2] This staff will attend training courses scheduled to promote early involvement in the implementation work.

R[3] These individuals may spend from 5-15 business days at a time at the Vendor's facility during system implementation and shall participate in the design reviews and integration of ADMS-SCADA programs as their primary responsibility.

R[4] The staff may also be involved in system integration and testing.

R[5] The staff may be trained to use the Vendor's standard software development, documentation, and quality assurance practices.

10.3.13 Operator Training

R[1] The objective of this course is to train AE staff in preparation for development of operator training courses by AE.

R[2] All operator-training documentation shall be delivered in source form to allow AE to revise and supplement the material.

10.4 Location and Number of Students

As a reference only, this course listing below is presented. It is recognized that the vendor will develop a list of courses including descriptions of the content of each course. Vendor will submit the course list and content to AE for approval.

R[1] The number of the students that shall attend each training course and the desired location for the course are listed in the following table.

Exhibit 10-1: Course Attendance and Location

Course	Total Number of Students	Number of Sessions	Location
SCADA/ADMS-SCADA Overview	30	2	AE site
Database and Display Building	10	2	AE site
Data Engineering Workshops	10	2	AE site
ADMS-SCADA Data Engineering Seminar	10	2	AE site
Information Management	10	2	AE site
Operating System Administration	10	2	AE site
System Programming Languages	10	2	AE site
Programming in the ADMS-SCADA Environment	10	2	AE site

Course	Total Number of Students	Number of Sessions	Location
Communications Software	10	2	AE site
System Administration	10	2	AE site
ADMS-SCADA System Administration Training	10	2	AE site
OTS Trainer	12	2	AE site
ADMS-SCADA Advanced Applications	10	2	AE site
OMS Applications	10	2	AE site
Training in Residence	2-4	N/A	Vendor's site (3-6 month rotations over the duration of the project) (reference Section 10.3.12)
ADMS-SCADA Operator Training - Train the Trainer	10	2	AE site

10.5 Training Costs

R[1] AE anticipates that the courses to be taken and the number of students attending each course may change over the course of the contract.

R[2] Exhibit 10-1 is a guide but may be changed by agreement of the project managers.

R[3] Therefore, the total price of all training included in the contract shall be considered as a training allotment, and AE, in consultation with the Vendor, may revise the training curriculum and the participants at each course as long as the training allotment is not exceeded.

R[4] AE will be responsible for all hardware and training facilities for training performed at AE sites.

10.6 No Additional Charges

R[1] The Vendor shall be responsible for any additional costs of training including, but not limited to, courses and the travel and living expenses of students attending the courses where the need for such training is attributed to any of the following conditions:

R[1.A] Delays in the project schedule caused by the Vendor as determined by AE.

R[1.B] Inadequate or poor quality training that fails to meet AE's standards or requirements for quality, content, or timeliness.

R[1.C] Changes to any software deemed necessary during the project to meet the requirements of the proposed Contract and this Specification.

R[1.D] Any change in the scope of the proposed Contract and this Specification, unless the cost of the additional training is included in the cost of the change.

Table of Contents

11. Project Implementation 11-1
11.1 Implementation and Project Management Responsibilities 11-1
11.1.1 AE's Responsibilities 11-4
11.1.2 Consultants 11-6
11.1.3 Third-Party Software 11-7
11.2 Project Organization 11-7
11.2.1 AE Project Manager 11-7
11.2.2 The Vendor's Project Manager and Project Personnel 11-9
11.2.3 On-Site Offices 11-9
11.3 Project Documents 11-10
11.3.1 Document Hosting Site 11-10
11.3.2 Documentation Plan 11-10
11.3.3 Project Progress Reports 11-11
11.3.4 Project Meetings, Agendas, and Minutes 11-13
11.3.5 Detailed Approved Project Schedule 11-14
11.3.6 Risk Management Process 11-14
11.4 ADMS-SCADA Testing, Shipment, and Commissioning 11-15
11.4.1 Factory Acceptance Testing (FAT) 11-15
11.4.2 Authorization for Shipment 11-16
11.4.3 System Installation 11-16
11.4.4 Start-Up 11-17
11.4.5 Site Acceptance Testing (SAT) 11-17
11.4.6 Availability Test 11-18
11.5 Services to be performed 11-18
11.5.1 Objectives 11-18
11.5.2 Implementation 11-19
11.5.3 Required Services 11-20
11.5.3.1 Project Management 11-20
11.5.3.2 Project Launch / Kickoff 11-23
11.5.3.3 Project Discovery Phase 11-24
11.5.3.4 Project Design Phase 11-25
11.5.3.5 Project Development Phase 11-28

Table of Contents

11.5.3.6 Project Test & Deployment Phase 11-30
11.5.3.7 Project Stabilization Phase 11-31
11.6 Project Assumptions 11-32
11.7 Fees 11-34

List of Exhibits:

Exhibit 11-1: Project Document References 11-10

11. Project Implementation

R[1] This section specifies project implementation requirements, including responsibilities of AE and the Vendor, project management procedures, project documents, the activities leading up to shipment of the ADMS-SCADA, and the installation, training, commissioning, and site test activities. The project life cycle will include all project related work including pre-planning, initiation, gap analysis, project kick-off, work breakdown structure development, execution of work, control of work, testing, commissioning and final acceptance; all phases of the project.

11.1 Implementation and Project Management Responsibilities

R[1] The general responsibilities of AE and the Vendor are presented below.

R[2] Other sections in the Specification may also present responsibilities.

The requirements of this section and other sections are all inclusive; in the event of a conflict, the more stringent of the responsibilities,as interpreted by AE will be required of the Vendor.

Vendor Responsibilities

R[1] The Vendor's specific responsibilities shall include:

R[1.A] Specifying all required ADMS-SCADA hardware and platform software to meet all functional and performance requirements.

R[1.B] Providing all engineering, software design, development, and integration services necessary for ADMS-SCADA implementation.

R[1.C] Providing and integrating all application software except that to be developed by AE. This responsibility extends to all software developed by Subcontractors.

R[1.D] Providing all ADMS-SCADA displays and reports other than those to be developed by AE.

R[1.E] During the early design phase of the ADMS-SCADA, Vendor shall, with AE's assistance, finalize the rules and procedures for developing a standard naming convention for populating the ADMS-SCADA and historian databases.

R[1.F] Load the distribution system operations databases of AE's existing systems, including GIS, and installing the converted databases into the Program Development Systems (PDS) and the ADMS-SCADA while at the Vendor's facility.

R[1.G] Allow all distribution system network model updates up until two months prior to the pre-Factory Test and an update two weeks preceding FAT.

R[1.H] Integrating the databases, displays, reports, and software defined and developed by AE.

R[1.I] Supplying a display style guide defining all discretionary display parameters used by the Vendor when developing standard ADMS-SCADA displays and reports.

R[1.J] Defining and coordinating a software and database management methodology that ensures synchronization of the system database definitions and applications software both between the Vendor's factory and AE site and for the ongoing maintenance of the ADMS-SCADA at AE.

R[1.K] Ensuring that all required security measures have been incorporated in the ADMS-SCADA and all software, upon delivery, is free of viruses, trapdoors, and other software contaminants, contains no software enabled with "electronic self-help", is purged of all sample scripts and sample code, and has had all default accounts and passwords removed or disabled.

R[1.L] Managing, coordinating, and scheduling the activities of all Subcontractors employed by the Vendor for this project.

R[1.M] Implementing the ADMS-SCADA according to the quality standards acceptable to AE.

R[1.N] Training AE's staff to be self-sufficient and able to operate, maintain, and upgrade the complete ADMS-SCADA.

R[1.O] Work closely with AE staff to facilitate a knowledge transfer.

R[1.O.i] As an example, during on-site activities, AE staff, guided by Vendor staff, will actively participate in installs, upgrades and modifications to ADMS-SCADA.

R[1.P] Supplying ADMS-SCADA documentation such as instruction manuals, maintenance manuals, drawings, software design and user documentation, and other appropriate material that together fully defines the supplied system and allows AE to operate, maintain, backup, restore, and upgrade the ADMS-SCADA software.

R[1.Q] Supplying final (“as built”) documentation that is accurate and complete.

R[1.R] Providing adequate facilities and resources for, as well as performing, factory testing.

R[1.S] Support AE in defining what data is required to test each function in FAT.

R[1.T] Providing an environment that allows for reproducible execution of all ADMS-SCADA functional performance tests conducted during factory acceptance testing.

R[1.U] Transportation and delivery of all Vendor-provided deliverables to AE site or sites.

R[1.V] Providing proper site planning information such as the power requirements, specifications for air conditioning, power grounding, EMI, seismic protection, dust protection, fire protection, equipment size, and other site requirements as necessary for the proper environmental control and operation of all ADMS-SCADA equipment.

R[1.W] Performing the installation of the ADMS-SCADA at AE’s sites with AE’s assistance (reference Section 11.4.3).

R[1.X] Performing, with AE’s assistance, system start-up after satisfactory system installation, i.e., powering up the system, loading correct versions of all software and databases, activating data links, verifying correct operation of the system, and turning over to AE an operational system ready for site testing.

R[1.Y] In addition, software install and build shall be performed at the Vendor’s factory from the source code that is placed in escrow by the Vendor

R[1.Z] Performing, with AE's assistance, after delivery and start-up of the system, but prior to any site testing, configuration and tuning of all functions for proper operation.

R[1.AA] Participating in testing at AE' site, including correcting all reported variances.

R[1.BB] Demonstrating weekly that the work is progressing according to the approved project schedule.

R[1.CC] Developing and maintaining the approved project schedule.

R[1.DD] Providing office space and services for AE personnel at the Vendor's site.

R[1.EE] Providing a mutually agreeable secure remote computer access from the Vendor's factory to support the field-installed systems.

R[1.FF] Maintaining the ADMS-SCADA up to the start of the warranty.

R[1.GG] Providing and implementing all required warranty services.

R[1.HH] Providing verification that all employees and subcontractors working on this project meet NERC background screening and security training requirements (Reference CIP-004 – Cyber Security - Personnel and Training).

R[1.HH.i] The Vendor shall conform and provide the required submittals to meet AE Corporate policy for Vendors (NG-SP-6).

R[1.HH.ii] Quality Assurance and Quality Control plan, approved by AE, ensures the data model is reviewed by the Vendor before delivering to AE. Vendor will be required to show evidence of quality control. Accuracy check of the data model by the vendor prior to providing it to AE shall include at a minimum a connectivity check, point to point check of major devices and verification of model convergence.

11.1.1 AE's Responsibilities

R[1] AE will be responsible for the following:

R[1.A] Providing input power to equipment enclosures.

R[1.B] Providing and installing all ADMS-SCADA hardware and platform software as specified by Vendor according to the approved project schedule.

R[1.C] Providing WAN and RTU communications media to connect to the EMS/ADMS-SCADA LANs.

R[1.D] Providing a high-speed data link to the Program Development System (PDS) to facilitate project implementation tasks, support and maintenance by the Vendor.

R[1.D.i] The data link will adhere to AE corporate standards for Vendor communications.

R[1.E] Providing the firewalls to connect the Corporate WAN to the EMS/ADMS-SCADA DMZ.

R[1.F] Supplying display conventions and standards to be followed by the Vendor when preparing or customizing displays for this project.

R[1.G] Final approval of project deliverables such as, but not limited to, approved project schedule, software and hardware functional design documents, documentation plan, user manuals, custom display and report formats, drawings, progress reports, training program, quality assurance plan, test plans and procedures, test results, support services (including maintenance), and as-built ADMS-SCADA documents.

R[1.H] Providing Small World XML extract for connectivity and Milsoft EDQB extract for electrical characteristics of AE system for conversion to the ADMS-SCADA database and installation in the ADMS-SCADA.

R[1.I] Providing distribution system network model database updates up until two months prior to the pre-Factory Test and again two weeks prior to FAT.

R[1.J] Populating the ADMS-SCADA with data not included in the existing AE databases.

R[1.K] Using the Program Development System (PDS) to create displays and generate reports according to samples and templates provided by the Vendor.

R[1.L] Providing documentation, interface details, engineering drawings, and schematic diagrams of AE-furnished equipment to be directly interfaced with the ADMS-SCADA.

R[1.M] Coordinating and supervising the Vendor's work to be performed at AE's facilities.

R[1.N] Attending pre-factory tests (at AE discretion).

R[1.O] Participating in factory tests and approving test results.

R[1.P] Assisting the Vendor with the installation.

R[1.Q] Conducting site tests and approving test results.

R[1.R] Performing the availability test.

R[1.S] Providing test data for processes external to the ADMS-SCADA.

R[1.T] Providing hardware that is not part of the ADMS-SCADA, but to which the system must interface to the Vendor for use during the factory tests.

R[1.T.i] AE will be responsible for all set up and configuration needed for such hardware sent to the Vendor by AE.

R[1.U] Verifying that all Vendor materials, installation practices, and workmanship conform to requirements.

R[1.V] Providing media to allow remote access to the field-installed ADMS-SCADA from an external Vendor site.

R[1.W] Providing facilities for on-site training and Vendor work space.

11.1.2 Consultants

R[1] AE may choose to retain the services of consultants for assistance with the project.

R[2] The Vendor shall consider such Consultants as part of AE's project team, give them access to all project documentation and information, and permit them to participate in project meetings and all other project activities, at AE's sole discretion. (Reference the Terms & Conditions)

11.1.3 Third-Party Software

R[1] Where any Vendor-provided applications software or software modules developed by a third-party are integrated into the ADMS-SCADA, the Vendor shall be responsible for integrating, testing, and meeting the functional, security, and performance requirements of this software in the ADMS-SCADA environment.

11.2 Project Organization

R[1] The Vendor, with assistance from AE, will be responsible for developing a project communication plan. AE will have final approval of the communication plan.

11.2.1 AE Project Manager

R[1] AE project manager shall be responsible for representing AE interests throughout the project.

R[2] The successful completion of the proposed scope of work depends on the full commitment and participation of AE management and personnel. AE will be responsible for performing the following actions in support of the project listed below:

R[2.A] Manage AE personnel and responsibilities for this project according to the approved project schedule.

R[2.B] Serve as the interface between the Vendor and all AE business units and other City departments participating in the project.

R[2.C] Participate in Project status meetings.

R[2.D] Work with the Vendor project manager to define expense reporting requirements

R[2.E] Resolve and/or communicate needs for project change control procedures to address deviations from the approved project schedule.

R[2.F] Assist Vendor in development of a formal change control process. Vendor will have responsibility for developing a process; AE will review and have final approval.

R[2.G] Help resolve project issues and escalate issues within AE's organization, as necessary.

R[2.H] Work closely with the Vendor to affect a knowledge transfer of Austin Energy's business processes and current software configuration to the Vendor.

R[2.I] Work closely with the Vendor to affect a knowledge transfer of the implementation process to Austin Energy staff.

R[2.J] Evaluate and approve the Vendor's personnel, including all third party contractors, or Vendors the Contractor employs on the project.

R[2.K] Provide access to Austin Energy's current environments as needed.

R[2.L] Attend workshop(s) to review technical and functional aspects of Austin Energy's current processes.

R[2.M] Assist in the install of the ADMS-SCADA in all environments.

R[2.N] Attend functional review of the installed ADMS-SCADA in AE's environments and provide feedback to the Vendor at the completion of the demonstration / functional review.

R[2.O] Assist Vendor with unit testing of the ADMS-SCADA in the Development environment. Document findings and provide feedback to Vendor.

R[2.P] Review, approve, and update Vendor's test acceptance plans, scenarios or outlines for system testing.

R[2.Q] Test the ADMS-SCADA in the Test environment. Document findings and provide feedback to Vendor.

R[2.R] With assistance from Vendor, deploy the ADMS-SCADA to AE's Production environment.

R[3] All written correspondence with AE shall be addressed to AE project manager. All electronic communication shall be directed to AE staff as required by AE.

11.2.2 The Vendor’s Project Manager and Project Personnel

R[1] The Vendor shall designate a project manager. The project manager will function independently of the technical leads on the project and shall be responsible for the co-ordination of all project work for the ADMS-SCADA and for the communications between the Vendor and AE.

R[2] Once the Vendor has designate a project manager, the manager named cannot change without AE approval in writing.

R[3] The project shall be staffed with a core project team. Additional personnel shall be assigned to work under the direction of the core team as required to effectively implement the ADMS-SCADA.

R[4] Core project team members shall have previous experience in a similar position on at least one other project that is similar in size and scope to this project.

R[5] The designated Vendor executive shall be available to attend executive level AE management meetings as required by AE.

R[6] The Vendor shall provide resumes for key personnel assigned to the project.

R[7] AE shall have approval rights for all personnel assigned to the project and any changes proposed by the Vendor.

R[8] AE shall have the right to request replacement of Vendor proposed staff at any time during the project.

11.2.3 On-Site Offices

R[1] Both AE and the Vendor shall make available office facilities for use by the other party.

R[2] Office space, furniture, and reasonable office services such as telephone, facsimile, copying, printing, mail and courier services, and access to meeting rooms shall be provided.

11.3 Project Documents

R[1] Project documents shall specifically include the following and shall be delivered to AE by the dates indicated in the reference section (where the content of the document is also further defined):

Exhibit 11-1: Project Document References

Document	Reference Section
Documentation Plan	Section 11.3.1
Project Progress Report	Section 11.3.3
Project meetings, Agendas and Minutes	Section 11.3.4
Project Correspondence	Section 11.3.5
Detailed Approved project schedule	Section 11.3.6
Risk Management Process	Section 11.3.7
Product User documents	Section 11.3.8

11.3.1 Document Hosting Site

R[1] The Vendor will provide a secure, internet accessible site (SharePoint based or equivalent) to facilitate the sharing of documents with AE.

R[2] AE staff will be issued logon ID's and passwords.

R[3] The passwords may be modified by the AE staff after first entering the site.

R[4] All project documents listed in Exhibit 11-1: Project Document References will be hosted on this site.

R[5] Provision will be made for other documents as necessary.

11.3.2 Documentation Plan

R[1] A documentation plan shall be submitted to AE twenty-business days after contract award. The plan will be integrated into the approved project schedule.

R[2] The documentation plan shall serve as a checklist throughout the project and shall be revised and resubmitted by the Vendor as necessary.

R[3] Documents shall be submitted in a sequence that allows AE to have all of the information necessary for reviewing or approving a particular document at the time of its submittal.

R[4] Documentation shall be submitted in a manner that allows for a reasonably paced review effort.

R[5] The documentation plan shall be subject to AE approval and shall be included in the approved project schedule.

11.3.3 Project Progress Reports

R[1] A project progress report shall be prepared by the Vendor and sent to AE by the third business day of each month through the start of the warranty period. AE will have final approval of the formatting and content of the reports.

R[2] A Vendor executive shall sign the project progress report.

R[3] The progress report shall include:

R[3.A] A general assessment of the progress on the project.

R[3.B] An explanation of existing and forecast costing, approved project schedule, staffing variances, the cause or source of the variance, alternatives and recovery plans considered, solutions adopted or recommended, and the outcome achieved or anticipated.

R[3.C] A list of external items that may affect the progress of the project that are not directly in the control of the project manager.

R[3.D] The required delivery date of AE-furnished information.

R[3.E] Unresolved contract issues including the status and action plan for resolution.

R[3.F] A list of action items.

R[3.F.i] The action item number

R[3.F.ii] The date the item was opened

R[3.F.iii] References to the originating transmittal and any reference documents

R[3.F.iv] Action item status (open, closed)

R[3.F.v] Resolution due date

R[3.F.vi] The responsible organization or person

R[3.F.vii] A description of the action required

R[3.F.viii] The date of action completion (when each item is closed)

R[3.F.ix] References to transmittals or other documents recording the resolution.

R[3.G] Anticipated activities for the following month.

R[3.G.i] The Vendor shall provide a minimum of three weeks advance notice to AE whenever any of AE's activities are placed on the critical path, so that AE will have time to make adjustments to ensure that the required staff is available.

R[3.H] Correspondence logs, one for transmittals to AE from the Vendor and one for transmittals to the Vendor from AE.

R[3.I] A contract change log containing information for each requested change in requirement: The Contract Change Log shall include the following information:

R[3.I.i] The Contract Change log/item number

R[3.I.ii] Change Description

R[3.I.iii] Impact to schedule and cost.

R[3.I.iv] The date the change was created and by whom

R[3.I.v] Appropriate documentation to support the change

R[3.I.v.a] Approval Date and Name of AE Project Manager. AE executive management will have final approval of changes that result in revised project schedule baselines.

R[3.J] Training Budget Status (Section 10.5, Training Costs).

11.3.4 Project Meetings, Agendas, and Minutes

R[1] Project meetings shall be held to review project progress, ensure correct interpretation of the contract, review technical and commercial issues, and maintain co-ordination between AE and Vendor.

R[2] Meetings shall be approved project scheduled at appropriate times, but shall be approved project scheduled every month on average.

R[3] The meetings shall be held on site at AE. The Vendor's project manager shall prepare a meeting agenda and submit to AE for review and approval at least 10 business days prior to the meeting.

R[4] The Vendor shall prepare minutes of each meeting. Both AE and the Vendor shall review and approve the minutes. AE will approve the format of the meeting minutes.

R[5] In addition, AE may choose to hold selected meetings via video teleconference and/or webex.

R[6] **Project Correspondence**

R[1] All requests and transfers of information between the parties shall be made in writing, using Microsoft Word (or .pdf documents for view-only documents) and shall be documented with letters of transmittal.

R[2] All correspondence from each party shall be dated and uniquely numbered.

R[3] Correspondence may be exchanged by electronic mail. Final invoices shall be submitted as required by AE.

R[4] All project management documentation (e.g., approved project schedule, correspondence, memos, meeting minutes, and monthly progress reports) shall be produced using the Microsoft Office suite.

R[5] AE will have final approval of numbering scheme developed and used by Vendor to minimize file storage and retrieval efforts. .

11.3.5 Detailed Approved Project Schedule

R[1] The Vendor shall submit for AE approval a detailed project schedule using Microsoft Project. The entire project life cycle will be planned and scheduled. Schedule will include project pre-planning, kick-off through final commissioning and acceptance of complete and totally functioning systems. The Schedule will include the training and documentation plan.

R[2] This shall describe all the project activities of both the Vendor and AE.

R[3] The approved project schedule shall show the phasing and details of the system implementation for the ADMS-SCADA (consistent with an agreed-upon implementation sequence).

R[4] However, the approved project schedule shall include all of the dependencies of tasks contingent on documentation and training tasks.

R[5] The Vendor shall use Microsoft Project to maintain the approved project schedule.

R[6] Microsoft Project shall be used to track the progress of the project from start through completion.

R[7] Project schedule monitoring shall be based on analysis of variances from baseline start and finish dates to accurately reflect final completion date for the entire project.

R[8] The approved project schedule presented to AE shall be that used by the Vendor to manage their internal resources.

11.3.6 Risk Management Process

R[1] As an additional control and quality assurance process, the Vendor shall implement a Risk Management Process to minimize potential internal and external risk items and help ensure the success of the project.

R[2] The Vendor shall follow AE's Risk Assessment and Management process.

R[3] As a first step, the Vendor shall perform a risk assessment with AE.

R[4] A Risk Assessment is useful for identifying, characterizing, prioritizing and deciding how to best handle each risk factor that threatens the project's ability to meet its objective within approved project schedule and budget.

R[5] Risk assessments shall be performed by the Vendor, with assistance from AE, throughout the life of the project and as required by AE. Vendor shall provide and propose detailed plans for resolving and mitigating risks. Vendor shall provide detailed plans for schedule recover when risks are identified.

R[6] The potential impacts on the project's success and the recommended contingencies to manage or mitigate the risks shall be communicated to all interested and involved parties.

R[7] The Risk Assessment process shall include the following techniques:

R[7.A] Set up a table that itemizes each risk factor

R[7.B] Identify and rate each risk with a factor of High, Medium or Low in terms of its potential impact, probability of occurrence, and difficulty of timely detection.

R[7.C] Extract the combined effect of these three values, and score each risk factor as High, Medium, or Low overall.

R[7.D] An issue with a high rating for either impact or probability of occurring should be mitigated and resolved as soon as it is identified.

R[8] The goal is to preemptively take the necessary actions to (1) decrease the impact of a risk should it occur and/or (2) decrease the chance of the risk occurring, as appropriate.

11.4 ADMS-SCADA Testing, Shipment, and Commissioning

R[1] The following testing and system commissioning activities shall be supported and supervised by the Vendor.

11.4.1 Factory Acceptance Testing (FAT)

R[1] Factory tests are described in Section 9, Quality Assurance and Testing, along with conditions for test initiation and completion.

R[2] These tests include a preliminary factory test and a factory test.

R[3] These tests shall be executed in the following sequence:

R[3.A] Preliminary factory test

R[3.B] Factory test

R[3.B.i] Equipment test

R[3.B.ii] Functional test

R[3.B.iii] Performance test

R[3.B.iv] Stability test

R[3.B.v] Unstructured test

11.4.2 Authorization for Shipment

R[1] Acknowledgement of the successful completion of all factory tests shall be deemed as authorization for the Vendor to deliver the tested software to AE site.

R[2] Shipment will not be authorized until all variances have been corrected as addressed in Section 9.5.3.

11.4.3 System Installation

R[1] After the equipment is delivered to AE sites and received by AE, the ADMS-SCADA installation activities shall commence:

R[1.A] Movement and placement of the equipment.

R[1.A.i] Delivered hardware shall be assembled and interconnected to allow redundant systems, except the QAS, to be installed with each component system of the redundant pair located in separate computer rooms at AE's discretion.

R[1.B] Interconnection of the equipment, including interconnection with previously delivered equipment.

R[1.B.i] Vendor will provide the LAN cabling to connect Vendor provided equipment to the AE connection points and will make these connections.

R[1.B.ii] AE will lay the cable between locations (*e.g. data center to control room) when required.

R[1.C] The installation test (refer to Section 9.10.1, Installation Test).

11.4.4 Start-Up

R[1] After installation of the ADMS-SCADA, AE will need to run the new ADMS-SCADA in parallel with the existing systems where appropriate.

R[2] The duration of this window of time will be mutually agreed by AE and the Vendor.

R[3] The Cutover/Transition plan (reference Section 8.11) shall be produced and used during this time period to facilitate an efficient and safe transition to the new ADMS-SCADA.

R[4] Start-Up of the ADMS-SCADA shall begin immediately after the successful completion of the installation test.

R[5] Start-Up activities shall include but shall not be limited to checking that the on-site operation of the ADMS-SCADA, including its communications interfaces to all field devices and external systems are ready for commercial operation.

R[6] AE shall be responsible for this activity, with support from Vendor. Per the Approved Project schedule, Vendor shall allocate a minimum of two core project team members full-time at AE site throughout this activity. The Vendor project manager will be required to be on-site as required by AE.

11.4.5 Site Acceptance Testing (SAT)

R[1] The site test at the ECC and BUCC (reference Section 9.10) shall be started after installation and AE field update activities are complete.

11.4.6 Availability Test

R[1] The availability test shall be started after site tests and ADMS-SCADA commissioning have been successfully completed, and the availability test prerequisites (Section 9.6.1, Test Initiation) have been completed to AE satisfaction.

R[2] The availability test shall be deemed to be started when the ADMS-SCADA is commissioned, is monitoring and controlling the complete power system, and all interfaces are operational for a minimum 10 business day duration.

11.5 Services to be performed

R[1] The implementation of an Advanced Distribution Management System (ADMS-SCADA).

11.5.1 Objectives

R[1] Conduct discovery / gap sessions to provide a complete solution definition to ensure business needs are being met.

R[2] Conduct design sessions to provide a detailed design to ensure all requirements are being met and system functionality is exposed as the system is implemented in AE's development, test and production environments.

R[3] Conduct planning sessions to provide a detailed plan for performing the system implementation in AE's development, test, backup and production environments.

R[4] Implement and tune all deploy instances of the ADMS-SCADA systems and models around the AE grid, like the State Estimation, Load Flow, Fault Location, Voltage and VAR control, among others.

R[5] Develop detailed manuals and provide training on how to tune the above models and systems.

R[6] Perform sensitivity analysis regarding the observability of different areas of the system in regard to the performance of the above systems and models.

R[7] Make sure that in those areas of the system identified by AE as critical, the above systems and models operate at top performance and advise AE when more instrumentation or communication system enhancements are necessary.

R[8] Identify areas of the AE system in which the implementations of the above systems and models are not expected to perform well due to insufficient instrumentation or limitations of the communications system.

R[9] Identify areas in which increasing the number of measurement points and enhancing communications could considerably improve observability and system performance.

R[10] AE will rely upon product configuration rather than product modifications and will attempt to modify its business processes to fit the technology workflow. AE seeks proposed solutions that minimize customization and impacts to future upgrades. However, the solution should offer a development framework for easily building custom applications for the new ADMS-SCADA.

R[11] The implementation must include Disaster Recovery and Business Continuity considerations that ensure the efficient and effective recovery and/or continued successful operation of the ADMS-SCADA under the loss of key infrastructure components.

R[12] Vendor must provide training for all aspects of the ADMS-SCADA.

11.5.2 Implementation

R[1] AE is limited in available-qualified resources to staff the project. Therefore, AE expects to rely heavily upon the Vendor's resources and expects knowledge transfer from the Vendor's resources to AE staff. The Vendor is encouraged to provide a high-level resource or partner with a firm that can supplement the project with qualified resources. The Vendor should include hourly rates for each category of personnel on the team, in case AE wants to increase the level of support by the Vendor.

R[2] The ADMS-SCADA solution must include all components required for a successful installation of the software in all AE environments (development, test, backup, production) and ongoing production operation. The ADMS-SCADA solution shall include application software, installation services, documentation, training, knowledge transfer, support, maintenance, travel and all related costs.

R[3] Information not specifically requested by AE, but is relevant and necessary for a full and comprehensive understanding of the proposed solution shall be included in the attachments of the submittal. In addition, the Vendor shall respond to all Requirements.

11.5.3 Required Services

R[1] This section describes the minimum services the Vendor will provide the AE. These services and the corresponding activities, tasks and deliverables shall be included in the Proposal.

11.5.3.1 Project Management

R[1] The Vendor will provide project management for the Vendor responsibilities in this scope of work. The project team will follow agreed upon processes to manage the project. Project changes must be agreed to and approved by AE prior to action. In this activity, the Vendor will perform services that include the tasks listed below. In order to accomplish these tasks, AE expects the Vendor to provide a full time Project Manager and a full time Project Documentation Specialist throughout the complete project life cycle and until 10 business days past production deployment (go-live).

R[1.A] Review the complete RFP and the contractual responsibilities of both parties with AE Project Manager and the AE Project Team.

R[1.B] Coordinate the establishment of the project environment such as procedures and processes to include both electronic documents and operational methods.

R[1.C] Establish documentation and procedural standards for all aspects of Deliverable Materials (software and written).

R[1.D] Prepare, communicate and maintain the Vendor's integrated (AE and Vendor tasks) approved project schedule via Microsoft Project Server 2007 (.mpp). The Approved Project Schedule must list the activities, percent complete, baseline start and finish dates, tasks and subtasks, resource assignments, appropriate logic for each task, milestones, deliverables, (risks, risk impacts and approved project schedule impacts), roles, assigned AE resources, durations, dependencies, and estimates for performance of this scope of work and communicate status (accomplishments, next steps, risks, issues, action items and all required detail) to the AE Project Manager through the close of the Project. The final approved project schedule will be approved by AE and will utilize the AE MS Project Server 2007 Enterprise calendar (AE Project Manager is responsible for publishing the updated approved project schedule to AE's MS Project Server).

R[1.E] Prepare, communicate, and update Work Breakdown Structure (WBS) and WBS dictionary pages throughout the project life cycle and in collaboration with AE. Vendor will provide updates following each phase of the project.

R[1.F] Review, define, and further develop project tasks, approved project schedules, and resources and make changes or additions, as appropriate following established Project Change Control Procedures. Measure, communicate, and evaluate progress against the approved project schedule (as above) with the AE Project Manager and AE Project Team. Any approved project schedule changes are subject to the defined Change Control processes.

R[1.G] Vendor will work to propose solutions and resolve deviations from the approved project schedule as required by the change control process.

R[1.H] Review with AE Project Manager the Vendor's standard invoice format and billing procedure to be used on the project.

R[1.I] Conduct weekly approved project scheduled project status meetings and if necessary web meeting.

R[1.J] Administer the Project Change Control Procedure.

R[1.K] Coordinate and manage the business and technical activities of Vendor project personnel, including Vendor sub contractors.

R[1.L] Execute project communications as defined within the Kick-Off Meeting and the ADMS-SCADA Project Management Plan.

R[1.M] Create, maintain, and communicate a project organizational chart and contact list to include Vendor project staff and Vendor subcontractor staff.

R[1.N] Manage control of project documents and Deliverables/Deliverable Materials utilizing AE Sharepoint collaboration site.

R[1.O] Maintain an issue log which tracks issues raised and their resolution including the establishment of urgency and escalation criteria to be posted on AE's Sharepoint.

R[1.P] Cooperatively work with all AE sub-contractors.

R[1.Q] Develop meeting minutes of proceedings and decision summary made in meetings and workshops to be posted on AE's Sharepoint. AE will have final approval of meeting minutes before posting to Sharepoint.

R[1.R] Vendor agrees to participate in Executive Steering committee meetings, either in person or by conference call as required by AE. The meetings may be schedule to review project status and address project issues. Vendor will have both project management and Vendor executives attend as required by AE.

R[1.S] Maintain and update project reports through the Closing phase of the project, past the production deployment (Go-Live) date and as requested by AE.

R[1.T] Vendor will review work products with AE project manager and AE project team. Documents will be posted to Sharepoint and will use that tool for version control. AE will have a minimum15 business day review period for all work products (written / software).

R[1.U] Vendor will deliver where applicable and utilize AE standard tools: MS Project Server 2007, Sharepoint, MS Visio 2003, and MS Office in compliance with AE versions installed and in use.

R[1.V] Vendor will work collaboratively with AE project manager and AE project team to coordinate answers to questions and issues identified during the scope of this project.

R[1.W] Vendor will ensure that technical experts respond and address technical issues within 5 business days of request from AE.

R[1.X] Vendor will work jointly with AE to verify remote access connectivity and prevent and resolve connectivity issues for Vendor resources on a jointly determined pre-arranged approved project schedule.

Completion Criteria:	
These Deliverables will be complete when the Vendor has satisfied the completion criteria for all activities in this Scope of Work and AE has provided its acceptance of same pursuant to the Deliverable Acceptance Procedure set forth in Section 29 of 0400 ("Deliverable Acceptance Procedure"), including signature approval of the AE Project Manager:	
Deliverables:	
Deliverable 1	Weekly Updated AE MS Project Server 2007 Approved project schedule
Deliverable 2	Weekly Updated Status Reports (Project Status, Accomplishments, Next Steps/Upcoming milestones, Risk/issue list)
Deliverable 3	Weekly Updated WBS & WBS Dictionary Pages

11.5.3.2 Project Launch / Kickoff

R[1] The Vendor shall collaborate with AE Project Manager to draft a project management plan that defines the SOW, administrative rules of engagement, status reporting approach, meetings, change control process, and issue and risk management. The approved project schedule shall merge AE's tasks and milestones with Vendor's tasks and milestones. In this activity, the Vendor shall perform services that consist of the tasks listed below.

R[1.A] Develop / review project management plan, approved project schedule, team member roles and responsibilities and SOW, revise plan if necessary.

R[1.B] Establish project office and make logistics arrangements (equipment, badges, etc…).

R[1.C] Conduct project kick off meeting. The meeting should include a draft of the complete project plan, including the entire project life cycle from pre-planning to final acceptance by AE.

R[1.D] Review AE functional assessment materials from AE attached requirements to begin development of the Design Specifications Document

R[1.E] Prepare draft of project management plan, project schedule with work breakdown schedule (WBS) and WBS dictionary pages, dependencies, proposed dates, deliverables, tasks, and resources in preparation of the project kick-off meeting.

Completion Criteria:	
These Deliverables will be complete when the Vendor has completed and submitted the Project Management Plan draft and Project Schedule to the AE Project Manager and they are accepted per the Deliverable Acceptance Procedure by the AE PM. The activity is complete only when AE has approved the Project Schedule:	
Deliverables:	
Deliverable 4	Draft Project Management Plan
Deliverable 5	Draft / updated Project Schedule
Deliverable 6	Draft / updated WBS & WBS Dictionary Pages

11.5.3.3 Project Discovery Phase

R[1] The purpose of the discovery phase is to develop the Discovery / Gap Definition document. The gap definition document is the key deliverable as it communicates to AE the gaps between current functionality / process and the solution. In this activity, the Vendor shall perform services which consist of the following tasks listed below.

R[1] Conduct a series of workshops to gather those specifics and review in detail the process and requirements for system configuration to meet AE's business needs.

R[2] If there are any requirements that are not supported by the base system, perform analysis to define the detailed requirements for these items identified in the workshop(s).

R[3] Define interface requirements. Interface transactions are defined as to the business triggers and the transaction types.

R[4] Based on information gathered during the workshops, a detailed gap definition document is prepared to define how the system will be configured to close gaps identified and to meet AE's business needs.

Completion Criteria:	
These Deliverables will be complete when the Vendor has completed and submitted the Discovery / Gap Definition document to the AE Project Manager and it has been accepted by the AE Project Manager per the Deliverable Acceptance Procedure by the AE PM:	
Deliverables:	
Deliverable 7	Draft Discovery / Gap Definition document
Deliverable 8	Draft Requirements Document (numbered for SAT (Site Acceptance Testing) traceability matrix)
Deliverable 9	Updated architecture / topology diagram

11.5.3.4 Project Design Phase

R[1] The design workshops will provide the Vendor with information and background needed to deliver the Design Specifications document to ensure business processes continue in a streamlined fashion with minimal change. During the design phase, particular focus is on generating and completing the design document. The design document is the key deliverable as it communicates to AE how the identified gaps will be resolved and how the solution will be implemented to meet the requirements. The Vendor will conduct a series of workshops to define how the system will be implemented and configured for normal business activities. The Vendor shall provide recommendations to prepare the business and technical environment that supports the implementation– balancing business needs of certain functional requirements against the general design goal of avoiding customizations to the fullest extent possible. At a minimum, the Vendor shall conduct five design specifications workshops to design the business and technical processes in support of the project. The design specifications workshop sessions shall be conducted in the following order:

R[1.A] AE Assessment Findings Workshop - Review of AE's exhibits (RFP including requirements, documents from Discovery / Gap Phase).

R[1.B] Core team interviews - To review AE business areas, users, internal and external information exchange. Identify/develop, with active participation of the AE Project Core

Team, the business functions, processes, and data that will be targeted for support using the software.

R[1.C] General Process Design Workshops; at a minimum 10 business days in duration.

R[1.C.i] Business Process Review Workshops – Review the existing business processes using existing applications and sub-systems and discuss the to-be processes with the new ADMS-SCADA implementation.

R[1.C.ii] Review the new ADMS-SCADA capabilities and functionalities.

R[1.C.iii] Define a set of business process flows for the new system and sub-systems based on the out of the box, standard flows and capabilities of the product.

R[1.C.iv] Identify impacts to current business processes that require changes/revisions to policies and procedures.

R[1.C.v] Identify and document additional business requirements, configurations, screen changes, and database configurations.

R[1.C.vi] Review existing domains and necessity for additions or modifications.

R[1.D] Integration Workshops; at a minimum 10 business days in duration.

R[1.D.i] The Vendor shall meet with AE's systems experts to discuss documenting new and existing integration points, flow of the integration, and timing of the integrations.

R[1.D.ii] Evaluate the impact of new processes or configurations to existing integrations.

R[1.D.iii] The Vendor will review the existing integration architecture and update the architecture / topology diagram(s).

R[1.D.iv] Discuss process scenarios and identify the processing scenarios that AE will implement.

R[1.D.v] Discuss any new requirements determined after the RFP, including the feasibility of implementing such requirements.

R[1.D.vi] Discuss elements of integration that need special attention for a successful integration.

R[1.D.vii] Discuss all integration points relevant to integration scenarios.

R[1.D.viii] Focus on reusability and flexible business processes.

R[1.D.ix] Discuss any configurations necessary for each integration point and identify feasibility of implementing the requirement.

R[1.D.x] Develop recommendations for change, if any, to the application integration, data integration, and any other aspects.

R[1.E] Data Elements Workshop; at a minimum 10 business days in duration.

R[1.E.i] The Vendor shall meet with experts for the system plus each legacy sub-system to discuss and document the system details, data formats, data models and data extraction formats and strategies.

R[1.E.ii] Review current data to be mapped into the new system for continued use.

R[1.E.iii] Review data that is not necessary for day-to-day activities but is often required for reporting purposes. This data shall be made available via configured business and technical processes designated to access the new configured data tables.

R[1.E.iv] Provide recommendations for data quality issues based on best practices and compatibility with ADMS-SCADA.

R[1.E.v] Develop and review data integration / migration plan.

R[1.F] Reporting Workshop; at a minimum 5 business days in duration.

R[1.F.i]Review out-of-the-box reports and standard reporting capabilities of the new ADMS-SCADA.

R[1.F.ii] Review AE’s existing report requirements.

R[1.F.iii] Identify reporting needs not met by current system.

R[1.G] Workshops shall be conducted in 2-4 hour increments based on subject matter and team approved project schedule availability, with allowance for advance preparation time and post workshop documentation.

R[1.H] Each of these designs shall be detailed into task level steps that will be represented in the Design Specifications Document

R[1.I] Assist AE in the development of an updated infrastructure document showing any changes to existing infrastructure including new hardware and firewall/security rules (architecture / topology diagram).

Completion Criteria:	
These Deliverables will be complete when the Vendor has conducted all the design specification workshops, submitted listed Deliverables and the draft Design Specifications document are accepted by the AE Project Manager per the Deliverable Acceptance Procedure:	
Deliverables:	
Deliverable 10	Draft Design Specification document
Deliverable 11	Draft Integration / Migration Plan document
Deliverable 12	Draft Deployment Plan document
Deliverable 13	Updated Discovery / Gap Definition document, as necessary
Deliverable 14	Updated architecture / topology diagram
Deliverable 15	Approved project schedule with AE approved baseline
Deliverable 16	Updated WBS and WBS dictionary pages
Deliverable 17	Summary of workshops, key decisions, and matrix of activities, tasks and durations for all key areas of work.

11.5.3.5 Project Development Phase

R[5] The configurations to the new system and workflow shall be completed as defined within the previously developed and accepted draft Design Specifications document. In this activity, the Vendor shall perform Services which consist of the following tasks:

R[5.A] Review architecture diagram to ensure integration points plus the security to-be implemented are accurate. Determine if integration points and / or security will need to be changed for the new users. Make appropriate modifications and document them.

R[5.B] Deploy software in AE development environment base configurations on the Design Specifications document, database configuration and domains in order to accommodate the new system plus required data and integration from any sub-systems.

R[5.C] Develop the required workflows identified in the design workshops as requirements. Documentation and unit testing are also included.

R[5.D] Report development for new reports defined during the design phase.

R[5.E] Develop any data migration scripts required for the data from sub-systems to be used.

R[5.F] Update the Design Specifications document to reflect updated configuration modifications within three business days.

R[5.G] Conduct FAT (Factory Acceptance Testing) based on draft Design Specifications document with the support of AE subject matter experts.

R[5.H] Migrate, install and configure required system integrations based on the draft Design Specifications document.

Completion Criteria:	
These Deliverables will be complete when the Vendor has completed FAT, submitted listed Deliverable Materials to and obtained Acceptance from the AE Project Manager and they are accepted per the Deliverable Acceptance Procedure by the AE PM:	
Deliverables:	
Deliverable 18	Updated Design Specification document, as necessary
Deliverable 19	Updated Integration / Migration Plan document, as necessary
Deliverable 20	Updated Deployment Plan document, as necessary
Deliverable 21	Final Discovery / Gap Definition document
Deliverable 22	ADMS-SCADA report templates
Deliverable 23	Updated / Approved Project Schedule

Deliverable 24	Updated WBS and WBS dictionary pages
Deliverable 25	Final SAT Plan document
Deliverable 26	Final SAT Defect Tracking Plan document
Deliverable 27	Final SAT Scenarios with Traceability Matrix
Deliverable 28	Provide, install, and properly configure the ADMS-SCADA software and interfaces in AE's Development Environment.

11.5.3.6 Project Test & Deployment Phase

R[1] The objective of this activity is to assist AE Technical staff with SAT and deployment of the ADMS-SCADA solution into AE's production environment. For testing, the scenarios will cover several different tests. Integration test ensures that the interfaces with the software function as specified, the data is mapping correct, the interface(s) are compiled, installed and configured accurately, and protocols are correct. The SAT Plan document is a key deliverable as it will provide instructions to AE for the complete testing of the new system. SAT / User acceptance testing shall be conducted by AE with on-site support from the Vendor. At the completion of this phase the Vendor will provide the final Design Specifications document. In this activity the Vendor shall perform services that consist of the following tasks:

R[1.A] Conduct user training for the AE test team.

R[1.B] Conduct user training for AE personnel.

R[1.C] Assist in the organization and management of test events based on the SAT (Site Acceptance Testing) Plan document.

R[1.D] Assist AE technical staff with the test environment deployment and SAT

R[1.E] Assist AE Technical staff with the deployment of the ADMS-SCADA solution into AE's production environment.

R[1.F] Assist AE while they execute the Deployment Plan in the production environment.

The Vendor is to provide onsite personnel for the 5 business days prior to go live to ensure the readiness of the production environment and prior to executing the Deployment Plan.

Completion Criteria:	
These Deliverables will be complete the first day of production go-live after AE has completed SAT and the Vendor has submitted the listed Deliverable Materials to and obtained Acceptance from the AE Project Manager and they are accepted per the Deliverable Acceptance Procedure by the AE PM:	
Deliverables:	
Deliverable 29	Final Design Specification document, as necessary.
Deliverable 30	Final Integration / Migration Plan document, as necessary.
Deliverable 31	Final Deployment Plan document, as necessary.
Deliverable 32	Final Discovery / Gap Definition document.
Deliverable 33	User training for AE test team.
Deliverable 34	User training for AE personnel.
Deliverable 35	SAT results and resolutions to defects found.
Deliverable 36	Support AE staff with installation and configuration of the ADMS-SCADA software and interfaces in AE's Test Environment.
Deliverable 37	Support AE staff with installation and configuration of the ADMS-SCADA software and interfaces in AE's Production Environment

11.5.3.7 Project Stabilization Phase

R[1] The Vendor shall provide onsite support to AE during post go live to address and correct any anomalies that may occur based on production data or events occurring in the production environment.

R[2] The Vendor will diagnose, document and rectify issues found in the production deployment of the software as part of this scope of work.

R[3] To ensure all environments (dev, test, prod) are equivalent, any issues to be resolved will follow the development, test, production implementation cycle.

R[4] The Vendor shall provide onsite resource(s) in support of the onsite portion of this activity for a minimum of five business days after go-live.

R[5] The Vendor will provide offsite post go-live support and problem resolution for a period of 365 calendar days immediately after onsite support portion ends with the objective of the following response guidelines:

R[5.A] Provide same day acknowledgement upon notification of issues.

R[5.B] Diagnose problem within 24 hours of notification.

R[5.C] Provide problem resolution within 48 hours after diagnosis.

R[5.D] For the offsite portion of the post go-live support, the AE Project Manager will record the offsite support requests, prioritize them and notify the Vendor.

Completion Criteria:	
This activity will be complete when the post implementation period defined has elapsed.	
Deliverables:	
None	

11.6 Project Assumptions

R[1] Upon the completion of project, software will be fully functioning and work as advertised.

R[2] Contract scope will include a Development Environment, Test Environment, Backup and Production Environment.

R[3] The Vendor will adhere to AE's security requirements, including cyber and physical.

R[4] In the event that AE believes the Vendor has not provided a qualified resource for the defined in the SOW, AE will immediately notify the Vendor PM and executives about this issue by email. At that point, the Vendor PM will instruct the resource to immediately cease work on their assigned task(s). The Vendor PM will resolve to AE's satisfaction, including the replacement of Vendor PM.

R[5] The Vendor and AE will work together to finalize a project schedule including assigned resources required from both AE and Vendor.

R[6] The Vendor will have the responsibility for drafting, developing, delivering and managing the project schedule. Vendor and AE executives will be required to approve deviations from the approved project schedule baseline.

R[7] Both Vendor and AE recognize that the Vendor and/or AE resources may be unable to continue to perform services due to illness, resignation, or other cause beyond reasonable control. The Vendor shall notify AE of an emergency discontinuance of assigned personnel and when a suitable replacement will be provided. AE shall have the right to an on-site interview of the replacement and may reject any replacement personnel before they begin work on services.

R[8] The Vendor will provide AE with training requirements, including all needed training documentation, 30 business days prior to on-site training classes. These requirements will be provided such that AE has enough time to setup for the class. All training classes will be shown on the approved project schedule so that all parties know when training classes will occur. The training schedule must remain in synch with the approved project schedule at all times.

R[9] Training will be led instructors who are experienced classroom trainers with knowledge of the ADMS-SCADA.

R[10] The Vendor will designate a PM who will work with AE's PM from the project initiation through project closeout.

R[11] The Vendor PM will provide weekly status reports to the AE PM.

R[12] The Vendor PM will communicate to the AE PM on a weekly basis any risks or issues that arise during the execution of this engagement and that may impact the critical path and project completion date.

R[13] The Vendor will provide AE with all applicable pre-engagement worksheet(s) or questionnaires in a timely manner so that AE is able to complete and return documents per approved project schedule.

R[14] The Vendor will verify that AE has all required supporting system hardware and software resources installed at the required configuration and release level prior to installation, the Vendor is responsible for development of network / system topology diagrams.

R[15] AE has made a good faith effort in identifying tasks and deliverables required to execute this implementation. As the industry expert, the Vendor is responsible for reviewing, identifying and disclosing to AE in writing all known issues, risks, incompatibilities, et cetera, in advance of both parties executing a signed scope / agreement.

11.7 Fees

R[1] Maintenance and support costs shall be paid only for User Account licenses in actual use in the production environment at the annual renewal time and only upon a Fully Operational go-live of each module.

R[2] User Accounts and licenses are fully transferable from one user to another at no additional cost to the City of Austin.

R[3] The User Account fee will include costs for all licensed software provided by Successful Proposer (e.g., third-party, bolt-on, middleware, open-source, integration) and includes all functionalities provided by Successful Proposer.

R[4] During implementation, testing, training, validation and integration, Successful Proposer will provide, at no additional cost to the City of Austin, sufficient numbers of and proper User Account licenses and access to enable the team to achieve a successful “go-live” into production.

R[5] A ten percent (10%) increase in the number of subscribed to User Accounts is allowed without immediate change in fee, based on the current User Account total. If the User Accounts exceeds the subscribed to number identified by the City of Austin, a proper invoice for the overage will be submitted by Successful Proposer and prorated by the product of a fixed User Account fee *times* the number of User Accounts for the remainder of the then current term. The new User Account number then becomes the new baseline. The City of Austin will notify the Successful Proposer in advance of special events and the City of Austin will not be charged User Account or maintenance and support fees for the short-term increase in User Accounts. Additionally, there shall be no User Account or maintenance and support fees for seasonal (e.g., summer) hires. Maintenance and support fee shall be prorated to account for the increase number of User Accounts.

R[6] The City of Austin shall incur no additional license or User Account costs associated with the implementation or change in archival, disaster recovery, business continuity, use of virtual or parallel processing capabilities, clustered hardware/software/databases or failover systems.

R[7] Prior to all Successful Proposer requests for all fee increases, the Successful Proposer shall provide, at least 90 business days in advance of requested increase, to the City of Austin for approval a list of increased service levels that necessitated a fee increase.

R[8] User Account fee will not be charged for users of current and future City-owned software systems that have been, or will be, integrated to the Licensed System.

R[9] User Account fees will be based on Production System use only and will include use in Training, Development, Test environments at no additional cost to the City of Austin. Additionally, all Training, Development and Test accounts will not be considered additional licenses.

Table of Contents

12. Cyber Security 12-1
12.1 Security Network Architecture 12-1
12.2 Critical Infrastructure Protection 12-3
12.3 NERC CIP Standards 12-4
12.4 Scrubbing and Removal of All Unused Services, Accounts, and Data 12-5
12.5 Changes to File System and Operating System Permissions 12-6
12.6 Hardware Configuration 12-7
12.7 Software Updates and Virus Scan 12-7
12.8 Free of “Electronic Self-Help” Enabled Software 12-7
12.9 Detection of Unauthorized Modifications to Software 12-8
12.10 Anti-Virus and Malware Detection Software 12-8
12.11 Security Monitoring 12-8
12.12 Generic and Default Accounts 12-11
12.13 User Authentication 12-11
12.13.1 Access Security Management 12-12
12.14 Appropriate Use Banner 12-13
12.15 Secure Maintenance Access 12-13
12.16 Authorization Process 12-14
12.17 Authentication Methods and Password Construction 12-14
12.18 Security of Remote Access for Maintenance by Vendor 12-15
12.19 Web-Based Interfaces 12-16
12.20 Installation of Third-Party Security Patches (Reference Terms & Conditions) 12-17
12.21 Obligation for Notification of Security Vulnerabilities in Vendor-Provided Software (Reference Terms & Conditions) 12-18
12.22 Disposition of Sensitive Information 12-19
12.23 Cyber Security Audit 12-20
12.24 Site Cyber Security Audit 12-21
12.25 Project Security Initiatives 12-21
12.25.1 Project Security Documentation 12-22
12.25.2 Security Preparation 12-22
12.26 General Security Considerations 12-22
12.26.1 Security Management Controls 12-23

Table of Contents

12.26.2 Personnel and Training 12-24
12.26.3 Electronic Security and Incident Reporting 12-25
12.26.4 Physical Security and Incident Reporting 12-26
12.26.5 Systems Security Management 12-27
12.26.6 Recovery Plans for Critical Assets 12-27

12. Cyber Security

12.1 Security Network Architecture

R[1] Each of the ADMS-SCADA sub-systems supplied (ECS Prod 1 &2, PDS, QAS, and OTS) by the selected Vendor shall reside within clearly defined electronic security perimeters.

R[1.A] All systems, networks, and equipment located within the electronic security perimeter (ESP), as well as the equipment that defines the security perimeter shall be treated and configured as Critical Cyber Assets.

R[1.B] All servers located within the ESP will be individually firewalled.

R[1.C] The primary access points through this perimeter shall be AE-provided Firewalls.

R[1.D] The secondary access points through the perimeter shall be the RTU Front-End Processors for non-IP communications circuits, which act as AE access points for RTUs and the ICCP servers.

R[1.E] Where technically feasible, communications shall be designed so that the most privileged application shall initiate communications.

R[1.E.i] Upon failed communications, the most privileged side shall restart communications.

R[1.E.ii] Except for certain control schemes, the master network device shall initiate communications.

R[1.F] All other access points, such as support modems shall be secured or normally disabled such that overt authorized manual intervention is required to enable them.

R[2] The Vendor shall provide documents and drawings depicting all interconnected ADMS-SCADA components all access points and all assets deployed or configured for controlling and monitoring access to the defined access points.

R[3] The Vendor shall limit required port access to a minimum and provide a list of all required ports, services and addresses requiring access through any and all Firewalls that support normal, emergency and ongoing maintenance functions.

R[4] As directed by AE, the Vendor shall provide assistance to AE in helping to determine the minimum required access permissions for the firewalls that allow a functional, yet secure, operation of the ADMS-SCADA, including normal, emergency and required ongoing maintenance actions.

R[5] Where external access into the electronic security perimeter is implemented, strong technical controls are required to ensure the authenticity of the accessing party.

R[6] Strong technical controls, in the context of this Specification, include authentication methods that augment static user names and passwords, such as two-factor authentication or any authentication method employing one-time or randomly changing passwords.

R[7] AE shall provide all information needed to interface to the ADMS-SCADA Vendor's two–factor authentication system.

R[8] Where applicable, and/or requested by AE, the Vendor shall propose additional network security architectures, including "DMZ" networks and associated systems, to provide external users access to data without impacting the performance, reliability or security of the ADMS-SCADA or its component systems.

R[9] Where DMZ networks are proposed, the network configurations shall be implemented to maximize the security of the ADMS-SCADA networks, while facilitating access to data resources located in the DMZ.

R[10] All routers supplied by AE shall be configured to generate log entries on attempted connection attempts, any successful connections and denied logins, and "enable" logins and successful unauthorized access and shall include Firewall IOS software.

R[11] All access permissions implemented during system development, factory test and site test shall be documented and reviewed for removal prior to system commissioning.

R[12] The Vendor shall submit to AE a written certification attesting that all access privileges have been scrubbed.

R[13] The electronic security perimeter shall, at a minimum, have the following characteristics:

R[13.A] No direct connection from the Internet to the ADMS-SCADA networks, and vice versa.

R[13.B] The Corporate network shall not have direct query or access capability to any data stores or processes within the ADMS-SCADA.

R[13.C] Well-defined rules outlining required and authorized traffic must be implemented at all access points.

R[13.D] Management of access control devices must be permitted only from a highly restricted subset of management devices.

R[14] The Vendor shall work with AE to establish the capability to record all network traffic, including heartbeat signals, for the purpose of detecting unauthorized activity, unusual activity, and attempts to defeat the security capabilities of the ADMS-SCADA or its electronic security perimeter.

R[15] AE will work with Vendor to document and analyze the process for determining "normal" network traffic, including all heartbeat signals.

R[16] Vendor will provide a document describing each port used in each unit.

R[17] AE, with Vendor's support, can use this document to establish rules for its Network Intrusion Detection Scanners (NIDS).

12.2 Critical Infrastructure Protection

R[1] The Vendor must base its security considerations and requirements on the requirements of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.

R[2] The Vendor must comply with AE's data security policies and procedures supplied herein.

R[3] All security functions required by this Specification must be implemented in a non-interfering manner, such that authorized and legitimate use of the ADMS-SCADA is not hampered, nor is the ability to perform required functions impeded by the security features.

12.3 NERC CIP Standards

R[1] The ECS (Prod 1 and Prod 2), PDS, QAS, and OTS, and all equipment, workstations, software and systems proposed and ultimately supplied with these component systems could be considered Critical Cyber Assets as defined by NERC Standard CIP-002 for the purposes of the ADMS-SCADA and this contract.

R[2] During the project implementation, AE will notify Vendor of the levels of security required for each of the above systems and which items will be considered part of AE's ESP for NERC CIP requirements.

R[3] The current CIP standards promulgated by NERC include:

R[3.A] CIP-002-3 Critical Cyber Asset Identification.

R[3.B] CIP-003-3 Security Management Controls.

R[3.C] CIP-004-3 Personnel & Training.

R[3.D] CIP-005-3 Electronic Security Perimeter(s).

R[3.E] CIP-006-3 Physical Security.

R[3.F] CIP-007-3 Systems Security Management.

R[3.G] CIP-008-3 Incident Reporting and Response Planning

R[3.H] CIP-009-3 Recovery Plan for Critical Cyber Assets.

R[4] The Vendor shall ensure compliance with the current versions of these standards at time of the ADMS-SCADA delivery.

R[5] The Vendor will provide suggested enhancements to the ADMS-SCADA LAN to meet these standards.

12.4 Scrubbing and Removal of All Unused Services, Accounts, and Data

R[1] Vendor shall provide a listing of services required for any computer system running ADMS-SCADA system applications or required to interface the ADMS-SCADA system applications.

R[2] The listing shall include all ports and services required for normal operation as well as any other ports and services required for emergency operation.

R[3] The listing shall also include an explanation or cross reference to justify why each service is necessary for operation.

R[4] All applications, utilities, system services, scripts, configuration files, databases, user accounts and all other software not required for operation of the ADMS-SCADA shall be removed prior to commissioning.

R[5] Additional security preparation tasks are described in Section 12.25.2.

R[6] The items to be removed (where technically feasible) or disabled shall specifically include, but not be limited to:

R[6.A] Games

R[6.B] Device drivers for devices not delivered.

R[6.C] Servers and clients for unused Internet services.

R[6.D] All software compilers except for the PDS.

R[6.E] Software compilers for languages that are not used in the ADMS-SCADA.

R[6.F] Unused administrative utilities, diagnostics, network management, and system management functions.

R[6.G] Backups of files, databases, and programs, used during system development.

R[6.H] Databases, configuration files, and other files used for development and testing.

R[6.I] Programs and scripts used for development and testing, including sample programs and scripts (exception PDS/QAS to be determined during project implementation).

R[6.J] Help systems not directly supporting ADMS-SCADA applications.

R[7] The Vendor shall also perform the following:

R[7.A] Additional “hardening”, particularly following established methods and guidelines, including, but not limited to those developed by the original software Vendor, the US Government National Institute of Standards and Technology, the US Government Department of Defense, the US Government Department of Energy, or similar recognized organizations shall be performed by the Vendor as part of the software installation and configuration activities.

R[7.B] The Vendor shall document and submit documentation that the foregoing has been completed.

R[7.C] The Vendor shall use the best possible means to scrub, or otherwise destroy beyond recovery all electronic Confidential Information in its possession, certifying such destruction in writing to AE, and providing AE a written explanation of the method(s) used for data disposal/destruction, along with a written certification that such method meets or exceeds AE’s data handling standards and industry best practices for the disposal/destruction of sensitive data.

12.5 Changes to File System and Operating System Permissions

R[1] Vendor shall configure hosts with least-privilege file and account access and provide documentation noting all file systems and access rights, and all System and User Account Privileges and access rights.

R[2] Vendor shall configure the necessary system services to execute at the least-user privilege level possible for that service and provide documentation of the configuration.

R[3] Vendor shall document that changing or disabling access to such files and functions has been completed.

12.6 Hardware Configuration

R[1] Vendor shall provide a written list of all disabled or removed USB ports, CD/DVD drives, and other removable media devices.

R[2] Vendor shall provide the documentation to allow the system administrators the ability to re-enable devices if the devices are disabled by software.

12.7 Software Updates and Virus Scan

R[1] All updates to the operating system and application software addressing cyber security shall be installed as specified in Software Maintenance, prior to installation on the production system.

R[2] All security patches and upgrades to the operating system (including Oracle, third-party products and upgrades provided by Vendor) and application software shall be tested and certified by the Vendor.

R[3] All software shall be scanned for viruses, worms, Trojan horses, and other software contaminants during the factory test and at the start of site testing with a Virus Scanning product approved by AE.

12.8 Free of "Electronic Self-Help" Enabled Software

R[1] The Vendor must state that any ADMS-SCADA software proposed does not contain embedded faults or back-door mechanisms that could allow the software Vendor, or any other party, to remotely disable some or all of the functions of the software, to affect their performance, or in any way to degrade its operation (so-called "electronic self-help" in the terms of the Uniform Computer Information Transactions Act).

R[2] The software shall not contain any mechanism that automatically disables some or all of its functions or degrades their operation on a certain date or upon the occurrence of a specific event.

12.9 Detection of Unauthorized Modifications to Software

R[1] The Vendor shall provide a mechanism for periodically scanning the integrity of the software and database on the ADMS-SCADA disks to determine if unauthorized modifications to the software have been made.

R[1.A] A tool, such as Industrial Defender, or the equivalent, may be used for this function and shall be subject to approval by AE.

R[1.B] The process of making an authorized modification to the software must include an update to the integrity database to ensure that the scanning tool does not detect valid or authorized changes as unauthorized.

R[1.C] The scanning software shall be configurable to run manually or periodically, and shall not impact the performance or operation of the ADMS-SCADA or any application.

12.10 Anti-Virus and Malware Detection Software

R[1] Where technically feasible and where appropriate commercial products exist (e.g., Microsoft Windows and Linux environments), the Vendor shall implement anti-virus, spyware, and other malware detection systems.

R[2] These products shall be installed and running throughout the development, test, commissioning and acceptance of the system to ensure that their performance impact is known and tested.

R[3] These products shall operate in a non-interfering manner.

R[4] The Vendor shall include procedures for the secure updating of configuration and signature files to ensure that the tools remain current with updates and releases and under tight control of AE support staff – not automatic.

12.11 Security Monitoring

R[1] The ADMS-SCADA shall log all access attempts at both the application and electronic security perimeter.

R[2] AE shall provide Vendor the appropriate Network Intrusion Detection System devices and Host Intrusion Detection System agents and require the Vendor to integrate them into their network and security monitoring system.

R[2.A] The ADMS-SCADA shall maintain logs of system events related to cyber security in sufficient detail to create historical audit trails and enable a root-cause analysis for a period of at least 90 calendar days.

R[2.B] Provision shall be given to copy the system event data to an alternate storage medium for storage longer than 90 days, if required as part of a longer-term investigation.

R[2.C] The logs shall be able to capture the following for both human users and application requests:

R[2.C.i] All attempts to log on, both successful and unsuccessful.

R[2.C.ii] Any privilege change requests, both successful and unsuccessful both OS and Application level.

R[2.C.iii] All user actions affecting security, such as changing passwords and level of security on user accounts

R[2.C.iv] All attempts to access files for which the user has no access privileges.

R[2.C.v] Attempts to perform an action not authorized by the security scheme.

R[2.C.vi] Detecting unauthorized access (intrusions), and attempts at unauthorized access at the access points to the electronic security perimeter(s) twenty-four hours a day, seven days a week.

R[2.D] The audit trails and logging files shall be time-stamped, encrypted, and access-controlled.

R[3] For the purposes of the above requirements, the term “user” shall refer both to human users and to applications requesting such actions.

R[4] All access records shall be stored within the ADMS-SCADA on auxiliary memory and shall be able to be copied to AE’s central security logging system.

R[5] The ADMS-SCADA shall include redundant syslog servers to aggregate all of the ADMS-SCADA syslogs.

R[6] AE shall be able to copy the application logs to an AE-provided long-term storage archive facility.

R[7] AE's central security logging service and interface is RSA Envision using syslog and other tools such as SNARE as required.

R[7.A] While the mechanism for this transfer will be determined later, it is envisioned that a mechanism such as "syslog" will be used.

R[7.B] The format of these records shall be consistent with that provided by other log generating devices, such as network routers, firewalls, and intrusion detection systems.

R[7.C] Files that record system activities shall be defined as "append-only". That is, it shall not be possible to delete an entry from a log file once an entry has been made.

R[7.D] The access security recording scheme shall include a feature to archive the record file and to direct the records to a new, empty file.

R[7.E] Record formats shall be compatible with AE's central security logging system.

R[8] The ADMS-SCADA shall either generate an alarm when access activity may be indicative of attempts to obtain unauthorized access to system services or data or provide a mechanism for the receipt of AE selected alarms from a security server.

R[9] Alarms shall also be sent to MSSP (Managed Security Service Provider).

R[10] A simple method shall be provided for the user to view and to change the rules for generating alarms.

R[11] Initially, an alarm shall be generated when the system detects any of following activities:

R[11.A] Repeated attempts from a specific workstation or external port to log in.

R[11.B] Repeated failed attempts at file/system access.

R[11.C] Port scans (attempts to access closed ports or services).

R[11.D] Unusual levels of traffic on the local area network.

R[11.E] Account lock-out for application accounts.

12.12 Generic and Default Accounts

R[1] The Vendor shall disable or remove, as technically feasible, all generic accounts, guest accounts, development accounts, maintenance accounts, and default accounts provided by hardware, operating system, database, application program, and other Vendors.

R[2] The Vendor shall provide written notification to AE stating that the generic accounts have been removed.

R[3] Where specific accounts cannot be removed, they shall be renamed or disabled to prevent unauthorized access and the Vendor shall provide written notification to AE stating the accounts that must remain and reason they cannot be removed.

R[4] Where technically feasible, all actions to be performed by shared or elevated-privilege accounts shall be initiated using a specifically named individual user account, followed by a “switch-user” function to the shared or generic account to perform a necessary or required function.

R[5] This action provides both authentication of a specifically named, valid user, as well as an audit trail of any elevated privilege actions performed.

R[6] If not technically feasible to do so, the Vendor shall provide written notification to AE for reasons why and specified mitigation measures.

12.13 User Authentication

R[1] A mechanism for defining and controlling user access to the operating system environment of the ADMS-SCADA shall be provided (Section 12.13.1). Operating System Administrative users will typically have access to all system functionality, whereas other/generic users may only have limited capabilities.

R[2] Operating System Administrative users shall have the authority to assign and define the different classes of users and their default class for login.

R[3] The ADMS-SCADA must support account management methods to enforce access authentication and accountability of user activity, and to minimize the risk of unauthorized access with the least privileged principle followed.

R[4] The ADMS-SCADA and the underlying operating system must support the requirement that users have individual accounts, without compromising the functionality and operating restrictions with the least privileged principle followed.

R[5] For implementations where individual computer nodes maintain their own unique internal user identification codes (e.g., UID numbers on UNIX nodes), the same named user shall use the same internal user identification code for all nodes within the ADMS-SCADA.

R[6] User credentials must not be transmitted in clear text.

12.13.1 Access Security Management

R[1] The cyber security controls shall be applied across all ADMS-SCADA applications and services and security shall be managed as a single service for all component systems of the ADMS-SCADA, including the ECS (Prod 1 and 2), PDS, and QAS.

R[2] The ADMS-SCADA shall record all attempts to access the ADMS-SCADA with all pertinent information (e.g., IP address, workstation identifier) both at the application level and at the “infrastructure” (operating system and application support software) level including:

R[2.A] All attempts to log on, whether successful or unsuccessful. A user shall be allowed to login at multiple workstation locations simultaneously

R[2.B] All changes to privileges assigned to users .

R[2.C] All user actions affecting security, such as changing passwords.

R[2.D] Attempts to access a file for which the user has no access privileges.

R[2.E] Attempts to perform an action not authorized by the security scheme

R[3] The ADMS-SCADA shall generate an alarm when access activity may be indicative of attempts to obtain unauthorized access to system services or data.

R[4] A simple method shall be provided for the user to view and to change the rules for generating alarms.

R[5] Initially, an alarm shall be generated when the system detects any of the following activities:

R[5.A] Repeated attempts to log in from a specific workstation or external port.

R[5.A.i] Multiple unsuccessful attempts to login shall be detected and the ADMS-SCADA shall include a configurable option to lock out a user when this is detected.

R[5.B] Repeated failed attempts at file access.

R[5.C] Port scans (attempts to access closed ports or services).

R[5.D] Unusual levels of traffic on the local area network.

R[6] The delivered ADMS-SCADA shall not include any guest accounts or default administrator or maintenance accounts.

R[7] All accounts shall require an interactive login.

R[8] The login for Operators shall prevent access to operating systems in all UNIX-based servers.

R[9] For Windows-based processors, the Operators shall not be able to modify the UI environment and associated directories.

12.14 Appropriate Use Banner

R[1] Users accessing the ADMS-SCADA through interactive or maintenance access shall be presented with an “Appropriate Use Banner”, the contents of which will be provided by AE.

12.15 Secure Maintenance Access

R[1] The Vendor shall demonstrate and shall maintain a secure maintenance access to the operating environment for both remote and local users.

R[1.A] The access shall provide authentication of valid users without transmitting plain-text passwords on the network.

R[1.B] An encrypted access mechanism such as ssh shall be used for "command line" access to POSIX nodes.

R[1.C] Secure file copy features included in ssh shall be used to manually transmit files between nodes when using the network.

12.16 Authorization Process

R[1] The Vendor shall maintain lists of all authorized personnel with access to AE's ADMS-SCADA while on site at the development site, including their specific electronic and physical rights to the systems, servers, or databases, and a date for which access will be terminated.

R[2] All access shall be reviewed yearly.

R[3] The selection of authorized personnel shall comply with the requirements in 12.26.2, Personnel and Training, and AE shall be informed in writing of all changes to the list.

12.17 Authentication Methods and Password Construction

R[1] Single-factor authentication is required for workstations within the physical security perimeter(s).

R[2] All accounts in the delivered ADMS-SCADA shall be configurable to require two-factor authentication of users.

R[3] One factor is expected to be a password assigned by AE. Both biometric recognition devices and tokens shall be supported as the second authentication factor, selectable at a later time by AE.

R[4] Passwords for maintenance access shall comply with AE security policy, to be provided to the Vendor.

R[5] A combination of upper- and lower-case alphabetic, numeric and special characters shall be used.

R[6] The minimum password length shall be configurable by AE, and initially set to 8 characters with a maximum of 32 characters allowed.

R[7] All accounts providing interactive or network access shall have passwords.

R[8] There shall be a limit of a configurable number of attempts allowed until the user is locked out.

R[9] Accounts that exist strictly for identification and ownership purposes shall be disabled from all interactive, networks, or other access.

R[10] The Vendor shall provide a mechanism to temporarily disable access and security authentication policies for individual users during emergency system recovery or other abnormal operations, where system availability would be negatively impacted by normal security procedures.

R[11] AE shall have review and approval rights for these “bypass” procedures. This rollback operation shall be logged in the system for reference purposes.

12.18 Security of Remote Access for Maintenance by Vendor

R[1] All access from Vendor’s facilities or Vendor’s staff to AE’s ADMS-SCADA will be controlled by AE.

R[2] Access will be provided for the purpose of maintenance shall be permitted on an as-needed basis only to the Program Development System (PDS) or to the Quality Assurance System (QAS), and not to any component of the on-line ADMS-SCADA.

R[3] In emergency situations, Vendors may be allowed access to the on-line system(s) only when authorized and initiated by AE.

R[4] Such access shall be subject to the security requirements for remote maintenance access as described in Section 2.1.6.4, Remote Maintenance Access.

R[5] All actions performed remotely shall be subject to audit-trail reporting and adhere to AE’s software version and configuration control procedures.

R[6] The Vendor's diagnostic system used for remote maintenance of AE's ADMS-SCADA is referred to here as the "Vendor's remote diagnostic system".

R[6.A] The Vendor shall ensure security of the physical access to Vendor's remote diagnostic system.

R[6.B] The Vendor's remote diagnostic system shall be a stand-alone system, and shall not be connected to any Vendor or external network without explicit, written authorization from AE.

R[6.C] The Vendor shall enforce strict physical and electronic security procedures for access to the Vendor's remote diagnostic system, such as having the system in a secure area and requiring a smart card or biometric identification as well as a password to gain access to the Vendor's remote communications line.

R[6.D] Upon termination of the maintenance contract, the Vendor's remote diagnostic system shall be dismantled, and all paper and electronic media shall be securely erased or destroyed as described in Section 12.26.5, Systems Security Management.

R[6.E] A certificate of erasure or destruction shall be provided as part of the contract termination documentation.

12.19 Web-Based Interfaces

R[1] Vendor shall remove or disable all software components and services that are not required for the operation and maintenance of the devices that run an HTTP server.

R[2] Vendor shall provide documentation on what is removed and/or disabled.

R[3] Vendor shall provide, within a negotiated period (pending the severity and risk of the vulnerability), appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

R[4] Vendor shall provide documentation on the actual process used for verification and validation of Web-based interface software.

R[5] Vendor shall follow secure coding practices and reporting for all Web-based interface software.

R[6] This requirement includes both Web applications and Web servers. Based on risk analysis, the Web applications must be protected using best practices.

12.20 Installation of Third-Party Security Patches (Reference Terms & Conditions)

R[1] Whenever the ADMS-SCADA Vendor and suppliers of software to the ADMS-SCADA Vendor, release a software change (“upgrade”, “update”, “modification”, “release”, or “patch”) to correct a security-related error in the code or to close a vulnerability, the Vendor shall take immediate steps to test, confirm, and deliver to AE a patch to install the software change on the ADMS-SCADA.

R[1.A] The Vendor shall review security patches daily after release by the third-party vendor.

R[1.B] The Vendor shall provide to AE, in a secure manner, a report that states the impact of the patches on the Vendor’s baseline software in 7 days.

R[1.B.i] The Vendor shall complete testing of the applicable security patches within 30 days.

R[1.C] The initial testing for AE’s ADMS-SCADA software configuration shall be done in an environment that is operationally similar to that of the ADMS-SCADA (e.g., the QAS).

R[1.C.i] Testing shall have the goal of confirming that the patch indeed does not introduce any new errors and does not interfere with the Vendor-supplied software.

R[1.C.ii] The security patch shall be tested and sent to AE by the Vendor in a secure fashion within the 30-day period.

R[1.D] AE will test the patches on the QAS to simulate an operational environment.

R[1.E] The implementation and testing of all security patches shall follow the established configuration management and change control processes.

R[1.E.i] This includes the execution of test procedures where the change is deemed “significant”.

R[1.F] If during testing on the QAS at AE, a patch is found to interfere with the operation of the ADMS-SCADA software, AE will notify the Vendor and the Vendor shall initiate the resolution process with the third-party vendor.

R[2] The ADMS-SCADA shall include a Vendor-supplied facility to enable AE to receive, test, install and distribute security patches throughout the system components.

R[2.A] This facility shall be located in a DMZ to protect the ADMS-SCADA and shall provide all hardware and software required to accurately manage the patch process.

12.21 Obligation for Notification of Security Vulnerabilities in Vendor-Provided Software (Reference Terms & Conditions)

R[1] The Vendor shall within 48 hours inform AE in a secure manner the discovery of an error in or a property of any software resident on the ADMS-SCADA that makes the ADMS-SCADA vulnerable to cyber-intrusion.

R[2] Vendor shall have a patch management and update process.

R[3] Vendor shall provide details on their patch management and update process during project implementation shortly after Contract award.

R[4] Responsibility for installation and update of patches shall be identified.

R[5] Post-contract award, Vendor shall provide notification of known vulnerabilities affecting Vendor-supplied or required OS, application, and third-party software within the 48-hour period after public disclosure.

R[6] Post-contract award, Vendor shall provide notification of patch(s) affecting security as identified in the patch management process.

R[7] Vendor shall apply, test, and validate the appropriate updates and/or workarounds on a baseline reference system before distribution.

R[8] Vendor shall provide within a negotiated period (pending the severity and risk of the vulnerability) appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

R[9] The Vendor shall diligently work to correct the error or modify the property to close the vulnerability, and shall make the correction fully tested and available to AE at no cost and must be corrected to AE's satisfaction.

R[10] This obligation for notification and the closure of security-related vulnerabilities shall remain during warranty and as long as a Service Agreement is in place.

R[11] After warranty, but without a Service Agreement, Vendor shall notify AE of security-related vulnerabilities.

R[12] Closure of security-related vulnerabilities in the absence of a Service Agreement will be handled on an individual contract basis.

R[13] The Vendor shall provide AE with a process to submit problem reports to be included in the system security process.

R[14] Submitted reports shall be reviewed and an initial action plan generated within two business days of submittal.

R[15] Vendor shall protect problem reports of a security nature from public disclosure and when notifying other customers shall not release any information to indicate that AE identified the problem.

R[16] Vendor shall verify and provide documentation that all services are patched to current status.

12.22 Disposition of Sensitive Information

R[1] Any documentation or other material replaced during maintenance shall be disposed in such a manner as to protect sensitive information, as described in Section 12.26.5, Systems Security Management.

R[2] This includes maintenance actions performed on the ADMS-SCADA, as well as the Vendor's remote diagnostic system.

12.23 Cyber Security Audit

R[1] The Vendor shall perform a cyber security audit with AE witnessing the audit.

R[2] The cyber security audit shall verify that the requirements of Sections 12.1 through 12.17, and 9.9.6 and others have been satisfied.

R[3] As a minimum, the following cyber security requirements shall be specifically tested, verified, and reviewed:

R[3.A] Permissions and configurations shall be reviewed to ensure that the deliverable configuration is accurately documented.

R[3.A.i] These final configuration documents will be the basis for the annual Cyber Vulnerability Assessment review required by the NERC standards.

R[3.B] Verify that network traffic recording and access recording have been enabled and are functioning.

R[3.C] Verify that unused services have been removed.

R[3.D] Verify that unused ports have been disabled.

R[3.E] Verify that all software has been updated with all applicable security patches released within 30 days of the date of the audit.

R[3.F] Perform a virus and malware scan of the system and verify that all virus and malware scanning tools are enabled.

R[3.G] Verify that all "electronic self-help" software has been removed.

R[3.H] Regenerate all signature files and other data used by the software integrity scheme.

R[3.I] Remove all generic and default accounts where appropriate.

R[3.I.i] The Vendor shall document any exceptions and the reason for any exceptions for AE approval.

R[3.J] Verify that all access authorization methods are properly configured.

R[3.K] Verify that all electronic access points (e.g., routers and switches) are properly configured.

R[3.L] Review the currency of cyber security training and background checks for all Vendor and SubContractor staff to be sent to the field and all staff remaining at the Vendor's facility who will access or work on the ADMS-SCADA.

R[3.M] Generate a full backup of software and databases (Section 9). Demonstrate a cyber security recovery plan for each type of installed server on the ADMS-SCADA and a sample of the workstations.

R[3.M.i] The demonstration shall be performed in parallel with FAT testing. (Section 9.9.6).

R[3.N] Demonstration of the Vendor's workstation hardening procedure.

12.24 Site Cyber Security Audit

R[1] The site cyber security audit shall repeat the audit performed during factory testing (refer to Section 12.23).

R[2] AE reserves the right to perform a post-shipment vulnerability assessment with AE or subcontractor staff as part of the Site Cyber Security Audit.

12.25 Project Security Initiatives

R[1] The Vendor shall be responsible for ensuring that its staff complies with all required security requirements and provisions for the life of the project.

R[2] For any software developed specifically for this project, the Vendor shall notify AE if that software development is being outsourced to a third party. AE shall have approval over any third party to which such development is outsourced.

12.25.1 Project Security Documentation

R[1] The Vendor shall produce documentation describing all physical, procedural, personnel, or other security measures that are necessary to protect the confidentiality and integrity of data in the supplied system, and to protect the reliability of the ADMS-SCADA process.

12.25.2 Security Preparation

R[1] Prior to the commissioning of the system, the Vendor shall remove any software, configurations or user accounts used during the development and testing of the system, but not required for ongoing normal, emergency or maintenance activities of the system (reference Section 12.4 and Section 12.5).

R[2] All updates to operating system and application software addressing cyber security issues shall be installed prior to system commissioning.

R[3] A complete and thorough scan by anti-virus software and file integrity monitoring tools shall be performed during the factory test, and again prior to the start of the site acceptance testing.

R[4] Software shall immediately be placed under source code control after scanning.

R[5] The Vendor and AE shall review the permissions and configurations of the system (including use of default accounts, access permissions, and network configurations) to ensure that the final configurations are accurately documented, and appropriate permissions are implemented.

R[6] These final configuration documents will be the basis for the annual Cyber Vulnerability Assessment review required by the NERC standards.

12.26 General Security Considerations

R[1] The following sections describe the non-technical security requirements required of the Vendor.

R[1] These security requirements are in addition to the technical security requirements described elsewhere in this specification.

R[2] These security requirements are based on the requirements described in NERC Standards CIP-003 through CIP-009.

12.26.1 Security Management Controls

R[1] AE shall supply the Vendor with a copy of AE's Security Policy and Procedure for review.

R[2] The Vendor shall review and accept the applicable sections of the policy and procedure. Vendor staff shall follow all applicable requirements of AE's Security Policy while on site at an AE location.

R[3] AE shall identify the classification of the information, as described in AE's Security Policy, for all information supplied to the Vendor.

R[4] The Vendor shall establish and comply with a policy that identifies access limitations to sensitive information related to the ADMS-SCADA, as well as information about AE's electrical system.

R[5] As a minimum, this document must address access to procedures, critical asset inventories, maps, one-line diagrams, floor plans, equipment lists and layouts, configurations, databases, and application software.

R[5.A] The document shall identify measures that provide both electronic and physical protection for the sensitive information.

R[5.B] When the Vendor no longer needs the information, all copies shall be returned to AE, or destroyed as specified by AE.

R[6] AE and Vendor shall protect all data transmitted between the Vendor's site and AE's site, and shall jointly determine the methods required to securely transmit any data required for this project.

R[7] Encryption programs with email integration, such as PGP shall be sufficient.

R[8] The Vendor shall provide AE a documented procedure for accessing AE's system while located at the Vendor's site.

R[9] This process shall include an approval and review process to ensure that only authorized personnel (i.e., Vendor staff, sub-contractors, vendors, and contractors) have access to the system and AE information.

R[10] AE may request a review of the procedure and the list of authorized personnel at any reasonable time during the project.

R[11] Logical or electronic access to the systems by Vendor staff shall be limited to that required for the staff to perform their job duties, based on appropriate roles and responsibilities documented as part of the access approval.

R[12] The Vendor shall maintain a list of personnel who are responsible for authorizing access to the ADMS-SCADA, identifying each by name, title, business telephone and the list of systems or application functions for which they are responsible to authorize access.

12.26.2 Personnel and Training

R[1] All Vendor staff with access to AE's system shall be trained in appropriate and applicable security practices. The training material will be provided by AE.

R[2] Alternatively, the Vendor shall provide copies of training materials to AE for review and approval.

R[3] AE may request the addition of specific topics to the vendor's training required for staff with access to AE's system based on its review of the Vendor training materials.

R[4] Training shall be conducted annually, with attendance records furnished to AE.

R[5] These training records shall include the date of training, attendance lists indicating the Vendor staff attendance, and a course syllabus.

R[6] Background screening shall be performed to a degree consistent with the access granted, and in accordance with national, state/provincial and local laws.

R[7] The Vendor shall provide AE with a copy of the process and requirements used in performing background screening.

R[8] The following minimum investigative scope is required:

R[8.A] Employee reference check.

R[8.B] Personal ID verification based upon US Social Security numbers when applicable.

R[8.C] Education/professional affiliation verification

R[8.D] Police clearance verification

R[9] The Vendor shall maintain records of background checks for 5 years, and shall provide evidence of background checks to AE upon demand.

R[10] The Vendor shall communicate any personnel changes to AE, and provide evidence of background checks and proper authorization and training for additions to the project staff.

R[11] Change in assignment shall be communicated to AE within 7 calendar days of the change, or 24 hours if removal for cause.

R[12] The Vendor shall provide quarterly summaries of personnel assigned or authorized for access to AE's system for reconciliation with AE's records.

R[13] AE and the Vendor will jointly investigate inconsistencies.

12.26.3 Electronic Security and Incident Reporting

R[1] The Vendor shall maintain a secure network for development of AE's system, and shall identify the electronic (logical) security provided to AE's systems while under the control of the Vendor, at the Vendor's development site.

R[1.A] This includes a description of the network access control implementations (e.g., firewall rule sets) implemented to limit or restrict unauthorized electronic access to AE's systems, or to information and documentation about AE's ADMS-SCADA or electrical system, and to protect AE's systems from inadvertent and inappropriate use.

R[1.B] Logs of unsuccessful and unauthorized access attempts will be reviewed on at least a next-business day basis to determine if any further action is required.

R[1.C] Summary reports of attempted and unauthorized access attempts shall be made available to AE at least monthly or more often if conditions warrant.

R[1.D] AE shall be notified of all Electronic Security breaches or aggressive attacks of the Vendor's network and systems while AE's systems are at the Vendor's site, regardless of whether they were successful.

R[1.E] The Vendor shall investigate the electronic security breach following established procedure, including applicable or required reporting to required local law enforcement.

R[1.F] AE and Vendor will jointly determine whether the breach will be reported to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), the US Department of Homeland Security National Infrastructure Coordination Center (DHS-NICC), the Federal Bureau of Investigation (FBI), US Secret Service (USSS), for further investigation or tracking.

12.26.4 Physical Security and Incident Reporting

R[1] The Vendor shall identify the physical security provided to AE's systems while under the control of the Vendor, at the Vendor's development site.

R[2] This includes a description of building and floor access controls, controls to the "test floor", and provisions for securing access to AE's systems within the test floor environment.

R[3] The physical security described shall include limiting access to information and documentation about AE's ADMS-SCADA or electrical system, and protect AE's systems from inadvertent and inappropriate use, as well as from damage and theft.

R[4] The Vendor shall provide monitoring and logging of physical access, and provide appropriate records of access to AE upon reasonable request, or for cause.

R[5] AE shall be notified of all physical security breaches targeted at AE's system while at the Vendor's site, regardless of whether they were successful.

R[6] The Vendor shall investigate the physical security breach following established procedure, including applicable or required reporting to required local law enforcement.

R[7] AE and Vendor will jointly determine whether the breach will be reported to the Electricity Sector Information Sharing and Analysis Centre (ES-ISAC), the US Department of Homeland Security National Infrastructure Coordination Centre (DHS-NICC), the Federal Bureau of Investigation (FBI), US Secret Service (USSS), for further investigation or tracking.

12.26.5 Systems Security Management

R[1] Media, such as paper documents and magnetic, electronic, and optical records containing or potentially information classified as sensitive by AE shall be destroyed by the Vendor when no longer needed, or at AE request.

R[2] Paper documents shall be shredded using a crosscut shredder (or equivalent).

R[3] Magnetic media may be re-used, but shall be erased prior to reuse such that retrieval or reconstruction of the data is impossible using reasonable methods of data recovery.

R[4] DVD and CD-ROM disks must be physically destroyed rendering the data completely unreadable.

R[5] The Vendor shall maintain business records of the destruction for inspection by AE.

R[6] Cyber assets containing hard drives may be redeployed within AE's ADMS-SCADA environment following an erasure/format of the hard drive and a reload of the appropriate software or data.

12.26.6 Recovery Plans for Critical Assets

R[1] The Vendor shall provide a comprehensive procedure for the restoration of

R[1.A] core ADMS-SCADA functions

R[1.B] full ADMS-SCADA functionality following a catastrophic failure of the ADMS-SCADA software or hardware.

Table of Contents

13. ADMS-SCADA Functional Requirements 13-1

13.1 Function Priorities 13-3
13.2 Distribution System Operations Model (DSOM) 13-3
13.2.1 ADMS-SCADA User Interface Features 13-6
13.2.1.1 Distribution Circuit Displays 13-6
13.2.1.2 Tabular Displays 13-11
13.2.1.3 ADMS-SCADA Schematic Auto-generation Functionality 13-12
13.2.1.4 Tracing Electrical Connectivity 13-13
13.2.1.5 Jumpers, Cuts, and Grounds 13-14
13.3 ADMS-SCADA Applications 13-14
13.3.1 Distribution Power Flow 13-15
13.3.1.1 Required Characteristics 13-17
13.3.1.2 User Input 13-19
13.3.1.3 Results 13-20
13.3.2 State Estimation 13-21
13.3.3 Switching Order Management 13-22
13.3.3.1 Manual Creation of Switching Orders 13-23
13.3.3.2 Automatic Generation of a Go-Back Order 13-24
13.3.3.3 Automatic Switching Order Creation and Execution 13-25
13.3.3.4 Maintenance of Switching Orders 13-25
13.3.3.5 Switching Order Execution and Checkout 13-26
13.3.4 Safety Tagging 13-27
13.3.4.1 Safety Tag Application 13-27
13.3.4.2 Safety Tag Clearances 13-28
13.3.5 Fault Location Isolation and Service Restoration (FLISR) 13-29
13.3.5.1 General 13-29
13.3.5.2 Required Characteristics 13-31
13.3.6 Distribution Circuit Fault Location 13-33
13.3.7 Integrated Volt/Var Control (IVVC) 13-35

13.3.8 Operations Device Monitoring 13-37
13.3.9 Outage Management/ Restoration Application 13-39
13.3.9.1 General Features 13-39
13.3.9.2 Outage Analysis 13-41
13.3.9.3 Outage Resolution 13-41
13.3.9.3.1 Multiple Outage Levels 13-42
13.3.9.3.2 Partial Restoration 13-42
13.3.9.3.3 Full Restoration 13-43
13.3.9.3.4 Distribution Abnormal Status Detection 13-43
13.3.9.3.5 In-Service Trouble Orders 13-44
13.3.9.3.6 Follow-Up Trouble Orders 13-44
13.3.9.3.7 System Messages (Case Notes) 13-44
13.3.9.3.8 Outage Reporting 13-45
13.3.9.4 Quality of Service Indices 13-46
13.3.10 Crew Management 13-48
13.3.11 Automatic Vehicle Location 13-53
13.3.12 Mobile Workforce Management 13-53
13.3.13 Distribution Load Forecasting 13-54
13.3.14 Protection Coordination 13-55
13.4 Study Mode 13-55
13.4.1 Study Analysis Execution Mode 13-55
13.4.2 Study Working Areas 13-57
13.4.3 Save Cases 13-57
13.5 External System Interfaces 13-59
13.5.1 ADMS-SCADA from EMS Interface 13-60
13.5.2 Geographic Information System (GIS) Interface 13-60
13.5.3 CIS Interface 13-63
13.5.4 ADMS-SCADA from/to AECall Interface 13-64
13.5.5 AMDS from/to Storm Center 13-65
13.5.6 ADMS-SCADA from/to AMI Interface 13-67
13.5.7 AMDS from/to WMS Interface (Requirement for future use) 13-67
13.5.8 ADMS-SCADA from/to MWM Interface (Requirement for future use) 13-67
13.6 Integration Architecture Approach 13-67
13.6.1 Application Programming Interfaces (APIs). 13-69
13.6.2 Transport Mechanism 13-69

13.6.3 Message Bus 13-70

List of Exhibits:

Error! No table of figures entries found.

13. ADMS-SCADA Functional Requirements

R[1] This Section describes the ADMS-SCADA capabilities that are required by AE to support operations of its distribution system.

R[2] These capabilities include monitoring, analyzing and managing the system and field forces that operate the system.

R[2.A] Monitoring includes:

R[2.A.i] Advanced visualization for situation awarness, including the ability to:

R[2.A.i.a] Zoom and pan to navigate displays and to present different levels of detail for any selected portion by selecting the desired view using a “rubber banding” technique.

R[2.A.i.b] De-cluttering of symbols, devices, data values, and text shall occur at selected zoom factors.

R[2.A.i.c] The ability to present different levels of display for any selected part of the system to the Primate Video Wall software.

R[2.A.ii] Power flow and characteristics (current, Watts, VARs…)

R[2.A.iii] Outage information (calls, device operations…)

R[2.A.iv] Equipment status

R[2.A.v] Real time topology information.

R[2.B] Analyzing includes:

R[2.B.i] Identify potential overloads, high/low voltage conditions and ways to correct those conditions

R[2.B.ii] Topology identification and validation.

R[2.B.iii] Determine fault location based on fault current, Fault Circuit Indicators (FCI - both telemetered and field reported), and Distance To Fault (DTF) supplied by IEDs

R[2.B.iv] Identify outage location and restoration alternatives

R[2.B.v] Identify ways to reduce distribution system losses

R[2.B.vi] Develop switching procedures to support recommended circuit changes

R[2.C] Managing includes:

R[2.C.i] Manage crews during the restoration process

R[2.C.ii] Exercise supervisory control to reconfigure the distribution system

R[2.C.iii] Manage crews through the switching process

R[3] This functional requirements section describes AE's expectation of ADMS-SCADA in support of the above capabilities.

R[4] The ADMS-SCADA functions shall operate in concert to provide a robust tool for managing the distribution system.

R[4.A] For example, as part of developing a switching procedure for partially restoring an outage, the ADMS-SCADA may incorporate a load flow to prevent low voltages or overloads due to the suggested sequence.

R[5] The ADMS-SCADA shall use a single real-time data model as the platform for all functionality.

R[6] Updates to the model shall be made once, in one place, for use by all ADMS-SCADA functions, modules and applications.

R[7] Similarly, data loaded into or edited within the ADMS-SCADA will be used by all modules without requiring manual intervention to recreate that data.

R[8] This model will be based on the Common Information Model (CIM), with extensions provided by the vendor to address elements not covered by the CIM.

R[9] AE requires that all ADMS-SCADA functionality be accessed through a single HMI, presenting a common appearance to the user.

13.1 Function Priorities

R[1] The ADMS-SCADA will provide a mechanism to allow higher priority operations to take precedence over lower priority ones.

R[2] These priorities will be managed so that processes or applications that are supporting one function will not inhibit the user's ability to perform a higher priority function.

R[3] The priority of the different functions shall be configurable. Examples of functional priority are:

R[3.A] *Control functions* – The control of a device and feedback on the success of the operation will be provided in a timely manner and will not be negatively impacted by other processes running on the workstation. Control shall have the highest priority.

R[3.B] *Outage operations* – Manual operations to outages shall typically fall next in priority.

R[3.B.i] Operations such as assigning a crew to an outage, confirming an outage or closing an outage shall respond in a timely manner and will not be negatively impacted by other lower priority processes running on the workstation.

R[3.C] *Informational* – Data provided to the dispatcher to aid in performing their tasks will fall lower in the priority list.

R[3.C.i] This information will be processed and presented in such a ways as to not negatively impact other, higher priority processes.

13.2 Distribution System Operations Model (DSOM)

R[1] The ADMS-SCADA shall include a single Distribution System Operations Model (DSOM).

R[2] The DSOM shall serve as a central information resource by representing the operating state of AE's distribution system, field devices, outages and field forces engaged in the support of the system.

R[3] Common points between the ADMS-SCADA and external systems shall be supported such that the respective applications work in an integrated fashion (See section 13.5 below).

R[4] The DSOM shall provide as a minimum:

R[4.A] Analytic models of electrically connected elements of AE's distribution system.

R[4.B] Information for schematic displays of the electrical facilities, showing individual elements and interconnections, along with the operating state and related information.

R[4.C] Information for geographically oriented displays of the distribution system showing the individual elements, their operating state, the distribution system network connectivity, operations data, facilities, equipment and the attribute of the objects (pole information, transformer information, customer information), locations of field crews, outages and other related information.

R[4.D] Landbase information such as street maps, buildings, waterways, aerial photography and other landmark details as an overlay.

R[4.E] Operations data such as feeder and device status indications, associated statistics, safety tags, operating limits, set points, power flows, voltages, currents, transformer tap positions, voltage regulator status and tap positions, load-shed breaker operation, quality codes, alarms, outage locations, scheduled or planned outages, estimated restoration time, and locations of field crews.

R[4.F] Facility and equipment information such as status, alarms, location and site details, electrical and mechanical design parameters, operating instructions, and maintenance procedures.

R[4.G] Field crew information such as names, planned assignments, complete assignments, and current location.

R[4.H] Modeling information for electrical devices, 3-phase unbalanced network connectivity, and loads.

R[4.H.i] All necessary interactive features that allow the user to execute system functions via display point-and-click, drag-and-drop, and other convenient user interface features.

R[4.I] The ability to transfer data into a corporate data warehouse for other reporting and analysis needs.

R[4.J] Trouble reports including customer name, street, address, phone number, account number, complaint type, and comments.

R[4.J.i] Trouble contact records may be originated as:

R[4.J.i.a] manual entries based on calls from customers

R[4.J.i.b] automatic entries from automated systems such as:

(a) IVR

(b) MDMS (“last gasp” reports from meters)

(c) Web based trouble reporting systems

R[4.K] These trouble reports may include requests from customers for a callback after service has been restored.

R[5] The sources for the circuit connectivity model will be a GE Smallworld GIS with Electric Office (EO) and other AE sources for electrical attributes.

R[6] The source for the landbase information will be a GE Smallworld GIS with EO.

R[7] The DSOM shall allow representation of typical power system elements such as generators, substation buses, on-load tap-changing transformers, reactors, breakers, reclosers, overhead lines, underground cables, submarine cables, voltage regulators, load-break switches, fuses, switched capacitor banks, distribution transformers, loads (e.g., constant power, constant current, constant impedance, and parameterized voltage dependencies), automatic transfer switches, and temporary connections and disconnections applied in the field using jumpers, grounds, and cuts.

R[8] The system will be able to model three-phase unbalanced system with both delta and wye subsystems.

R[9] The system shall be able to model a closed loop, meshed, or radial fed distribution power network.

R[10] Operational changes made to the system shall be reflected immediately throughout the model.

R[11] These may include corrections to the model, the addition of jumpers/cuts and reconfiguration due to switching.

R[12] Impacts including customer count changes and movement of open outage orders will be incorporated.

R[13] The DSOM shall maintain records of all forced (fault or overload caused) outages and all planned (user-directed) outages, providing a convenient central repository of distribution outage information that can be used to support historical analysis, the calculation of outage reliability indices (SAIFI,SAIDI, CAIDI and MAIFI) and current real-time operations such as responding to trouble calls and interacting with field crews.

R[14] Statistics produced by this system may be used for planning the repair work and identifying failures or deficiencies in the distribution system components.

13.2.1 ADMS-SCADA User Interface Features

R[1] The ADMS-SCADA shall include an advanced graphical user interface to optimize the Operator's monitoring, managing and control of the AE distribution system.

R[2] This interface shall include the capabilities defined in the User Interface section of this Specification plus those described in the subsections below.

13.2.1.1 Distribution Circuit Displays

R[1] The ADMS-SCADA shall include two representative display formats as follows:

R[1.A] Geographically oriented Distribution Circuit Displays, R[1.B] Schematic feeder displays that are geographically relevant, but are not generated to scale for clarified presentation to system operations (refer to Section 13.2.1.3).

R[2] Both sets of feeder displays shall be created from information that is imported from AE's Smallworld GIS and other asset data sources.

R[3] The scaled view shall present world-map views of AE's Distribution System within the context of geographical landmarks such as streets, buildings, and hydrology.

R[4] The displays shall include landmark and facility names and all associated information to properly locate the Distribution System elements such as poles, customer service drops, distribution transformers, capacitor banks, reclosers, switches, fuses, feeder circuits, substations, RTUs and all other field equipment.

R[5] The schematic view will include only those elements which are necessary to support operating the system.

R[6] The system shall provide the user with a seamless view of the company's complete set of maps.

R[6.A] That is, the user will not have to manually load map sheets or map files for display, but that the system will keep the physical storage structure invisible to the user's navigation and display functions.

R[7] The display shall show current in-service, out-of-service, alarm conditions, crew locations, outages and their extent.

R[8] Highlighting and the colors used to distinguish the operating states of the different system elements shall be consistent with the AE's system overview display.

R[9] Outage highlighting color will indicate the status of the outage, such as predicted, confirmed, assigned, dispatched, restored and completed. The assigned colors should be customer configurable,

R[10] Graphical depiction of outages will include highlighting that distinguishes predicted and confirmed.

R[11] The user shall be able to zoom and pan to navigate the display and to present different levels of detail for any selected portion by selecting the desired view using a “rubber banding” technique.

R[12] De-cluttering of symbols, devices, data values, and text shall occur at selected zoom factors.

R[13] The ADMS-SCADA shall be able to present different levels of display for any selected part of the system on the Primate Video Wall software.

R[14] For all -possible views, the user shall be able to interact with the geographic display to perform any of the associated user interactions such as data entry and supervisory control.

R[15] This display shall also present relevant electrical, mechanical, and operational factors (e.g., maintenance, outage, and operating history) for individual elements of AE’s Distribution Systems. Features of the system will include:

R[15.A] An advanced graphical user interface (GUI) with a geographic map display capability showing

R[15.B] It shall include normal pan, zoom, and locate functionality.

R[15.C] The user shall be able to save the extents of the currently displayed graphics window as a named area.

R[15.D] A method of linking raster images; vector design files; jpeg, bitmap gif or PDF files; operating procedures, and other documents such as MS Word or Excel to specific objects shall be included to allow an operator to select the object to display the associated document, image or file.

R[15.E] The system shall support the notion of navigation gazetteers.

R[15.E.i] These navigational aids shall be based on the information dispatchers use to find locations.

R[15.E.ii] Sample subsets of potential gazetteers are:

R[15.E.ii.a] Facility Ids: switch number, breaker number

R[15.E.ii.b] Alarm ID

R[15.E.ii.c] Pole number & street name

R[15.E.ii.d] Customer info: name, phone, address

R[15.E.ii.e] System shall zoom and center on the device the customer is attached to. Typically a transformer or primary meter.

R[15.E.ii.f] Street address, cross street

R[15.E.ii.g] Circuit Name

R[15.E.ii.h] Line Name

R[15.E.ii.i] Substation Name

R[15.E.ii.j] Saved user view name

R[15.E.ii.k] Outage Event ID

R[15.E.ii.l] Crew Name

R[15.E.ii.m] Switching Order

R[15.F] Control Operation may be initiated from any representation of the device (object) on either the geographic or schematic views of the distribution system

R[15.G] The user shall be able to select a device on any graphics display and be able to toggle/cycle through all of the views that the device is graphically depicted on.

R[15.G.i] This shall include the device's representation on its geo-reference view, on its single circuit view, on its 3-phase schematic backbone view, and for substation equipment, on its substation one-line view.

R[15.H] Support using different symbols for differentiating equipment status, different types of crews and outages.

R[15.I] This geographic map display shall support user-defined settings for display of various layers of graphical data (land, roads, poles, switches, all outages, predicted locations, etc.) at various scale factors.

R[15.J] The user shall be able to view the list of critical customers and/or key accounts served by the selected facility by phase.

R[15.K] The advanced GUI will provide the ability to suppress the display of lower priority information such as low priority calls or alarms.

R[15.L] The advanced GUI shall include functionality for locating outages and crews

R[15.M] Outages affecting sections of primary shall highlight the affected circuit(s).

R[15.M.i] The graphical user interface shall allow manual placement of outages by the Operator.

R[15.N] A graphical display of the electric sub-transmission and distribution system with dynamic symbols indicating outages, crews and predicted failure points

R[15.O] Predictive engines to identify potential outage devices based on the number, type, and location of customer outage calls.

R[15.O.i] Multiple prediction engines/rules are required based on weather conditions (e.g., blue sky vs. storm vs. scattered disturbances).

R[15.P] A management information capability to allow management access to summaries and details of outage status and progress via the intranet.

R[15.Q] Ability to capture and time-stamp the history of a storm (e.g., trouble calls, Operator data entries, crew assignment, active outages) for playback and further analysis in a time-sequenced simulation environment.

R[15.R] A database that calculates monthly, year-to-date, and annual industry-standard outage statistics using the latest IEEE heuristics or other industry standards (e.g., SAIDI, SAIFI, CAIDI, MAIFI)

R[15.S] A predictive engine to provide information on estimated times for restoration (ETR) with a facility to manage ETR updates, both dynamically (e.g.; if travel time is 45 minutes and crew arrives in 20 minutes, ETR should adjust automatically) and manually.

R[15.S.i] ADMS-SCADA shall be able to accept manually entered ETRs as either a time duration (e.g., 30 minutes) or a specified date and time.

R[15.T] Crew scheduling and tracking capability to manage crews and field personnel during outages (as well as history).

R[15.T.i] Easy creation of crews (e.g., foreign crews)

13.2.1.2 Tabular Displays

R[1] Tabular displays shall be provided for alarm information, device status, trouble call entry, crew dispatching, outage analysis results, trouble call status, and outage resolution information.

R[2] All display views shall be automatically refreshed whenever any information that affects the real-time accuracy of the display data has changed, unless refresh is explicitly suppressed by the user.

R[3] Filtering will be provided to hide unwanted information based on user selectable criteria.

R[4] Various sorting, selection, and tracing criteria shall be provided for the tabular displays.

R[5] It shall be possible to utilize these criteria in any combination, both in predefined displays created by AE using the Vendor's furnished display tools and for ad hoc queries :

R[5.A] List of alarms

R[5.B] List of telemetered devices

R[5.C] Select list of trouble orders by substation, feeder, lateral, fuse, or transformer

R[5.D] Select all customers on a feeder, lateral, fuse, or transformer

R[5.E] Select all customers on a portion of the distribution system demarcated by a user-specified set of controlling devices (fuses and/or switches)

R[5.F] Identify all customers affected by an outage, regardless of whether a trouble call was received from the customer

R[5.G] Select trouble orders by priority level or priority level range

R[5.H] Select trouble orders by creation time or range

R[5.I] Select trouble orders by Area of Responsibility or Region

R[5.J] Select trouble orders by type

R[5.K] Select trouble orders by facility code

R[5.L] Select trouble orders for key accounts

R[5.M] Select dispatched trouble orders by crew assignment

R[5.N] Select undispatched trouble orders

R[5.O] Select single trouble order by customer name, address, telephone number, or account number

R[5.P] Select General Trouble orders.

13.2.1.3 ADMS-SCADA Schematic Auto-generation Functionality

R[1] The Vendor shall provide “on-the-fly” Schematic Auto-generation functionality.

R[2] This function shall create pseudo-geographic displays that maintain the geographic orientation of devices, but compress the distances between devices to allow a more compact display for use by the Operators.

R[3] Regeneration of the schematic will not substantially alter the orientation of devices from their placement in the previously generated schematic.

R[4] This function shall be configurable to allow AE to create rules and standard layouts that are then used by the Schematic Auto-generation function during its display creation process.

R[5] The Schematic Auto-generation function shall also allow the Operator/user to take the output of the generation and make modifications to the display (e.g., via display generation tools) to allow AE to create displays that adhere to their conventions and standards and shall be of high quality for use by operations.

R[6] The ADMS-SCADA shall enable these displays and the current system conditions to be saved for continued use by real-time operations.

R[7] This facility shall maintain a record of the manually initiated changes so that in the event that the underlying circuit is revised and a new schematic is automatically generated, these changes can be applied to the new display.

13.2.1.4 Tracing Electrical Connectivity

R[1] A feature shall be provided for tracing the electrical connectivity of any user-selected element of the world map in a unique and distinctive manner (e.g., by color) in both an upstream and downstream direction.

R[2] Examples of required tracing are:

R[2.A] The user shall be able to select a device or segment of circuit and trace from the selection downstream to the next protective or sectionalizing device, its distribution transformers, open points and tie switches.

R[2.B] The user shall be able to select a device or segment of circuit and trace from the selection upstream to the previous protective or sectionalizing device.

R[2.C] The user shall be able to select a device or segment of circuit and generate a trace set from the selection upstream to its source.

R[2.D] The user shall be able to select a device or line segment within a URD loop and manually trace to its open point.

R[2.E] The user shall be able to select a device and trace to nearest SCADA controllable device

R[2.F] The user shall be able to select a device or segment of circuit and generate a highlighted trace from the selection to the next occurrence of a specific device type: fuse, switch, The system shall keep all trace sets highlighted while the user pans and zooms until the user deactivates the highlighted trace set.

R[2.G] The user shall be able to select a device or segment of circuit and generate a highlighted trace from the selection to its set of sources.

13.2.1.5 Jumpers, Cuts, and Grounds

R[1] A feature shall be provided for the free-form placement of temporary jumpers, grounds, and cuts.

R[2] This feature shall allow the user to make temporary changes to a world map (avoiding the burden of permanent database changes) to reflect repairs and temporary load transfers between phases of a circuit that are being implemented by jumpering, grounding, and cutting in the field.

R[3] These changes shall be accomplished easily using special symbols.

R[4] Once installed, jumpers, cuts and grounds shall be considered devices that can have safety tags added and deleted from them.

R[5] When the repair is completed, it shall be possible to back out the temporary changes in a simple manner and quickly return the system display to its original state.

13.3 ADMS-SCADA Applications

R[1] The ADMS-SCADA Applications consist of a set of tools to help the Operator monitor, control and aid in the restoration of the distribution system.

R[2] Also included are analysis tools to assist in planning and configuration. These applications include:

R[2.A] Distribution Power Flow (13.3.1)

R[2.B] State Estimation (13.3.2)

R[2.C] Switching Order Management (13.3.313.3.3)

R[2.D] Safety Tagging (13.3.4)

R[2.E] Fault Location Isolation and System Restoration (13.3.5)

R[2.F] Distribution Circuit Fault Location (13.3.6)

R[2.G] Integrated Volt/Var Control, IVVVC (Capacitor, Regulator and LTC Control) (13.3.7)

R[2.H] Operations Device Monitoring (13.3.8)

R[2.I] Outage Management/ Restoration Applications (13.3.9)

R[2.J] Crew management (13.3.10)

R[2.K] Automatic Vehicle Location (13.3.11)

R[2.L] Mobile Workforce Management (13.3.12)

R[2.M] Distribution Load Forecasting (13.3.13)

R[2.N] Protection Coordination (13.3.14)

R[3] These applications are functionally defined in the following subsections.

13.3.1 Distribution Power Flow

R[1] The Distribution Power Flow (DPF) shall calculate the state of the distribution system based on (a) real-time measurements at substations and of locations along the feeders, (b) manually-entered input, (c) facilities data imported from the various AE sources, (d) a model of the operation of automatic devices such as reclosers, ATOs, LTCs, voltage regulators, and capacitor banks, etc. (e) a model of the loads along the feeder and (f) model distributed generation.

R[2] The DPF shall be based upon a robust three-phase, unbalanced distribution system model typical of North America. Common points represented in the EMS power system model and ADMS-SCADA model shall be accommodated.

R[3] The computed voltage magnitude and angle from the State Estimator shall be used as the input values of the source for the DPF or a study power flow.

R[4] Also, a DPF study shall be able to be initiated from a historical data snapshot from the Historian.

R[5] The DPF shall have the ability to analyze looped systems, but is restricted to the distribution model defined in the DSOM.

R[6] The DPF shall run periodically at the frequency (a user-definable parameter) as well as when triggered by an event (whenever a change in the topology of the distribution system or pre-defined change in status or analog data is detected).

R[7] The Operator shall be able to execute DPF on demand for an Operator-specified feeder or all feeders associated with a substation via the graphical User Interface and see the results on the same display.

R[8] DPF shall also run in study mode in conjunction with other application programs, such as the IVVC and FLISR functions.

R[9] The DPF shall also allow the user to execute power flow studies in study mode on selected areas within the distribution power system to determine, for example, the effects of feeder configuration and/or voltage adjustments on feeder load balancing, voltage drops, and losses.

R[10] Study mode will be used to run “What If” scenarios.

R[11] The application must provide the capability for storage,retrieval and playback of the number of “Save Cases” for study purposes.

R[12] The operator shall have the capability to modify the parameters such as connectivity, device parameters and other operational parameters before running a “What If” scenario.

R[13] Study mode operation shall be distinguished by a unique background color for the window or such other means so that it is not confused with real-time windows.

R[14] Distribution systems operated by AE are primarily radial, but on occasion, loads may be fed from parallel sources.

R[15] Distribution (Medium) voltage lines operate at nominal 34.5 kV, 12.47 kV.

R[15.A] The distribution system may be constructed as overhead, underground, or “mesh network”

R[16] Secondary (Low) voltage lines operate at nominal 480V, 277 V, 240 V, 216 V, 208 V, 125 and 120 V.

R[17] The DPF shall include models of the distribution transformers and approximate models of the secondary voltage lines.

R[18] Most loads are supplied at secondary voltages, but some large industrial and commercial customers are supplied at distribution voltage.

13.3.1.1 Required Characteristics

R[1] The DPF shall include the following characteristics:

R[1.A] The discrete transformer tap positions of LTCs and line voltage regulators shall be adjusted to maintain specified voltages while complying with prescribed ranges on voltages and tap positions.

R[1.A.i] The switching deadband shall also be modeled

R[1.B] Line charging effects shall be modeled, including the insulation losses of underground cables where applicable

R[1.C] Provision shall be made to accommodate capacitor banks that are switched on and off based on locally measured parameters.

R[1.C.i] As a minimum, DPF shall model capacitor banks that switch according to day of week, holidays, time of day, temperature, voltage measurements, or Var measurements with voltage override. Deadbands shall also be modeled.

R[1.C.ii] Automatic switching shall be enabled or disabled, as determined by the user or associated local/remote status points.

R[1.D] Automatic transfer switch positions shall be modified according to associated line energization status values

R[1.E] It shall be possible to model each load as proportional to a pre-specified normalized load profile.

R[1.E.i] The real and reactive components of each load profile will be specified independently as functions of time, day-type, and season.

R[1.E.ii] The DPF shall accommodate a minimum of twenty distinct load profiles (for example, residential, small commercial, large commercial, school, etc.).

R[1.E.iii] Each load profile shall be defined (at a minimum) as a set of 24 hourly values of real and reactive load for a minimum of seven day-types and four seasons.

R[1.E.iv] The DPF shall also allow for individual telemetered loads whose values are acquired through direct telemetry or through an interface with a future AMR (automatic meter reading) system.

R[1.E.v] The modeled load shall be scaled by multiplying the load from the load profile by a scale factor which may be defined to be proportional to the capacity of the distribution transformer, be proportional to the customer's monthly kWh usage, or be another scale factor specified by AE.

R[1.F] The system topology, connectivity, symbology, attribute data and location of the loads shall be derived from input from the Smallworld GIS and other AE sources. Changes in any of these, including symbology, will be reflected in the DPF.

R[1.G] The system shall support modeling discontinuities in feeder construction, where a feeder may be a single phase (say A phase) and may transition to multiple phases for a short distance, for example where a line that crosses a freeway is constructed with 3 phases for efficiency purposes, even though only one of the phases is being used.

R[1.H] The variation of load with voltage shall be modeled using separate expressions for real and reactive power.

R[1.H.i] Loads shall be adjusted to account for the changes in voltage that occur during the iterative power flow solution process.

R[1.I] Transformers shall be modeled by explicitly considering their copper losses, core losses, and voltage dependence.

R[1.J] Voltage drops on secondary voltage lines may be calculated with a simplified model that assumes that the secondary voltage drop is proportional to the transformer loading of the distribution transformer and that the maximum designed secondary voltage drop (a parameter initially set to 5%) occurs when the transformer load is at the nominal loading.

R[1.K] The DPF shall interface with a third-party relational database to obtain distribution circuit ratings.

R[1.L] The DPF must interface with customer loading information stored in a third-party relational database. DPF shall use allocated and spot loads where the allocated load is computed by a load allocation application.

R[1.L.i] Both load allocation and spot loads can derive their measurement from billed energy (specified as either kwh or kVA) that originates from AE's Customer Systems.

R[1.L.ii] However, the interface to AE's Customer Systems is separate from DPF.

13.3.1.2 User Input

R[1] The DPF function shall be designed to run in periodic or event trigger mode without user intervention and shall be extremely user friendly requiring very little Operator input when run on demand.

R[2] This input shall largely be limited to identifying the base case for the study and then making all desired changes prior to execution.

R[3] Line-out, re-sectionalizing, or other configuration change studies shall simply require the user to change the status of the appropriate switching devices on the associated geographic or schematic display in study mode.

R[4] Other changes shall only require simple numerical entries and, where appropriate, the selection of any relevant solution option available.

R[5] The user shall be able to execute the DPF function for a particular circuit, a particular substation, or a particular "area" (that is, combination of substations and/or circuits) selected by the user, using current base case or postulated load conditions.

13.3.1.3 Results

R[1] Multiple independent users shall be able to execute the DPF function concurrently, starting from the last execution or a selected save case. In these “what if” studies, limit violations generated by DPF shall not be treated as real-time violations, but shall be retained for display at the workstation on which the function was run.

R[2] In modifying the base case prior to execution, the user shall be able to scale loads, specify loads individually, modify bus voltages, and change device status values.

R[3] As a minimum, DPF shall calculate the following quantities:

R[3.A] Real power, reactive power, and current for all circuit elements

R[3.B] Voltage on each phase at all nodes, including secondaries of distribution transformers

R[3.C] Total real and reactive losses, line losses (load and no load), and transformer losses (load and no load), both in kWh and kvarh, and in percent

R[3.D] Monthly accumulated losses, in kWh and kvarh, and in percent by “total system”, substation, power bank, or feeder.

R[3.E] Tap positions for substation transformers and line voltage regulators

R[3.F] Switch positions for capacitors and automatic transfer switches

R[3.G] Feeder voltage drops along distribution voltage and secondary voltage lines

R[3.H] Phase imbalance of 3-phase circuits calculated by percent imbalance (e.g., average phase current minus largest individual phase difference from the average, divided by the average current)

R[3.I] Voltage imbalance of 3-phase buses (e.g., average voltage minus largest individual phase difference from average, divided by the average voltage).

R[3.J] Identify overloaded equipment (in amps or percentage of rating).

R[4] The DPF results shall be presented on the graphical displays used for real-time dispatching as well as in tabular form on dedicated displays.

R[5] The results of the DPF calculation shall be subject to the same limit checking as other calculated data, i.e., each calculated variable shall be tested against three pairs of limits, and a limit violation shall be generated when an overload is detected.

R[6] Limit violations determined by DPF shall be indicated to the user simply and clearly.

R[7] All line sections that are overloaded and all buses that have voltage violations shall be highlighted in color. All loops and parallel-fed loads shall be highlighted in a distinct manner.

13.3.2 State Estimation

R[1] The State Estimator function shall incorporate both telemetered (measured) and modeled information and dynamically estimate the states of unmonitored portions of the system.

R[2] In order to increase the accuracy of the State Estimator, especially in the feeder headers area, telemetry from the substation power transformers shall be used.

R[3] Feeder headers's active and reactive power estimates shall be made available to the SCADA/EMS Estate Estimator to increase its robustness.

R[4] Telemetered values shall be compared against a set of user adjustable "reasonability limits" to determine trustworthiness.

R[5] State Estimator shall consider "trusted" telemetry values as accurate and re-calculate estimated values between telemetered points.

R[6] The application iteratively predicts values at control points, calculates the difference between the predicted and actual values, determines a correction factor based on the difference and applies that correction factor to other areas of the model.

R[7] The state estimator information will be used by the other components of AMDS in actively managing the system in near real time.

R[8] State Estimator may interact with the Distribution Power Flow application for use by other ADMS-SCADA applications such as IVVR.

13.3.3 Switching Order Management

R[1] A switching order is a list of operations to be directed by the user when carrying out a procedure for switching elements of the power system.

R[2] Switching orders are typically used for maintenance, for transferring substation feeder loads to other sources, and for emergency switching procedures.

R[3] The ADMS-SCADA shall support the manual creation, automatic creation, execution, display, modification, maintenance, and printing of switching orders; to be done in either the geographical, schematic or tabular views.

R[4] This shall include the ability to define time delays and breakpoints as part of switching orders as well as to add switching actions, relay settings, and content (e.g., comments) that are not modeled in the DSOM.

R[5] The Switching Order Management function shall include the capability to define normal operating procedures and sequences that reflect AE's policies and procedures to simplify the switch order creation process (e.g., rules for grounding).

R[6] After a switching order has been created, the user shall be able to save it.

R[7] Switching orders shall be executable in real-time and in study mode.

R[8] Study mode execution shall allow the user to determine the switching order's potential impact on the power system prior to actual execution

R[9] The ADMS-SCADA shall allow DPF to be run in study mode at any stage of the switching procedure to determine the potential impact.

R[10] Switching order management shall be functional in both a geographical and an operating schematic view of the system.

13.3.3.1 Manual Creation of Switching Orders

R[1] The user shall be provided the ability to create a switching order by using a full-screen editor to enter information for the header and the body of the switching order.

R[2] Preparation of the switching order shall require as little user interaction as possible.

R[3] This shall include the ability to "point and click" to create a switching order from the Geographic and schematic displays.

R[4] This may be created based on a new switching order or from an existing order.

R[5] The header shall contain information such as the following:

- R[5.A] Switching order sequential number
- R[5.B] Circuit name
- R[5.C] Permit required (Yes/No)
- R[5.D] Start date and time
- R[5.E] Complete date and time
- R[5.F] Crew ID: Service truck/car number, crew names, and phone/contact number
- R[5.G] Nature of work
- R[5.H] Location of work
- R[5.I] Prepared by whom and when (If created automatically, "Created by System" shall be indicated).
- R[5.J] Checked by whom and when.

R[6] The body of the switching order shall consist of multiple entries defining the actions to be taken.

R[7] Each entry shall have a sequence number automatically assigned by the ADMS-SCADA.

R[8] The user shall be able to enter the text of each entry directly, or employ a macro capability in which the macro has already been defined as a complete or partial switching order.

R[9] The user shall be able to edit the text of the macro expansion.

R[10] In some cases, the user will have to fill in the blanks in the macro expansion to complete the entry.

R[11] The exact form and content of the switching order headers and macros will be determined by AE during the course of the project.

13.3.3.2 Automatic Generation of a Go-Back Order

R[1] Many switching orders are created to perform temporary work.

R[2] When the work is completed, there is often a requirement to restore or back out the circuit to normal conditions.

R[3] This is frequently the opposite procedure from the one used initially.

R[4] The ADMS-SCADA shall provide a mechanism to automatically generate a go-back switching order.

R[5] Starting from an initial switching order, when the user requests "Generate Go-back Order", the ADMS-SCADA shall reverse the order of all entries in the body of the initial switching order and shall change each of the "reversible" entries to its opposite.

R[6] For example, an entry CLOSE BREAKER shall be reversed to OPEN BREAKER, an entry PLACE TAG shall be reversed to REMOVE TAG, and an entry TAKE OUT LEAD shall be reversed to PUT IN LEAD.

R[7] The ultimate list of "reversible" entries and their associated "opposites" will be developed in coordination with AE during the course of the project.

R[8] The user shall be able to edit the text of the various entries.

R[9] Before the user is permitted to save the go-back order, the ADMS-SCADA shall prompt the user to edit its header.

13.3.3.3 Automatic Switching Order Creation and Execution

R[1] The user shall be able to initiate the automatic creation and execution of a switching order that will reconfigure feeders according to rules supplied by AE.

R[2] This shall include the rules used by the Fault Location Isolation and Service Restoration function (Section 13.3.5).

R[3] To initiate automatic creation and execution of a switching order, the user shall be able to identify (e.g., by a point-and-click operation) the feeder or feeder sections to be reconfigured (i.e., disconnected or reconnected) and then request the ADMS-SCADA to automatically create and execute the appropriate switching operations.

R[4] If desired, the user shall be able to review the switching operations created by the ADMS-SCADA, make any necessary changes, and then request their automatic execution in a user-controlled step-by-step process.

R[5] Each switching operation shall be listed in the order in which the switching devices need to be controlled (e.g., tagged, opened, closed).

13.3.3.4 Maintenance of Switching Orders

R[1] After a switching order has been created, the user shall be able to save it.

R[2] The ADMS-SCADA shall save the actual expanded text of the switching order, not the text of the macros or the supervisory control procedure used to create it.

R[3] The ADMS-SCADA shall maintain a directory of switching orders, organized by area of responsibility with user search capability by substation name and/or range of date and time.

R[4] The user shall be able to use the directory to review, copy, rename, print, and delete switching orders, and to call them up for review and modification.

R[5] The Operator shall be able to sort and filter the switching order directory to help locate orders by any of the directory parameters and all or part of the switching order title or name.

R[6] The ADMS-SCADA shall also maintain a file of switching order macros, organized by area of responsibility, and sorted alphabetically.

R[7] The user shall be able to add, delete, and modify the macros in this file according to the user's assigned areas of responsibility.

R[8] While manually creating a switching order, the user shall be able to open a window, view the contents of the macro file, and select the macro to be expanded and placed in the switching order being created.

13.3.3.5 Switching Order Execution and Checkout

R[1] Switching orders (including go-back orders) shall be executable in real-time and in study mode.

R[2] Execution shall take place in proper sequence (automatically configurable option) or in manual step-by-step mode based on assigned breakpoints.

R[3] All built-in time delays and breakpoints shall be recognized. Alternatively, the user may temporarily assign new time delays and breakpoints.

R[4] For steps involving the execution of SCADA actions, the user shall be able to perform those operations in both the Tabular and Geographic/schematic displays

R[5] Study-mode execution shall allow the user to check out the switching order's potential impact on the distribution system prior to actual execution of each switching step.

R[6] This capability shall also be available during the course of preparing the switching orders.

R[7] In particular, it shall be possible to verify whether a planned switching order will result in overloads and voltage problems.

R[8] The new circuit configuration, the energization of the circuit segments, the current and voltage values expected from the planned switching order shall be shown on study versions of the distribution system world-map displays using dynamic coloring to highlight all possible limit violations.

13.3.4 Safety Tagging

R[1] Safety tags are conditions applied to database values in order to call the users' attention to exception conditions for field devices and to inhibit supervisory control actions.

R[2] Technical requirements for tagging are described in Section 6.4.1, Safety Tag Types and Supervisory Control Inhibit.

13.3.4.1 Safety Tag Application

R[1] The user shall be able to create a safety tag on system one-line displays and tag summary displays for any ADMS-SCADA data point, both telemetered and calculated/pseudo.

R[2] The selected device shall be highlighted on the display.

R[3] The user shall be required to enter, for each safety tag, the following information:

R[3.A] Date and time of safety tag placement, supplied by the system at time of Operator entry

R[3.B] Safety tag type

R[3.C] Point identification (supplied by the ADMS-SCADA)

R[3.D] Comment - As part of the safety tag placement process, the ADMS-SCADA shall prompt the user to enter alphanumeric comment information to be stored with the safety tag (80 characters).

R[3.D.i] The comment field shall be included in the event messages recording the addition or removal of a safety tag.

R[3.E] The user ID of the user applying the safety tag, supplied by the system

R[3.F] Order number/Clearance number

R[3.G] Clearance Person

R[4] The ADMS-SCADA shall retain a copy of all changed data so that the data can be retained on a cold start or incorporated into a new database at the option of the user.

R[5] Each safety tag shall be presented on a safety tag summary display listed by AOR with an alphabetical sort.

R[6] It shall be possible to edit and delete safety tags from this display.

R[7] Safety tag application, all safety tag changes (e.g., safety tag comments), and removal shall be recorded as events.

R[8] An indication shall be provided that multiple safety tags are associated with the device.

R[9] Selection of the device safety tag shall bring up the safety tag summary display.

R[10] The ADMS-SCADA shall include the capability to enter and edit multiple safety tags simultaneously by selecting the data points and entering the data common to the set of safety tags.

13.3.4.2 Safety Tag Clearances

R[1] The ADMS-SCADA Safety Tag Clearance number/Order number shall be used to help AE manage the completion of work, track staff working related to a clearance, and control the removal of safety tags associated with the clearance.

R[2] The Clearance Person field shall show a separate line for each person assigned to the clearance.

R[3] The ADMS-SCADA shall not allow the clearance number to be cleared until all clearance person names have been removed.

R[4] At that time, the Operator shall be able to clear the clearance number field.

R[5] The ADMS-SCADA shall allow safety tags to be removed only after the clearance number field is cleared.

R[6] Additional characteristics of this function shall include:

R[6.A] Display showing a summary listing of all active clearances, shown by district (e.g., AOR)

R[6.B] Displays showing all safety tags associated with a clearance

R[6.C] Ability to show all names (clearance persons) associated with a clearance

R[7] Ability to add/remove names from a safety tag with a clearance number, without having to select all safety tags in the clearance

13.3.5 Fault Location Isolation and Service Restoration (FLISR)

13.3.5.1 General

R[1] The Fault Location Isolation and Service Restoration (FLISR) module shall be aware of substation and feeder fault conditions that are considered permanent (based on the un-commanded trip and lockout of interrupters and/or blown fuses) and develop solutions (switching plans) for restoring service. Toward this objective the FLISR module shall:

R[1.A] Accept input as to fault location from:

R[1.A.i] The system's Distribution Circuit Fault Location (DCFL) module

R[1.A.ii] Direct input from users

R[1.B] Analyze the Distribution system and determine alternative power source availability based on current load conditions, protection parameters, historical information, etc.

R[1.C] Develop both "upstream" and "downstream", tiered restoration solutions (switching instructions) as follows:

R[1.C.i] Tier 1 - a solution that involves only the currently available, telemetry (remotely) controlled devices

R[1.C.ii] Tier 2 - a solution that involves all switchable components – both local (manual) and remote

R[1.D] Once restoration solutions have been developed they shall be either:

R[1.D.i] Presented to the Dispatcher for review / modification and subsequent manual execution (open loop operation). The Dispatcher may select individual switching steps or the presented order in whole as desired for execution.

R[1.D.ii] Automatically executed (closed loop operation)

R[2] It is Austin Energy's intention to use FLISR in an "open loop" operation initially. However, the system proposed shall be delivered fully capable of "closed loop" operation. Because initial configuration will be for "open-loop" operation, this specification's requirements are generally written in that context. Where applicable, all requirements listed shall apply to "closed loop" operation as well.

R[3] Suspension of Automation - At all times, the Operator shall have the ability to suspend (block) any and all automated execution of telemetry based control actions through minimal HMI interaction. The Operator shall be able to activate or de-activate automated controls in defined areas as follows:

R[3.A] system wide
R[3.B] per substation
R[3.C] per feeder
R[3.D] per device.

R[4] FLISR shall analyze all proposed solutions through modeled simulation.

R[4.A] Simulation used for FLISR purposes shall take into account:

R[4.A.i] Current load conditions

R[4.A.ii] Projected load conditions over a 6 hour window

R[4.A.iii] Equipment ratings

R[4.A.iv] Protective equipment settings

R[4.A.v] Alternative protective equipment settings (where available)

R[5] All tiered restoration solutions shall be ranked (based on "expected results") and presented to the Operator.

R[5.A] The system shall rank "expected results" based on individually weighted factors such as:

R[5.A.i] Quantity of meters restored

R[5.A.ii] Quantity of load (as modeled) restored

R[5.A.iii] Designated critical loads

R[6] Based on the predicted faulted line section, the FLISR shall determine the optimal (electrically nearest) switching devices for use.

R[6.A] A list of these devices shall be presented to the Operator.

R[7] The Operator shall have the option to initiate the isolation automatically through minimal HMI interaction.

R[8] When automatic switching is unavailable, the recommended switching shall be readily available as a guideline to perform necessary remote controls or manual switching in the field.

R[9] FLISR produced switching plans shall be adequate for the Operator to analyze the tie points suggested from available alternative power sources for restoration of healthy downsteam feeder sections.

R[10] The recommended switching may then be performed automatically by executing a switching order or manually where necessary or desired.

R[11] Once an outage is cleared, FLISR shall be capable of producing (and executing if enabled) a plan for returning the power system to its pre-fault configuration.

13.3.5.2 Required Characteristics

R[1] The FLISR function shall include the following characteristics:

R[1.A] FLISR shall be functional on both telemetered and non-telemetered circuits.

R[1.B] FLISR shall be designed to react appropriately to “looped” distribution circuits (fed from multiple sources).

R[1.C] FLISR shall be capable of processing single or multi-phase faults and shall not be restricted by time of occurrence on one or more feeders.

R[1.C.i] The ability to simultaneously process multiple faults of different types, on multiple feeders, shall be provided

R[1.D] FLISR shall react to fault indications the same whether fault location is manually entered by the Operator or submitted by the Distribution Circuit Fault Location module.

R[1.E] A remotely controlled circuit breaker and/or line recloser that is undergoing maintenance may temporarily be replaced or bypassed by a “non-remote controlled” device. The system shall be designed to allow an Operator to re-designate a device as “unavailable for remote operation”. FLISR shall functionally accommodate these re-designations in determining tiered restoration solutions.

R[1.F] To avoid potential difficulties during severe storm conditions, the Operator shall be able to suspend FLISR restoration capabilities by activating a single control point.

R[1.F.i] Otherwise, FLISR shall continue to operate for fault detection and isolation purposes.

R[1.F.ii] The Operator shall be able to resume FLISR's normal operation by deactivating the “storm-mode” control point.

R[1.F.iii] When this occurs, FLISR shall be ready to detect and make recommendations for isolating faults following the next outage event.

R[1.G] FLISR shall be capable of monitoring circuit breaker and line recloser status. This shall include:

R[1.G.i] discrimination between commanded and un-commanded trips

R[1.G.ii] determination of lockout conditions.

R[1.H] FLISR shall incorporate fault indications from telemetry to determine the line section where the fault has occurred.

R[1.H.i] After the fault has been location has been predicted, FLISR shall issue an event message that identifies the faulted feeder section.

R[1.I] FLISR shall recommend only devices that are available for switching operations.

R[1.I.i] Devices shall be considered unavailable if any of the following conditions exist:

R[1.I.i.a] The presence of a control inhibit tag

R[1.I.i.b] Bad telemetry

R[1.I.ii] As a configurable parameter, the FLISR shall also identify safety-tagged devices as potential devices for switching, but shall not include the device in the switch order unless the Operator takes appropriate actions to have the safety tag removed in accordance with AE’s safety procedures.

R[1.J] FLISR shall ensure that no potential overloads or problems such as excessive voltage drops shall occur as a result of proposed switching.

R[1.K] FLISR shall be capable of distinguishing substation and/or transmission related faults (that cause loss of outgoing feeder voltage) from distribution faults.

R[1.K.i] If FLISR monitors a continuous loss of feeder supply beyond an Operator-adjustable time interval, FLISR shall determine the switching orders that can be used to reconfigure available tie-switches in order to connect the de-energized feeders to alternative energy sources, such as other substations and/or feeders.

R[1.L] FLISR shall be capable of estimating and displaying the load that is to be restored following each recommended control action.

R[1.L.i] In addition, the Operator shall have access to an interactive environment to investigate the impact of alternative restoration strategies prior to the Operator's actual execution of a final restoration control sequence.

R[1.L.ii] This shall include comparisons such as line loadings, voltage profiles, load restoration levels, system losses, and number of affected customers.

13.3.6 Distribution Circuit Fault Location

R[1] The Distribution Circuit Fault Location (DCFL) function shall have the ability to detect, in an expeditious and reasonably accurate manner, the presence of substation and feeder faults, including lockouts that are above the substation IED sensing device threshold setting.

R[2] Fault location(s) shall be predicted based on the following general concepts:

R[2.A] When a fault occurs, the peak fault current shall be measured and reported to the ADMS-SCADA for processing .

R[2.B] The ADMS-SCADA shall perform an "appropriately scoped" short circuit study to determine all possible locations that could result in the measured fault current.

R[2.B.i] This "short list" of potential locations (based on fault current) shall be represented visually on the circuit display(s) and ranked by probability (most likely first).

R[2.C] When (if) other information can contribute to narrowing the potential list of locations it shall be applied.

R[2.C.i] "Other contributory information" shall include (but not be limited to)

R[2.C.i.a] Telemetry based Fault Circuit Indicators (FCIs)

(a) Imbedded FCI functionality of reclosers, motor operated air switches, etc. and/or

(b) Independent telemetry based FCIs

R[2.C.i.b] Field reports of manual FCIs

R[2.C.i.c] Field reports of actual fault location (visual evidence)

R[2.C.i.d] Meter "last gasp" reports

R[2.C.i.e] Meter "pinging" results

R[3] DCFL functionality shall not be dependent on any status change experienced by the substation feeder breaker.

R[4] The objective is to help AE reduce event analysis and location time.

R[5] The DCFL shall be performed at all substations and all feeder circuits.

R[6] It is anticipated that the DCFL will identify multiple locations that meet a given data profile.

R[7] Fault analysis shall be done internal to the DCFL.

R[8] The fault location shall use the ADMS-SCADA data model.

R[9] This model includes connectivity, switching devices, switch status, and power system parameters required to execute the fault analysis.

R[10] Users shall be able to disable the DCFL (i.e. stop sending/receiving fault data) with a single action when conditions warrant

13.3.7 Integrated Volt/Var Control (IVVC)

R[1] The IVVC function shall be used to achieve a variety of defined goals or "strategies" including but not limited to:

R[1.A] limit reactive power flows in the related distribution system

R[1.B] reduce system losses (including system reconfiguration)

R[1.C] reduce energy demand (including CVR - Conservation Voltage Reduction)

R[2] This shall be accomplished by sending various control signals automatically to the switchable shunt capacitor banks in the system and adjusting the tap positions of regulators and transformer LTCs, including those on feeders and in substations.

R[3] The IVVC function shall operate in either an "open-loop" or "closed-loop" mode. The user shall be able to selectively enable or disable IVVC based on:

R[3.A] Individual device (capacitor bank or voltage control)

R[3.B] feeder

R[3.C] substation power bank (group of feeders sharing a source transformer)

R[3.D] substation

R[3.E] system wide basis.

R[4] The system shall be used to minimize losses by controlling voltage and reactive power, consistent with maintaining customers' delivery voltages within user-defined norms, under continuously varying load conditions.

R[5] To meet the above objective, the function shall be capable of:

R[5.A] Identifying the switchable shunt capacitors that are available

R[5.B] Monitoring substation active and reactive power loads and voltages

R[5.C] Leverage voltage information available from the AMI deployment

R[5.D] Estimating voltages at the critical locations on the feeder and the low voltage lines (i.e. the highest and the lowest voltages delivered to customers)

R[5.E] Checking reactive demand against desired limits, where the limits may be expressed in either leading or lagging VARs

R[5.F] Sending control signals to bring capacitors on-line or off-line, as appropriate, to maintain power factor and/or voltage within Operator adjustable limits.

R[5.G] Sending control signals to adjust regulator and transformer LTC voltages, as appropriate, within Operator adjustable limits.

R[5.H] The ability to interface to various communications systems for communicating control signals to feeder capacitor banks.

R[6] Volt/Var Control shall execute continuously. It shall use deadbands to ensure that no unnecessary control actions are taken.

R[7] Volt/Var Control shall use the DPF calculation (see Section 13.3.1) to determine voltage effects prior to taking control action, so that Operator-adjustable voltage limits shall not be violated, i.e., if the expected voltage violates a limit for any customer, control of the associated capacitor bank shall not be executed.

R[8] Control shall also be skipped if the device (capacitor, regulator or LTC) was last operated by the function within an adjustable time period.

R[9] The number of operations of a device shall be limited to a user defined limit.

R[10] Volt/Var Control shall confirm the correct operation of each control action, and shall issue an alarm if a controlled device fails to operate. In the case of capacitor banks controlled by one-way radio or pager, Volt/Var Control shall monitor the change in Vars at the substation to confirm the action.

R[11] Volt/Var Control shall calculate and maintain system, substation, and feeder records that can be used to report device operating statistics and the effect of the function's control actions.

R[12] The records shall be used for review and analysis and for producing reports.

R[13] A test report shall be generated that provides the Operator with the operational status and health of the devices including:

R[13.A] General

R[13.A.i] A control malfunction

R[13.A.ii] A communications problem

R[13.B] Capacitor

R[13.B.i] The bank's switch position is in a different operating state than expected

R[13.B.ii] The fuse of the capacitor for an individual phase is blown

R[13.B.iii] A switch malfunction

R[13.B.iv] A single-phase capacitor value is different than expected (too much or not enough capacitance).

R[13.C] Regulator or Transformer LTC

R[13.C.i] The tap is in a position different than expected

R[14] The Operator shall be able to execute the IVVC function on demand as well as in its normal automatic mode.

13.3.8 Operations Device Monitoring

R[1] The Operations Device Monitoring function shall track the number of operations made by every breaker, capacitor switch, recloser, and load-break switch that is monitored by the ADMS-SCADA.

R[2] It shall also track an associated contact-replacement index.

R[3] Devices shall be identified by area of responsibility, substation, feeder, and device ID to provide the necessary information for condition-based maintenance of these devices.

R[4] This identification shall continue to track operations when a device is switched temporarily from one feeder to another to restore customers during a circuit-switching process.

R[5] For each monitored device, the following counters shall be maintained:

R[5.A] Operations – not associated with DMS control functions

R[5.B] Operations – initiated by DMS functionality (automation and Operator remote control actions)

R[5.C] Operations - total

R[6] When a multiple changes (such as a trip-close-trip sequence) are reported by an RTU, each operation shall be registered.

R[7] The date and time of the last operation shall be saved for each device.

R[8] An Operator with proper authorization shall be able to edit any and all counters.

R[9] For each counter, an "Operator definable" limit may be entered. The ADMS-SCADA shall calculate the present number of operations expressed as a percent (which may exceed 100%) of its corresponding limit.

R[10] An Operator with proper authorization shall be able to inhibit operations counting for individual devices.

R[11] Such devices shall be included in summaries based on areas of responsibility.

R[12] Resetting and inhibiting counters shall be permitted only for devices that belong to the areas of responsibility to which the user is assigned, and resetting shall require the user to be assigned to an appropriate mode of authority.

R[13] The date and time when each counter was last reset shall be saved.

R[14] The counters, contact-replacement index values, and other related information shall be available for display and inclusion in reports.

R[15] The user shall be able to view the date and time of a device's last operation together with its accumulated operations data by simply selecting the device on any display where it appears.

13.3.9 Outage Management/ Restoration Application

13.3.9.1 General Features

R[1] ADMS-SCADA Outage Management/ Restoration Application (OMRA) shall support AE personnel in managing the outages for optimal power restoration solutions and improved management of crews and resources for resolution of these outages.

R[2] It will also allow AE to indicate where other AE crews are performing work to provide situational awareness.

R[3] OMRA shall analyze the trouble calls to identify the cause and location of the outage.

R[4] AE will then use this information to respond to the calls, dispatch field crews, and take other actions to restore supply to all AE customers who are affected.

R[5] The system shall support the notion of an outage event life cycle. Describe your system's support for

R[5.A] Unacknowledged – new events as yet unacknowledged by any dispatcher

R[5.B] Acknowledged - addressed/being analyzed by a dispatcher

R[5.C] Dispatched - manually or automatically assigned time and confirmed by a crew that is on the way to the location

R[5.D] Arrived – time crew has arrived at dispatched event

R[5.E] Assigned - assigned to specific crew for future work

R[5.F] Planned – switch plan related outage event

R[5.G] Restored - crew got power back

R[5.H] Complete - detailed root cause, failed device, weather conditions, follow-up routine work orders generated, etc…

R[6] The outage information received via trouble calls shall be converted into circuit information for outage analysis.

R[7] This will assist Operators in the timely restoration of all customer outages.

R[8] The analysis shall be based on a search of customer and distribution system databases, applying logic that can perform the following functions:

R[8.A] Locate the callers geographically and their connection point to the distribution system

R[8.B] Associate groups of callers with the status of feeders and devices (such as distribution transformers)

R[8.C] Apply any other useful data to identify the likely outage or outages that prompted the customer calls.

R[8.D] Have the ability to handle customers that are not associated to a feeder (customer mismatches and police and/or fire type calls)

R[8.E] Have the ability to separate outage calls (no power) from non-outage calls (Tree on wire has power)

R[9] The results of this analysis shall be shown on the displays of the affected feeder circuits.

R[10] The OMRA shall include an outage analysis engine to provide real-time outage information to the Operators and support the restoration activities for the distribution system.

R[11] It shall provide all standard functionality that is required to support the outage restoration process.

R[12] This includes data acquisition from the various sources: customer trouble calls, AMR power out reports, Distribution System Operations Model (DSOM) data and real-time device status from the SCADA functions.

R[13] The Crew Management (CM) function is the tool to manage crew workload.

R[14] CM shall provide all standard functionality that is required to manage and monitor crew performance, workload, and location.

R[15] Requirement for future use – The CM function shall use Global Positioning System/Automatic Vehicle Location (GPS/AVL), where it is available, to determine crew location information.

13.3.9.2 Outage Analysis

R[1] Outage Analysis shall use a real-time connectivity model to estimate the location of each reported outage based on input from the customers' calls, AMR data and input from telemetry reporting the status of feeder breakers, feeder reclosers, and de-energized substation busses.

R[2] The ADMS-SCADA shall possess the ability to ping meters through the AMR system to confirm outage prediction results.

R[3] OMRA shall automatically roll or group trouble orders to the predicted device outage and shall have the following analysis capabilities:

R[3.A] To have multiple sets of configurable and customizable rules that are based on weather conditions and that dictate how the trouble orders are rolled or grouped together (i.e., under what circumstances trouble orders initially associated with distinct devices are grouped together and associated with a single upstream protective device).

R[3.B] To manually edit (via drag and drop) the trouble orders grouped together. This includes moving a order from one group to another.

R[3.C] To manually change or add trouble orders to groups as well as dissolve groups into their individual trouble orders.

R[3.D] To allow the Operator to create, split, and combine groups based on information not known to the OMRA function.

R[4] The system shall assign an estimated restoration time based on device type, number of active outage events, and number of active crews.

13.3.9.3 Outage Resolution

R[1] The field crews will report resolution of a single or grouped outage via voice radio.

R[2] Future alternative, field crews will report resolution, via the Mobile Workforce Management System interface (option described in Section 13.3.12).

R[3] The crew times (order assigned, received, enroute, arrive, completion and closed), description of the resolution, the crew that resolved the trouble order, the time of resolution, field complete time, and the Operator that entered the resolution into the Outage Information System shall become part of the permanent trouble order record.

R[4] OMRA shall provide tools to assist the Operator in locating the appropriate trouble orders that should be closed when field crews report that they have performed repairs other than those called for in a specifically assigned trouble order.

R[5] These tools shall include, as a minimum, the following:

R[5.A] Search for trouble orders on the repaired feeder, lateral, and phase

R[5.B] Search for trouble orders on the street where the repair was made

R[5.C] Search for the nearest trouble order (in Cartesian distance) to the location of the repair.

13.3.9.3.1 Multiple Outage Levels

R[1] A significant challenge to most outage grouping algorithms is that outages at lower levels (e.g., a fused group or customer drop) may be erroneously believed to be cleared when a higher level outage (e.g., a feeder or lateral) is resolved in the ADMS-SCADA.

R[2] The OMRA shall provide a mechanism to help overcome this potential problem.

13.3.9.3.2 Partial Restoration

R[1] The OMRA function shall recognize conditions under which a switching operation changes the configuration of the system and restores some customers, even if the full grouped trouble order has not been resolved.

R[2] The source of the switching operation may be entry of the switch status by the Operator or the receipt of switching information from the ADMS-SCADA.

R[3] The ADMS-SCADA will correctly handle conditions where customers are restored from adjacent feeders. Statistics for the remaining customers that are still without service shall be updated accordingly.

13.3.9.3.3 Full Restoration

R[1] The ADMS-SCADA will provide the ability to indicate the successful restoration of service along with completion notes.

R[2] The ADMS-SCADA shall possess the ability to ping meters through the AMR system to confirm service has been restored.

R[3] Completion will update the IVR system to initiate customer call-backs.

13.3.9.3.4 Distribution Abnormal Status Detection

R[1] The OMRA shall be able to detect the following abnormal conditions on the distribution system and place these on the distribution condensed abnormal listing:

- R[1.A] Any switch in abnormal state
- R[1.B] Any circuit feeder or line section that is not energized.
- R[1.C] Any circuit feeder or line section that is being fed from an alternate source
- R[1.D] Any circuit feeders or line sections that are paralleled abnormally

R[2] The condensed abnormal listing shall be categorized by feeder and substation.

R[3] It shall allow sorting and filtering by area of responsibility, subregion, area, and voltage class.

R[4] The OMRA shall be able to detect the following abnormal conditions on the distribution system and place these on the distribution world map using dynamic coloring:

- R[4.A] Any switch in abnormal state
- R[4.B] Any circuit feeder or line section that is not energized (color by energized phases)

R[4.C] Any circuit feeder or line section that is being fed from an alternate source (color by source)

R[4.D] Any circuit feeders or line sections that are paralleled abnormally (color by normal state)

13.3.9.3.5 In-Service Trouble Orders

R[1] In-Service Trouble Orders refer to those that are not associated with an outage.

R[2] These may be generated in two ways:

R[2.A] An In-Service Trouble Call may be entered by the CSR in AECall

R[2.B] A Dispatcher may manually place an In-Service Trouble Order in the ADMS-SCADA using the geographical display.

R[3] In-Service Trouble Orders will be managed in the ADMS-SCADA along with the other Trouble Order types.

13.3.9.3.6 Follow-Up Trouble Orders

R[1] Follow-up trouble orders shall be used in the OMRA to indicate work that is required, following the initial resolution of a trouble order, to complete additional repairs or to make temporary repairs permanent.

R[2] The OMRA function shall allow the Operator to create a Follow-up Trouble Order that shall include a reference to the original trouble order, but its type and priority will be different.

R[3] The Follow-up Trouble orders shall be routed to the individual responsible for its resolution.

R[4] Future – OMRA shall provide the capability to transmit follow-up work requests via the Mobile Work Management System Interface (Section 13.3.12) for action by AE using its normal (non-outage) work processes and procedures.

13.3.9.3.7 System Messages (Case Notes)

R[1] The OMRA shall provide for storage of individual text messages or Case Notes for the system, each Area of Responsibility, and each device to which grouping can be performed (feeder, recloser, fuse, and transformer).

R[2] The Case Notes will be written and maintained by the Operators and will contain estimated restoration times as well as the cause of the outages.

13.3.9.3.8 Outage Reporting

R[1] The Outage Reporting component shall maintain all available data pertaining to restored outages on-line for a configurable period (initially 13 months) that does not impact real-time performance.

R[2] Partial restoration statistics shall be stored to account for users that are restored due to switching and transfer operations.

R[3] Momentary outage information for substation circuit breakers shall be time and date stamped for future review and analysis.

R[4] Using the geographic or the schematic display, the Operator shall be able to enter additional information pertaining to an outage, edit the non-archived data, insert additional partial restoration points and times, and combine existing outages into a single grouped outage and by separating a grouped outage into multiple outages.

R[5] The user will not be allowed to edit archived information using ADMS-SCADA.

R[6] The Outage Reporting component shall archive periodically, once per day (configurable), all available data.

R[7] The system shall allow for archiving of information to allow extended reporting of restored outages.

R[8] The archived data shall be accessible at a minimum by time and date, Trouble Order identifier, distribution feeder circuit, protective device, and customer and shall provide complete information regarding the outage order.

R[9] In response to a user request, the OMRA function shall calculate the interruption frequency and duration for a specific customer, transformer, or feeder, and the actual interruption history for a specific customer, transformer, or feeder.

13.3.9.4 Quality of Service Indices

R[1] The OMRA shall provide the ability to calculate quality of service indices that can be used to track and report on the performance characteristics of AE's Distribution System over various time periods (custom dates, monthly, quarterly, seasonally, annually or multi-year) as specified by the user.

R[2] This shall include quality of service indices pre-defined in the database or created by the user on-line. At least, the following quality of service indices shall be implemented: SAIDI, SAIFI, CAIDI, and MAIFI.

R[3] The OMRA shall record all input data related to the calculations of quality of service indices down to the customer level.

R[4] The user shall be able to view the quality of service indices and the variables used to calculate them via interactive displays that allow the user to:

R[4.A] Create, verify, and edit quality-of-service formulas

R[4.B] Verify and edit individual values of the calculation variables

R[4.C] Enable and disable one or more index calculations

R[4.D] Enter schedules for index calculations.

R[4.E] Set the minimum and maximum duration to be included in a calculation

R[4.F] Variables for calculation should include but not be limited to feeder breaker, map grid, zip code, cause, date, time of day, type of customer (commercial, residential, etc.), and type of equipment operating, including, but not limited to, outages originating in the distribution, substation, transmission, and generation systems.

R[5] The calculation variables shall include any values available, including real-time and historical data.

R[6] Tools shall be provided to compare sets of indices created at different times and over different time periods.

R[7] These tools shall allow statistical information to be generated for user-selected indices.

R[8] In addition, the user shall be able to generate, review, and schedule reports based on the quality of service indices.

R[8.A] In particular, the Vendor shall implement the quality of service indices defined as follows:

R[8.B] SAIFI = (Customers interrupted) / (System Customers), where only customers whose duration is greater than a configurable time are counted

R[8.C] SAIDI = (Customer minutes)/ (System Customers), where only customers whose duration is greater than a configurable time are counted

R[8.D] CAIDI = (Customer minutes) / (Customers interrupted) , where only customers whose duration is greater than a configurable time are counted

R[8.E] $CEMI_n$ = (Customers interrupted) for customers experiencing more than "n" interruptions / (System Customers), where customers whose duration is greater than or less than a configurable time are counted

R[8.F] MAIFI = (Customers interrupted) / (System Customers), where only customers whose duration is less than a configurable time are counted

R[8.G] where:

R[8.G.i] SAIFI = System Average Interruption Frequency Index

R[8.G.ii] SAIDI = System Average Interruption Duration Index

R[8.G.iii] CAIDI = Customer Average Interruption Duration Index

R[8.G.iv] MAIFI = Momentary Average Interruption Frequency Index

R[8.G.v] CEMIn = Customers Experiencing Multiple Interruptions

R[8.G.vi] Customers interrupted = number of interrupted customers per interruption event , counting each customer affected only once per event

R[8.G.vii] System customers = a variable calculated automatically that refers to the number of customers in the system for which the index is being calculated. This could be all AE customers, customers of a certain type, customers in a map grid, zip code, by feeder breaker, etc.

R[8.G.viii] Customer minutes = length of outage X customers interrupted for each step of restoration per interruption event) or the individual customer outage times for each customer affected)

13.3.10 Crew Management

R[1] The Crew Management (CM) function shall provide convenient access to all information necessary to track, contact, and assign work schedules to AE's field crews.

R[2] As a minimum, this information shall include:

R[2.A] Crew name or ID

R[2.B] Contact information (e.g., cell number, radio)

R[2.C] Planned and unplanned work assignments

R[2.D] Crew composition details (e.g., size and individual names)

R[2.E] Crew skill levels

R[2.F] Vehicle capability (type)

R[2.G] Crew and truck locations

R[2.H] Available equipment (e.g., Personal Protective Equipment (PPE), hot-line equipment, etc.)

R[2.I] Work assignments completed

R[2.J] Work assignments uncompleted

R[2.K] Assignment start and end times (actual or estimated)

R[2.L] Work assignment forms

R[2.M] Availability information

R[2.N] Tag and comment fields

R[3] The ADMS-SCADA will support the following functions in creating and updating crew information

R[3.A] The user shall be able to define preconfigured crews.

R[3.A.i] The crews are made up of crew members, trucks and special equipment.

R[3.B] The user shall be able to mark a crew as active or inactive.

R[3.C] The user shall be able to quickly create new crews containing contractors and make them active so they can have events dispatched or assigned to them.

R[3.D] The user shall be able to quickly split or merge crews based on crew restrictions or outage event conditions.

R[3.E] The system shall track hours on the job for each individual crewmember.

R[3.F] The system shall generate an alarm that color codes the crew on both the graphical and tabular displays they are displayed on when any member of the crew has reached a user definable threshold of hours on the job.

R[3.G] This system shall alarm the dispatcher when a crew member is overdue for a meal or rest period.

R[3.H] The user shall be able to generate a list of crew members that have reached a threshold number of hours on the job.

R[3.I] The user shall be able to list for each crew, its members and the hours (and partial hours to the tenth of an hour) currently on the job for each crew member and all events that have either been dispatched or assigned to the crew.

R[3.J] The user shall be able to view the list of available crews.

R[3.K] The user shall be able to view list of crews that have been dispatched to trouble events in the field.

R[3.L] The user shall be able to assign multiple trouble events to a crew.

R[3.L.i] A crew may only be actively working on one trouble event at a time.

R[3.M] The user shall be able to assign multiple crews to a given trouble event.

R[3.N] The user shall be able to view the list of crews who have no trouble events dispatched or assigned to them.

R[3.O] The system shall generate and display for each crew the estimated time they have left on the trouble events that have been dispatched or assigned to them.

R[3.P] The system shall be able to generate the number of additional crews required based on the current set of known and predicted outages and the number of active crews, their remaining availability and the user entered desired outage completion time.

R[4] Each crew location shall be shown on world-map displays of the power system in the form of distinct symbols defined by AE.

R[5] AE currently uses different symbol types for outage versus non-outage calls, plus varying colors indicating priority.

R[6] The symbols may be associated with user selected tag and comment fields.

R[7] Tags that indicate crew availability shall be supported along with others to be defined during project implementation.

R[8] Requirement for future use – The crew locations shall be capable of automatic entry based on truck location signals received via GPS facilities (i.e., Automatic Vehicle Locator-AVL) or manual entry by Operator input.

R[9] The Operator interface shall enable the user to display all current Trouble Orders based on user-specified filtering criteria.

R[10] The following minimum sorting, selection, and tracing criteria shall be provided for tabular displays.

R[10.A] View all Trouble Orders in a specified Area of Responsibility

R[10.B] Sort Trouble Orders chronologically

R[10.C] Select Trouble Orders on a feeder or device

R[10.D] Select Trouble Orders by priority level or priority level range

R[10.E] Select Trouble Orders by creation time or range

R[10.F] Select Trouble Orders by user category

R[10.G] Select Trouble Orders by type

R[10.H] Select Trouble Orders by facility code

R[10.I] Select Trouble Orders for specific key accounts (strategic accounts)

R[10.J] Select dispatched Trouble Orders by crew assignment

R[10.K] Select unassigned crews (i.e., crews that are in the clear)

R[10.L] Sort on any displayed field as either a primary or secondary sort field.

R[11] It shall be possible to define and subsequently request hardcopy reports of any tabular information, using the sorting, selection, and tracing criteria described above.

R[12] The CM function shall determine the preferred crew or crews for handling a Trouble Order based on crew member skills, vehicles available to the crew, crew proximity, current workload, activity priorities, remaining time before the crew's scheduled off time and other such considerations.

R[13] A Trouble Order refers both to outage work and In Service, or non-outage work The CM function shall determine what work should be assigned to a crew that is available for a new assignment and shall prioritize Trouble Orders when the number exceeds the number of crews.

R[14] The Operator shall be able to override the priority set by the ADMS-SCADA.

R[15] Once the Trouble Order is assigned, the Operator shall be allowed to dispatch, re-assign, edit, or cancel the Trouble Order.

R[16] The Operators shall be able to use drag and drop functionality to assign or re-assign a Trouble Order between crews.

R[17] A Trouble Order Tracking view shall display the following trouble order resolution information gathered by the field crews (all of them shall be custom configurable by AE):

R[17.A] "Construction Type" code – shall include codes for at least 100 construction types (e.g. 13.8 kV, streetlight, traffic signal, etc.).

R[17.B] "Problem" code – shall include codes for at least 30 problem types.

R[17.C] "Cause" code – shall include codes for at least 100 Cause types.

R[17.D] "Action Taken" code – shall include codes for at least 10 possible field crew actions.

R[17.E] "Failed Component" code – shall include codes for at least 150 possible power system components.

R[17.F] Material Code – shall include codes for at least 100 material codes.

R[17.G] "Refer To" code – this field shall identify the organizations within AE to which the trouble order should be referred for follow up actions.

R[17.G.i] At least 30 possible codes shall be custom configurable by AE.

R[17.H] Observations field – this field shall include space for at least 256 characters (configurable) of free form input for comments.

R[18] Crew Management shall maintain various AE-defined statistics on crew performance over a period of at least one year.

R[19] These statistics shall be capable of being displayed and edited on workstation monitors and printed in the form of crew management reports.

R[20] The crew management information shall also be capable of being archived and retrieved for review and analysis on demand.

13.3.11 Automatic Vehicle Location

R[1] AE employs Global Positioning System (GPS) receivers in field crew vehicles used by AE to operate the distribution power system.

R[2] The geographical location (latitude and longitude, or map coordinates) of each of the vehicles will be transmitted to a GPS master station.

R[3] AE will provide an interface to allow the GPS master station to be integrated to the ADMS-SCADA.

R[4] The CM function shall have an interface to the GPS master station to receive the location of each crew vehicle, along with associated miscellaneous status information (e.g. vehicle parked, bucket in use, etc.).

R[5] The CM function shall display a symbol to represent each vehicle at the appropriate location on an Outage and Crew Management graphic map.

R[6] It shall be possible to define different symbols to represent different types of vehicles or their associated crews (e.g. overhead versus underground, multiple vehicle types, assigned “mission” such as capacitor bank truck, etc.)

R[7] When the Operator clicks on the symbol for a vehicle, the associated Crew Information View shall be brought up.

13.3.12 Mobile Workforce Management

R[1] AE has future plans to implement the Oracle Mobile Workforce Management (MWM) solution.

R[2] The ADMS-SCADA should have standard messages already developed to allow ease of integration when MWM is eventually implemented.

13.3.13 Distribution Load Forecasting

R[1] To support operations planning and analysis, area loads (15 minute intervals at a minimum) shall be forecast for up to eight days in the future and back cast at least 8 days in the past.

R[2] The user shall be able to save forecasts in any of a user selectable number of save cases, one of which shall contain the active forecast that shall be available for study functions such as DPF.

R[3] The user shall be able to make adjustments to the active forecast.

R[4] In addition, Distribution Load Forecast shall make adjustments to future load forecasts automatically.

R[5] This shall be based on the amount of mismatch between the forecasted loads and the actual loads of previous periods as they become known.

R[6] The user shall be able to import weather data from various sources such as weather services, the generation QSE load forecasting spreadsheet, etc..

R[7] These conditions can include: temperature, barometric pressure, relative humidity, precipitation level, wind speed, wind direction, and luminosity.

R[8] A similar-day forecast shall be used that is based on the normalized load values stored for each of seven day types.

R[9] Provision shall be made for storing day types for the last 25 months.

R[10] The storage shall be updated each day by replacing the oldest of the same day type with the most current actual load curve.

R[11] The similar-day forecast shall search the 25-month file for the same day type whose weather conditions best match those entered by the user.

R[12] It shall then present the user-entered and best-matched conditions, for user comparison, together with the chosen day's loads as the suggested forecast.

R[13] The user shall be able to modify any of the forecast's loads manually.

R[14] In addition, the user shall be able to scale the entire forecast by simply specifying an appropriate peak load value.

R[15] Multi-day forecasts shall be constructed by permitting the user to define the input data for each forecast day.

R[16] The user shall be able to print and display the forecasts in both tabular and graphical form.

R[17] This shall include the ability to display the active forecast with the actual loads of current and past days superimposed.

R[18] The load-forecasting tool must be able to interface to an Oracle-based program that contains historical information for locations without telemetry.

13.3.14 Protection Coordination

R[1] The Protection Coordination application will use the system characteristics in the ADMS-SCADA model to analyze and assure proper coordination between the protective devices (relays, reclosers, fuses, etc.) on the feeder.

R[2] Information such as the curves associated with the devices and available short circuit current will be the basis for the coordination, the software will analyze this information, identify areas of potential problems and guide the user in recommended changes for proper coordination.

13.4 Study Mode

13.4.1 Study Analysis Execution Mode

R[1] In the study mode, programs shall be executed on user demand to analyze current, past, and future power system conditions.

R[2] The following study network analysis functions shall be provided:

R[3] Study Case Initialization

R[3.A] Distribution Power Flow Study (DPF)

R[3.B] Study State Estimation

R[3.C] Fault Location Isolation and Service Restoration (FLISR)

R[3.D] Integrated Volt/VAR Control (IVVC)

R[4] Operators shall have the capability to easily initiate or cancel studies at any time.

R[5] Given the AOR authority, the study sequences can be terminated.

R[6] A study sequence execution control display shall be provided, which shall allow the Operator to control study setup (including easily selecting groups of adaptive parameters for initialization), sequencing, and execution, and which shall show study completion as well as the occurrence of error conditions.

R[7] If a study is canceled, the execution shall stop as soon as possible and no database areas shall be corrupted with inconsistent data.

R[8] A canceled study shall be re-executable with no adverse affect on the results.

R[9] The control of each study function shall be totally independent of the real-time version, and each study function shall have execution and tuning parameters that can be adjusted independently of the real-time functions.

R[10] Study network analysis functions, except where noted for a specific study function, shall not generate any real-time alarms due to detected violations or solution failures; these types of conditions shall be available on solution results and diagnostic displays.

R[11] It shall be possible to initialize a study base case using information available from:

R[11.A] The most recent complete state estimator solution:

R[11.A.i] A study work area can be initialized to either the latest SE solution of real-time or to the equipment default values on a global basis

R[11.B] Distribution Power Flow study save cases

R[11.C] State estimator save cases

R[11.D] Real-time SCADA data (Applicable to study State Estimator only).

R[11.E] Normal state for all devices. Devices without a normal state shall be defined as open

R[12] By specifying a date and time, the base case for the given date and time shall automatically be constructed using data from the parameter adaptation function.

13.4.2 Study Working Areas

R[1] Multiple users with multiple independent working areas shall be supported.

R[2] Each user shall have an individual working area, which shall be used as a temporary location to gather information needed to run a study, modify the data as needed to represent the desired study conditions, and temporarily hold the study results.

R[3] Modifications made by a user in the user's working area shall not affect the source of data or any other user's working area.

R[4] When a saved case is moved to an individual's study working area a new working case will be created to minimize interference with use of the cases saved in the save case library.

R[5] Upon retrieving a save case, the user can manually change the study case title in order to make the test case unique before storing it into another save case. Interaction between users shall only be through permanent save cases. It shall be possible for multiple users to simultaneously prepare input cases, execute programs, and examine the output.

13.4.3 Save Cases

R[1] The following applications shall include save case capability:

R[1.A] Distribution Power Flow Study (DPF)

R[1.B] Study State Estimation

R[1.C] Fault Location Isolation and Service Restoration (FLISR)

R[1.D] Integrated Volt/VAR Control (IVVC)

R[2] The save cases generated and used by different applications may be significantly different in structure and content.

R[3] However, the following characteristics shall be present in all save cases:

R[3.A] The saved information shall include all input and output data, as well as all information needed to identically reproduce the output by rerunning the application.

R[3.A.i] Where necessary to meet this requirement, it must be possible to revert to previous models if the model has been changed subsequent to the original execution of the application.

R[3.A.ii] The original save case can be retrieved again to revert to the previous study case.

R[3.B] Save cases shall be stored in a library.

R[3.B.i] The library shall be sorted by application (or separate libraries may be supported for each application) and by date and time.

R[3.B.ii] Filtering will be supported via general HMI capabilities

R[3.C] Each save case shall include the following information: the name of the application, the time and date the save case was produced, an 50-character user-entered title, and a user-entered comment field of at least 512 characters.

R[3.D] Save cases may be copied and moved to archive media and restored from archive media to the save case library.

R[3.E] A locking mechanism shall preclude deletion from the library.

R[3.E.i] The lock shall be set and removed by any user.

R[3.F] Capability to merge new model updates into the existing save cases to the extent possible to allow each save case to reflect the new on-line production system model.

R[4] Save cases shall contain all information needed to describe the distribution system at the time it was saved.

R[5] This includes not only data normally considered as dynamic, such as system load, switching device statuses, and generating unit limits, but also a full definition of the network model (node level connectivity and electrical characteristics).

R[6] Save case information shall be sufficient to execute a study for a previous network model and generation schedule, even after a database change of any of this data.

R[7] Save cases shall be accessible by all users.

R[8] A user-selectable locking mechanism shall be provided to prevent users from inadvertently purging, overwriting, or modifying specific save cases.

R[9] Save cases shall not be lost on a database update. It shall be possible to copy save cases to permanent storage medium and to reload save cases from permanent storage medium.

13.5 External System Interfaces

R[1] These interfaces are the set of hardware and software elements that allow the integration with the various AE external systems. Common points between the ADMS-SCADA and external systems shall be supported such that the respective applications work in an integrated fashion.

R[2] These include:

R[2.A] EMS/SCADA

R[2.B] ICCP data

R[2.C] Data concentrators such as DC System's Intelligent Communication Gateway (ICG)

R[2.D] IBM Websphere Bus

R[2.E] Smallworld GIS with EO version 3.3 (will be upgrading to 4.2)

R[2.F] Oracle Customer Care and Billing (CC&B) CIS – go live date 2nd Q of 2011 (Current Customer Information System – Vertex E-CIS version 3.1C1)

R[2.G] Automated meters (AMI) may be interfaced directly with Landis + Gyr or a local Ecologic Meter Data Management System (MDMS) for power out (last gasp), power up reporting and pinging.

R[2.H] AECall - a homegrown trouble call recording application

R[2.I] 21st Century High Volume calling system – an automated call answering service

R[2.J] iFactor Storm Center v1.5.1 – internal and external web based outage location viewing and trouble call submittal tool

R[2.K] OSI PI Historian

R[2.L] Oracle Mobile Workforce Management

R[2.M] Automatic Vehicle Locator (AVL)

R[2.N] TOA

13.5.1 ADMS-SCADA from EMS Interface

R[1] Common points represented in the EMS power network model and ADMS-SCADA model shall be accommodated.

R[2] Device status data (e.g., feeder breaker operation/lockout, etc.) and analog values shall be sent (one-way) from the existing EMS to the ADMS-SCADA for status and analysis purposes.

13.5.2 Geographic Information System (GIS) Interface

R[1] The AMDS shall be interfaced with AE's existing Geographic Information Systems (GIS), whose connectivity implementation is complete for the implementation of the ADMS-SCADA.

R[2] AE's GIS is a tool able to capture, store, edit, update, analyze, consult, and display all the referenced geographic information of the distribution system.

R[3] This information is useful to all corporate areas as a powerful and functional tool for the decision-making process, asset assessment, maintenance, and operational job documentation.

R[4] The existing AE GIS is based on GE's Smallworld (Electric Office).

R[5] Therefore, adequate interfaces to extract and export alphanumeric and graphical data from/to these platforms are required.

R[6] The GIS contains the information to define the distribution system, the feeder topology and all devices associated with the distribution system including their features, attributes, and connectivity.

R[7] The GIS also contains distribution transformers, secondaries and load point to which the customer relationship is maintained.

R[8] The data to be imported from GIS shall include both actual power system facilities as updated by AE on a daily basis and planned data for modifications or additions planned for the future.

R[9] The Operators will have the capability to validate planned construction/work and to permit it to become a part of the actual distribution power system model (DSOM) once work is completed in the field.

R[10] This shall include the capability to update the model to reflect the actual work performed in the field based on as-built information from the field crews performing the work.

R[11] Graphical differentiation of each type of data is required. Incremental updates of data shall be possible at any time.

R[12] The distribution system network is modeled based on device connectivity. In addition, the geographic division shall also be identifiable.

R[13] It shall be possible to import complete feeders at once without requiring identifying the geographic areas where the feeder is located.

R[14] The data imported from the GIS shall be subjected to two levels of validation before it is incorporated in the ADMS-SCADA database: automatic and manual.

R[15] The ADMS-SCADA shall perform automatic data checking and validation when the data are first received from the GIS.

R[16] The automatic validation shall include the following checks:

R[16.A] All required parameters are specified

R[16.B] All devices are connected to one and only one power source, loops shall be identified and highlighted

R[16.C] Phase connections are made correctly

R[16.D] Values of all numeric parameters fall within pre-specified ranges, etc.

R[16.E] All devices are connected (de-energized devices shall be identified and highlighted)

R[16.F] All unconnected devices and line segments shall also be identified and highlighted.

R[17] The data received shall be placed in a provisional layer, with all errors listed in a table and flagged or highlighted on a graphical display.

R[18] The user of the ADMS-SCADA shall be provided the ability to correct errors and supply missing data.

R[19] Then, as a separate step, a properly authorized user (typically a supervisor) will review the data in the provisional layer and may choose to accept it.

R[20] The performance of the interface shall be such that the expected daily incremental changes of AE data during a normal day shall be incorporated in the ADMS-SCADA within an estimated time of one hour maximum.

R[21] During the data update period there shall not be degradation of the normal ADMS-SCADA operation as defined by the specified performance figures for response times.

R[22] Only after the data has passed the complete suite of validity checks and has been accepted by an authorized user shall the ADMS-SCADA incorporate the data in the database, overlaying or supplementing the existing graphical and facilities data. Data received from the GIS shall not cause the loss of any real-time information, any manually-entered data, any user-entered notes, or any temporary changes to the topology (such as temporary cuts, jumpers, or grounds).

13.5.3 CIS Interface

R[1] The ADMS-SCADA shall interface with AE's existing Customer Information Systems. CIS functions include new customer connections information, customer information modification.

R[2] Information to be exchanged with the CIS is as follows:

R[2.A] CIS sends to the ADMS-SCADA all new customer installations, changes in the customer meter number, customer change of status, removal and customer consumption historical record for use by ADMS-SCADA applications.

R[2.B] The ADMS-SCADA shall receive incremental updates to customer information including, at a minimum, all changes for the customer's name, phone, premise address, and its priority code.

R[3] All of the above parameters shall be configurable.

R[4] The data imported from the CIS shall be subjected to two levels of validation before it is incorporated in the ADMS-SCADA database: automatic and manual.

R[5] The ADMS-SCADA shall perform automatic data checking and validation when the data are first received from the CIS.

R[6] The automatic validation shall include the following checks:

R[6.A] All required parameters are specified

R[6.B] All customer are connected to a valid load point

R[7] The data received shall be placed in a provisional table, with all errors identified.

R[8] The user of the ADMS-SCADA shall be provided the ability to correct errors and supply missing data.

R[9] Then, as a separate step, a properly authorized user (typically a supervisor) will review the data in the provisional table and may choose to accept it.

R[10] The performance of the interface shall be such that the expected daily incremental changes of AE data during a normal day shall be incorporated in the ADMS-SCADA within an estimated time of one hour maximum.

R[11] During the data update period there shall not be degradation of the normal ADMS-SCADA operation as defined by the specified performance figures for response times.

R[12] Only after the data has passed the complete suite of validity checks and has been accepted by an authorized user shall the ADMS-SCADA incorporate the data in the database, overlaying or supplementing the existing customer data.

R[13] Data received from the CIS shall not cause the loss of any real-time information, any manually-entered data or any user-entered notes.

13.5.4 ADMS-SCADA from/to AECall Interface

R[1] The ADMS-SCADA shall interface with the AECall, an application, developed by AE to support their CSR's and to capture information necessary to create a trouble call.

R[2] AECall allows a CSR to determine if a customer is involved in an outage, provide the customer with status information regarding the outage and capture new outage information.

R[3] New trouble call records are to be used by ADMS-SCADA in outage analysis.

R[4] In addition to capturing trouble call information entered by the CSR, AECall is also used as the mechanism to capture trouble call information captured by the TFC IVR.

R[5] The following are high level flows of information that need to go to/from the ADMS-SCADA and AECall:

R[5.A] The Vendor shall provide APIs to allow AECall to insert new trouble call into ADMS-SCADA. This includes all calls received by AE through the IVR, and trouble call information entered into AECall by customer service representatives.

R[5.B] The Vendor shall provide an API to allow AECall to query and determine if an individual customer is involved in an outage. If the customer is part of an existing outage, the information to be returned shall include:

R[5.B.i] Initial outage time

R[5.B.ii] confirmed outage status

R[5.B.iii] crew dispatched information

R[5.B.iv] cause of outage

R[5.B.v] estimated restoration time

R[5.B.vi] Number of customers affected

R[5.B.vii] The number of times the customer has been part of an outage for a given date range (configurable)

R[5.B.viii] Detail regarding past outages that the customer called in on (differentiating between outages they called in on, and being involved in outages they did not call in on)

R[5.C] the Vendor shall provide an API to send AECall individual outage customer calls that have been resolved

13.5.5 AMDS from/to Storm Center

R[1] Storm Center is a web-based application developed by iFactor Consulting that allows AE's customers to directly view and enter outage information using the internet.

R[2] Storm Center provides the following functionality:

R[2.A] View general outage information

R[2.B] Enter a new outage Trouble Call

R[2.C] Access current status of their outage.

R[3] The trouble call information entered via Storm Center shall be used by ADMS-SCADA for outage prediction.

R[4] The following are high level flows of information that need to go to/from the ADMS-SCADA and AECall:

R[4.A] The Vendor shall provide an API to allow Storm Center to query ADMS-SCADA for overall status information that it may display on a map of the AE territory. This information will include:

R[4.A.i] The location of all outages within the extent requested

R[4.A.ii] The size of each outage within the extent requested

R[4.A.iii] The ADMS-SCADA shall provide APIs to allow AECall to insert new trouble call into ADMS-SCADA

R[4.A.iv] The ADMS-SCADA shall allow AECall to query and to determine if an individual customer is involved in an outage.

R[4.A.iv.a] Information to be provided includes: confirmed outage status, crew dispatched information, cause of outage, and the estimated restoration time

R[4.B] The Vendor shall provide an API to allow AECall to send Trouble Call information to ADMS-SCADA. ADMS-SCADA will incorporate this Trouble Call in outage analysis.

R[4.C] The Vendor shall provide an API to allow Storm Center to query the outage status for a given customer and determine if they are involved in an outage.

R[4.D] If the customer is part of an existing outage, the information to be returned shall include:

R[4.D.i] Initial outage time

R[4.D.ii] Confirmed outage status

R[4.D.iii] Crew dispatched information

R[4.D.iv] Estimated time of restoration

R[4.D.v] Cause of the outage

R[4.D.vi] Number of customers affected

13.5.6 ADMS-SCADA from/to AMI Interface

R[1] The system shall be able to acquire and use data from the AE hosted L+G server located in Kansas City.

R[2] The system shall provide a mechanism to obtain voltage readings, load readings last gasp, and restoration status from the Operator workstation and display the returned status visually for the Operators on the geographic and schematic displays.

13.5.7 AMDS from/to WMS Interface (Requirement for future use)

R[1] There will be an interface between the ADMS-SCADA and existing Work Management System (WMS) to create work orders for follow-up work from an outage, such as additional investigative work, clean-up, broken pole replacement, tree trimming, service and meter re-attachment.

13.5.8 ADMS-SCADA from/to MWM Interface (Requirement for future use)

R[1] The ADMS-SCADA shall include an interface between the ADMS-SCADA and the existing Mobile Workforce Management (MWM) Systems.

R[2] The interface will allow passing of outage condition and status information from the field to the ADMS-SCADA, as well as provide the capability to dispatch crews and individuals to outage locations.

R[3] The interface shall also support the transmission of Trouble Orders to a mobile crew and geographic maps indicating the location of the outage/work.

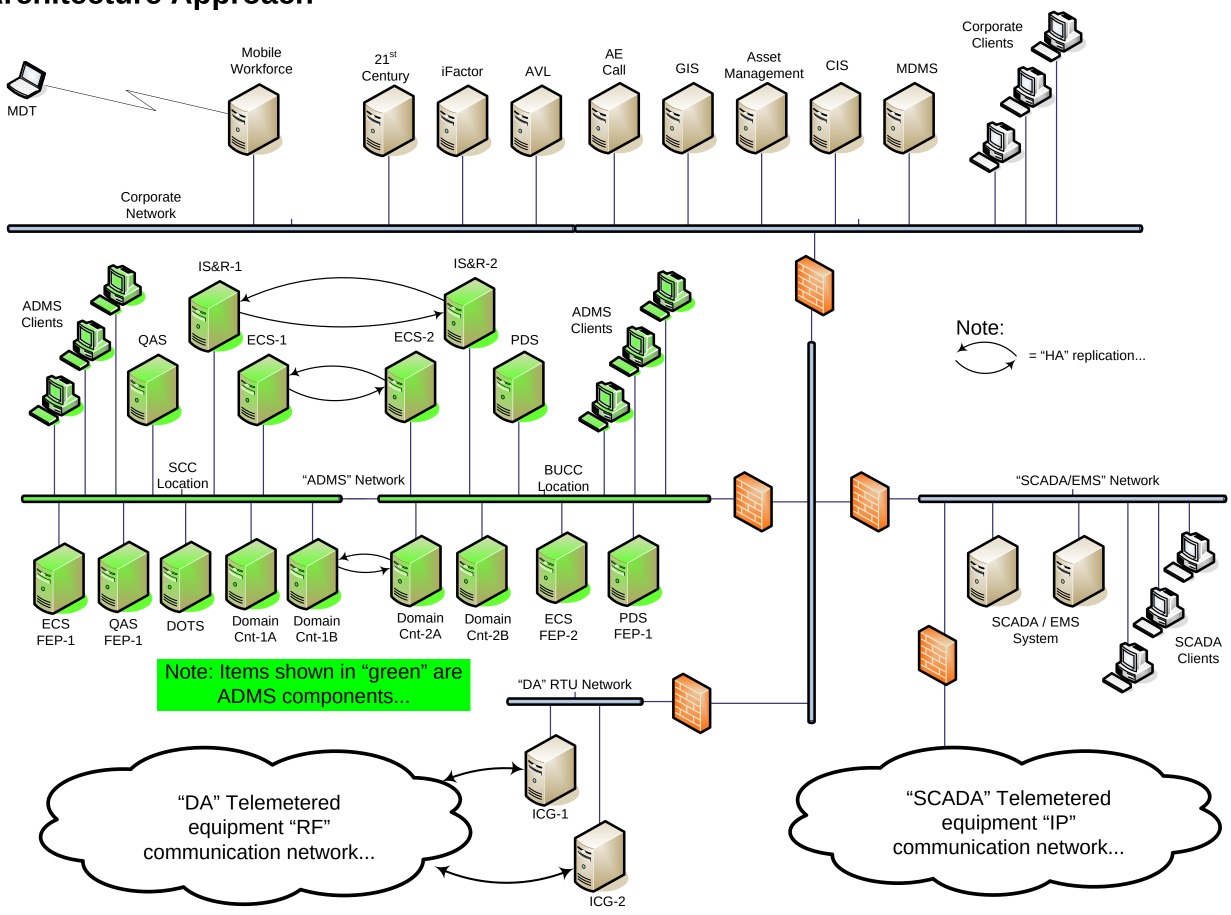
13.6 Integration Architecture Approach

R[1] In order to implement the ADMS-SCADA and support the integration needs of AE, the Vendor shall use a standards-based, CIM-compliant Enterprise Integration Bus (EIB) using a message bus concept or similar data-transfer mechanism.

R[2] The message bus architecture shall be seen as a virtual rather than physical entity. In the ADMS-SCADA project, the integration of different systems shall be achieved by passing information among systems and processing the exchanged information to provide seamless data integration across platforms and application environments.

An overview of this requirement is shown below and shall be based on standards or de-facto standards as far as possible.

Exhibit 13-1: Integration Architecture Approach



R[3] The main objective of AE is to develop an architecture that will be easily expandable to accommodate new requirements and/or systems in the future while maintaining the high `performance and availability required from the ADMS-SCADA.

13.6.1 Application Programming Interfaces (APIs).

R[1] Application Programming Interfaces (APIs) shall be provided by the Vendor to support the communication with other system components.

R[2] The APIs shall facilitate the integration of other Applications into the ADMS-SCADA environment.

R[3] APIs shall be considered as active elements in that they are subject to change in the future as new standards are defined and future releases of the software shall conform to the standards.

R[4] A point-to-point architecture approach whereby the ADMS-SCADA would be interfaced with AE's existing and future enterprise-wide systems is not acceptable to AE.

R[5] This is because changing, replacing and/or upgrading one or several applications and/or subsystem(s) could potentially impact all the other applications and/or subsystem(s).

R[6] Rather, the ADMS-SCADA interfaces with other AE's systems shall be predicated on message-bus architecture.

R[7] In the message-bus system, only the specific API that interfaces an application to the message bus would need to be changed when the application changes. Furthermore, the use of the message-bus technology facilitates the use of a single API per application or system.

R[8] The Vendor shall provide all software code, licenses (if any) and related documentation to AE.

13.6.2 Transport Mechanism

R[1] The transport mechanism for interfaces shall employ a request-and-reply model, whereby an application sends a suitable notification message to the message bus every time it has new or updated data.

R[2] In response, the ADMS-SCADA shall request the data that has changed and retrieve it from the source via dedicated transport mechanism.

13.6.3 Message Bus

R[1] The message-bus concept is required as an approach to AE's enterprise-wide integration and business process automation.

R[2] The Vendor shall implement an interface (or "adapter") to a message-bus product provided by a recognized third-party developer of middleware.

R[3] If the Vendor can offer interfaces to several middleware products, then AE shall be allowed to choose the middleware product that is best suited for their environment.

R[4] The solution proposed shall meet the following requirements as a minimum:

R[4.A] Based on message-oriented middleware

R[4.B] Guaranteed message delivery mechanism, e.g. persistent messaging

R[4.C] Based on Publish and Subscribe methodology

R[4.D] Availability of standardized adapters

R[4.E] Support of XML Schemas

R[4.F] Scalability of the solution

R[4.G] Support of Metadata model

R[4.H] Compliance with the most recent version of the IEC 61968 standard

Table of Contents

14. Operator Training Simulator 14-1
14.1 Outage Management/ Restoration Application (OMRA) Simulator 14-3
14.1.1 Call initiation 14-4
14.1.2 Call Creation 14-4
14.2 Control System Simulator 14-5
14.3 Scenario Builder 14-5
14.4 OTS Execution Management 14-8
14.5 Distribution System Simulator 14-9
14.6 The Operator Training Simulator model 14-10
14.6.1.1 Customer Calls Associations 14-11
14.6.1.2 SCADA Telemetry Model 14-11
14.6.2 Relay and Field Logic Modeling 14-11
14.6.3 Load Allocation Modeling 14-13
14.6.4 The Outage Management Database Model 14-13
14.6.5 The ADMS-SCADA database model. 14-14

14. Operator Training Simulator

R[1] The OTS shall mimic the actions of AE's distribution system and this Advanced Distribution Management System.

R[2] All functionality that is available in the production system will be available in the OTS.

R[3] OTS shall have the ability to be synchronized with the ADMS-SCADA at any time.

R[4] Previous ADMS-SCADA models shall be available to recreate past events.

R[5] OTS shall have the ability to download scenarios from past events, from the ADMS-SCADA and from the PI Historian.

R[6] OTS shall have the ability to interface with the ADMS-SCADA and PI using CIM.

R[7] OTS shall have the ability to interface with the EMS OTS or at the very least shall be able to mimic relevant Transmission System conditions.

The OTS shall be used for the following purposes:

R[7.A] Train AE's operating staff and other users who participate in the management and administration of the distribution system

R[7.B] Test software, applications, and database changes

R[7.C] Study configuration changes to distribution feeders

R[7.D] Develop and test operating procedures

R[7.E] Analyze past storm conditions and other distribution network disturbances

R[7.F] Create scenarios for restoration training

R[8] The Vendor shall providing pricing for functionality in the following optional groupings:

R[8.A] OTS Option 1 – Outage Restoration Training

R[8.A.i] Outage Management simulator

R[8.A.ii] Scenario builder (for outage)

R[8.A.iii] Execution management (for outage)

R[8.B] OTS Option 2 – Complete OTS

R[8.B.i] Outage Management simulator

R[8.B.ii] Scenario builder

R[8.B.iii] Execution management.

R[8.B.iv] Distribution system simulator

R[8.B.v] Control system simulator

R[9] The appropriate portions of the simulators and models as contained herein will be included in the associated options to support the necessary functionality.

R[10] All of these functions shall be integrated and work in concert to accurately represent the real world environment.

R[11] The OTS shall support its operation from two perspectives as defined in this section:

R[11.A] *Trainer* – an ADMS-SCADA user responsible for development of training scenarios, supervision and presentation of training exercises, and maintenance of the OTS

R[11.B] *Student* – an ADMS-SCADA user or users normally assigned to operate the distribution network.

R[12] While making distinctions between functions used by trainers and students, there is no intent to require access controls for trainer functionality beyond that required by Section 3.

R[13] The distinction is made solely to better describe the required functionality.

14.1 Outage Management/ Restoration Application (OMRA) Simulator

R[1] The control system simulator shall be a replica of the ADMS-SCADA functions and User Interface components of the ADMS-SCADA (as described in Sections 4 and 13)

R[1] The OMRA Simulator shall support a simulation environment as a training facility for AE's operating staff and other field supervisors that participate in the management and administration of trouble calls associated with customer outages.

R[2] Functions the trainee shall perform include taking ownership of an outage, dispatching crews, performing switching operations, installing and removing jumpers and closing outage orders.

R[3] In addition, the OMRA simulation mode shall be used as an analysis tool for replaying historical OMRA events, including trouble calls, Operator data entries, crew assignments and active outages, in a time-sequenced simulation.

R[4] The simulation shall operate with an overall user performance that is consistent with real-time operations.

R[5] The OMRA Simulator will send simulated outage calls to the ADMS-SCADA.

R[6] This information will be the foundation for predicting outages within the system.

R[7] Sets of calls will grouped to form scenarios.

R[8] These scenarios will be used to simulate multiple concurrent outage events.

R[9] The system will allow an individual (typically a trainer) to in near real-time indicate which scenario should be executed and when.

R[10] Scenarios may be grouped to allow concurrent execution of a number of events. This will allow creation of similar outages in the variously assigned areas of responsibility.

R[11] The OMRA Simulator will have the ability to reset the system back to normal (device state, customer calls, outages…)

R[12] Under OTS Option 2, the OMRA Simulator will work with the Control System Simulator and the Distribution System Simulator to emulate operation of the complete ADMS-SCADA. This will include the use of external telemetry as well as advanced ADMS-SCADA functions such as DPF and FISR.

14.1.1 Call initiation

R[1] The OMRA model will have the ability to generate calls that are associated with customers connected to the distribution system.

R[2] Ability to simulate last gasp calls with various traffic volumes and multiple origination circuits

R[3] These calls will be used in predicting outage location and the device that operated. The Customer Calls Model will include:

R[3.A] Calls associated with customers to be used in the following ways

R[3.A.i] Triggered when part of an outage caused by the operation of an ADMS-SCADA device (in real time or with the outage scenario builder)

R[3.A.ii] Loaded into a queue to be used by outage prediction engine to identify the outage location

R[3.B] Scenario based groups of calls that may be sent to the OMRA to drive sets of outages

14.1.2 Call Creation

R[1] The OMRA Simulator will allow the trainer to create a new trouble call to be used in training outage scenarios.

R[2] Calls shall be created via a point and click approach, interacting with the customer representations on the screen. A mechanism shall be included to select multiple customers and create multiple calls at a time from the screen.

R[3] The system shall also provide the ability to load calls from an external database, facilitating the replaying of a prior outage event.

14.2 Control System Simulator

R[1] The control system simulator shall be a replica of the ADMS-SCADA functions and User Interface components of the ADMS-SCADA (as described in Sections 4 and 13) with the following exceptions:

R[1.A] The data acquisition functionality shall be simulated by the distribution system simulation (Section 14.5).

R[1.A.i] Telemetered data shall appear to the student to be originating from the same data source as in the real-time Production system.

R[1.B] The IS&R functionality shall be supported to the extent required for scenario replay (Section 7).

R[2] The control system simulator shall reproduce the operation of all ADMS-SCADA functionality, except as described above.

R[3] The required functionality specifically includes the following items:

R[3.A] Supervisory control, including tags.

R[3.A.i] Where a supervisory control is linked to a switching device in the distribution system model, the distribution system simulator shall reflect the change in network topology from a control action.

R[3.A.ii] Where the supervisory control is linked to a device not in the distribution system model, the control action shall change the state of the value.

R[3.B] Data entry.

R[4] Any workstation shall be able to be used for training.

14.3 Scenario Builder

R[1] An OTS scenario shall represent the system activity to be simulated over the course of a training session.

R[2] A scenario shall include the initial state of the distribution system and control system simulators, load allocation modeling, and events that occur over the duration of the scenario.

R[3] OTS shall have the ability to capture snap shots from the ADMS-SCADA and from PI historian.

R[4] OTS shall have the ability to import and export CIM files.

R[5] OTS scenarios shall be managed in a similar manner as and work with save cases as defined in Section 13.5, Study Mode.

R[6] The trainer will have the ability to begin a particular scenario to initiate similar events in multiple Areas of Control for the students.

R[7] Scenario "building" (definition or modification) shall be possible while another scenario is being executed.

R[8] Scenario building shall include the following activities:

R[8.A] Setup of execution parameters, including simulation time

R[8.B] Setup of the initial conditions.

R[8.B.i] Initial conditions may be set by copying another scenario, by importing a distribution power flow save case, or by retrieving power system measurements for a specified time and date from the Historian.

R[8.B.i.a] Data retrieved from the Historian shall be processed by the distribution power flow function to produce valid initial conditions.

R[8.B.ii] Initial condition data not available from power flow save cases or Historian shall be manually entered by the trainer.

R[8.C] Definition of the feeder load profiles

R[8.D] Definition of events.

R[8.D.i] An event shall be defined by specifying the event type (see below), one or more distribution system devices or control system elements on which the event is to act, and a time (in simulation time) for the event.

R[8.D.ii] Where an event is to act on a power system device, the trainer shall be able to select the device from any one-line or tabular display containing the device.

R[8.D.iii] For Outage Management simulation, events will generate calls from affected customers.

R[8.D.iv] Sets of call captured during an actual event may be used as basis for creating an Outage Management event.

R[9] Event types shall include at least the following items:

R[9.A] Switching device operations, both single operations (such as trip or close) and multiple operations (such as trip/close).

R[9.A.i] For multiple operations, each simulated operation (such as trip and close) shall be reported to the control system model to ensure that actions that are triggered by the operation of the device will occur.

R[9.B] Changes in the state of status points

R[9.C] Changes in the value of analog points not defined in the distribution system model

R[9.D] Changes in the value of analog points defined in the distribution system model.

R[9.D.i] The changed value shall override the value provided by the distribution system simulator.

R[9.E] Changes in the state of relay and field logic enable/disable flags. (This can be used to simulate failure of devices to operate.)

R[9.F] Single load changes. Load changes shall override load values set by the load allocation simulation.

R[9.G] Change in generator unit output for a distributed generation source connected to the modeled low-voltage or medium-voltage network.

R[9.H] Single-phase and multiple-phase outages along a feeder.

R[9.I] New outage calls

R[9.J] New non-outage (in-service) trouble calls.

R[9.K] Occurrence of a momentary or sustained fault (simulated by relay operation acting on circuit breakers).

R[9.K.i] Reclose operations where the reclose time is less than the simulation periodicity shall be simulated as occurring over consecutive cycles.

R[9.L] Loss of telemetry from a data source. (Data sources are defined in Section 6.1, Data Acquisition.

14.4 OTS Execution Management

R[1] OTS execution management features shall facilitate execution and management of scenarios and interaction between the student and the trainer, including the following actions:

R[1.A] Initialize the OTS simulation to a scenario

R[1.B] Start the simulation at any time within the scenario

R[1.C] Stop the simulation at any time within the scenario

R[1.D] Pause the training sequence at any time within the scenario and resume the simulation

R[1.E] Generate a snapshot of the simulation.

R[1.E.i] The snapshot shall include sufficient information so that the simulation can be returned to that point in the scenario and simulation resumed.

R[1.F] Control the speed (periodicity) of simulation, from step-on-demand, through normal simulation speed, through fast (where the simulation is executed as quickly as possible)

R[1.G] Generate events (Section 14.3) spontaneously, without creating a scenario entry.

R[2] All scenario events, trainer actions, and student actions (excluding actions such as display callups, window sizing, and study application executions) shall be recorded in the scenario.

R[3] The capability to replay a scenario shall be provided, including the capability to pause, fast forward, and rewind the scenario, including trainer and student actions, beginning at the start of the scenario or from any point within the scenario.

14.5 Distribution System Simulator

R[1] The OTS simulation shall be executed for the distribution network, including the bulk power source points.

R[2] The OTS distribution system simulator will have the ability to work with the Outage Management Simulator and the Control System Simulator, allowing analyzing circuit conditions during restoration.

R[3] The OTS shall have the ability to be driven in steps as well as in continuous mode.

R[4] The distribution system simulator shall reproduce the operation of the distribution network in a discrete time-step manner (as opposed to a continuous manner).

R[5] At each time step, the simulation shall produce a complete unbalanced, three-phase distribution network solution, with voltages and flows at each network node.

R[6] The distribution system simulator shall be able to solve parallel, looped, and meshed circuits as defined in the Distribution Operations model.

R[7] On-demand executions shall be performed for an Operator-assigned area of the distribution network when triggered by an event (e.g., whenever a change in topology or pre-defined change in status or analog data occurs).

R[8] The voltage and flow solution shall be passed to the control system simulator as a simulation of telemetered data.

R[9] The power system simulation shall produce a valid result for the following conditions:

R[9.A] Operation of the distribution system with multiple isolated feeder segments that might contain low-voltage generation facilities as well as loads.

R[9.B] Pick-up of de-energized feeders.

R[10] For data included in the ADMS-SCADA database model, but not included in the Distribution Operations model, facilities for the trainer to simulate telemetry by changing the value or attributes of a point shall be provided.

R[11] The distribution network shall be simulated in the OTS, with the definition of the distribution system derived from the OTS model components.

14.6 The Operator Training Simulator model

R[1] This OTS database component shall include all distribution network information necessary to model the dynamics of the distribution system that are not used by the real-time ADMS-SCADA functions.

R[2] The OTS shall have the ability to copy current ADMS-SCADA configuration.

R[3] Except for temporary grounds, jumpers, and circuit cuts that might be added during a training session, the Distribution System Operations Model in OTS shall be identical to the source DSOM of the real-time Production System as defined in Section 13.2, Distribution System Operations Model.

R[4] The OTS model shall include all busses, feeders, loads, and network devices defined in the source DSOM.

R[5] Changes to the source DSOM made for any ADMS-SCADA function shall also be automatically made to the OTS Distribution Operations model.

R[6] The Outage Management OTS model shall include all active elements defined in the source DSOM.

R[7] This OTS database component shall include all the information necessary to model the inputs that drive the behavior of the ADMS-SCADA Outage Management functions.

R[8] The OTS shall include the ability to randomly simulate load and events previously defined by the instructor in a realistic manner.

R[9] In addition to recording all trainee operations, the OTS shall measure its response time and file them for purposes of evaluation and benchmarking.

14.6.1.1 Customer Calls Associations

R[1] The Outage Management OTS model will contain the elements necessary to generate calls that are associated with customers connected to the distribution system.

R[2] These calls will be used in predicting outage location and the device that operated.

R[3] The Customer Calls Model will include:

R[3.A] Calls associated with customers to be used in the following ways

R[3.A.i] These will be triggered when affected by an outage when the ADMS-SCADA operates a device (in real time or with the outage scenario builder

R[3.A.ii] Loaded into a queue to be used by outage prediction engine to identify the outage location

R[3.B] Scenario based groups of calls that may be sent to the Outage Management OTS to drive sets of outages

14.6.1.2 SCADA Telemetry Model

R[1] Scenario based groups of trip signals that may be sent to the Outage Management OTS to drive outage prediction

14.6.2 Relay and Field Logic Modeling

R[1] The OTS shall simulate the following types of relays and field logic:

R[1.A] Overcurrent relays

R[1.B] Overvoltage relays

R[1.C] Undervoltage relays

R[1.D] Overfrequency relays

R[1.E] Underfrequency relays

R[1.F] Synchronism check relays

R[1.G] Recloser relays, with up to three reclose actions

R[1.H] Transfer tripping

R[1.I] Relay lockout

R[1.J] Load tap changers, voltage regulators, capacitor banks and controllers (including operating constraints).

R[2] Each relay and field device shall be modeled with an enable/disable flag.

R[3] When set to disable, the relay or device shall not operate.

R[4] When set to enable, the relay or device shall operate as normal.

R[5] Selected relays devices may be implemented for supervisory control of the enable/disable flag.

R[6] For those devices, the OTS shall link the supervisory control command to the enable/disable flag.

R[7] Selected underfrequency and lockout relays shall include a reset feature.

R[8] When implemented, the reset feature shall be linked to a supervisory control point in the control system simulator.

R[9] The relay shall inhibit operation of the switching device it controls until the student operates the reset supervisory control.

R[10] Except as described above, no other field logic such as special protection schemes shall be modeled in the OTS.

14.6.3 Load Allocation Modeling

R[1] Distribution feeder loads shall be modeled for conforming and non-conforming loads using predefined daily area load profiles.

R[1.A] Sets of daily load profiles for 24 hourly periods are required based on load type (e.g., small & large commercial, residential, industrial) as a function of both day types and seasons.

R[1.B] The real and reactive components of each load profile shall be specified independently as functions of time, day type, and season.

R[1.C] The load profiles shall be selectable through displays.

R[1.D] The trainer shall be able to modify the load by entering individual load values or by applying a scale factor to the entire load profile.

R[2] Each conforming feeder load shall be scaled as a function of transformer capacity or, if available, monthly KWh usage.

R[2.A] Where a switching device operation results in the disconnection of load from the feeder circuit that load shall not be reallocated among the other connected loads.

R[2.B] Each modeled load shall include features to simulate changes in the load due to changes in voltage.

R[2.C] Individual loads on a feeder that are telemetered shall be linked to the control system simulator (Section 10.2).

14.6.4 The Outage Management Database Model

R[1] This OTS Outage Management Database component shall include all ADMS-SCADA database objects and their attributes.

R[2] This includes operational devices such as breakers, reclosers, sectionalizers, fuses and transformers. It also includes all switchable devices such as switches and regulators.

R[3] The Outage Management database model shall be populated by the Control System Simulator described in Section 14.2.

R[4] Changes to the ADMS-SCADA production database model shall be carried to the OTS without requiring the changes to be redefined on the OTS.

R[5] The OM database model can be refreshed from the production database upon request.

R[5.A] Calls – associated with devices on the distribution system.

R[5.B] Outage Scenario – Allow sets of calls and device telemetry

R[5.C] Scenario grouping – Allows execution of multiple scenarios

14.6.5 The ADMS-SCADA database model.

R[1] This OTS database component shall include all ADMS-SCADA database objects and their attributes, whether or not these objects are linked to Distribution Operations model (e.g., field device control status, calculation results).

R[2] The ADMS-SCADA OTS database model shall be populated by the Control System Simulator described in Section 14.2.

R[3] Changes to the ADMS-SCADA database model shall be carried to the OTS without requiring the changes to be redefined on the OTS.

Table of Contents

A. Glossary A-1

A. Glossary

This document is intended to provide clarification to Acronyms and terms found in the RFP, and is not intended to describe any functional requirements.

ADMS-SCADA	AE defines the ADMS-SCADA as a single integrated system that shares a common database and performs traditional DMS functions, newer/advanced applications, Outage Management functions and traditional EMS or SCADA functions
AECall	An application developed by AE that is used by customer service to enter customer outage calls and sends them to the ADMS-SCADA. It also captures calls from IVR and Storm Center
AMI	Advanced Metering Infrastructure
AMR	Automatic Meter Reading
ANSI	American National Standards Institute
API	Application Program Interface
AOC	Award of Contract
AOR	Area of responsibility – the specific geographic area for which an operator has responsibility for monitoring, switching, controlling devices, managing outages and dispatching crews. AOR's are hierarchical in nature based on boundary areas. A boundary can be a small as a single device, or made up of multiple devices as grouped by geography (e.g. group of zip codes) or grouped by electrical network characteristics (e.g. group of feeders).
ASAI	Average System Availability Index
ASU	Automatic Sectionalizing Unit
ATO	Automatic Throw-Over

AVL	Automatic Vehicle Locator
AVLS	Automatic Vehicle Location System
BIM	Business Intelligence Model
Blue Sky Day	Terminology used to describe a normal day in the control room with regard to call and job volumes.
BUCC	Back-Up Control Center
BW	Bandwidth
CA	Consumer Advocates
CAI	Computer Aided Instruction
CAIDI	Customer Average Interruption Duration Index
CAIFI	Customer Average Interruption Frequency Index
CBK	Callback – AE will call a customer to ensure power has been restored
CBT	Computer Based Training
CL	Critical Load Customer
CCAPI	Control Center API
CCM	Critical Customer Management
CE	Control Engineering (SCADA group)
CIM	Common Information Model
CIP's	Critical Infrastructure Protection
CIS	Customer Information System

CM	Crew Management
Commercial Use	The period of time when AE begins to use the new DMS/OMS as the main primary system for operation of the electrical distribution system and ceases parallel operation and/or a potential fallback plan to the older systems
Confidence Testing	A limited test (checklist level test) on hardware and/or software to make sure it functions properly upon initial set up and installation
Cover Sheet	A portion of the switching order that contains general information about the details of a switching order. The Cover Sheet is a special type of Section that does not require its own approval(s). The primary source of most of the cover sheet information is AE's TOA application.
Console	The Operator's work location which includes the desk, ADMS-SCADA Workstation and other equipment such as a Corporate PC, telephone and radio system.
CR	Control Room
CR	Consumer Representative
CS	Customer Systems
CSS	Customer Service Systems
CSR	Customer Service Representative
DBA	Database Administrator
DCFL	Distribution Circuit Fault location
DDS	Data Distribution Service
Design Specification	

DHS-NICC	US Department of Homeland Security National Infrastructure Coordination Center
Display	A window that contains application specific information such as tabular data, data entry screens, schematic or geographical map information
DMS	Distribution Management System
DMZ	Demilitarized Zone
DPF	Distribution Power Flow
DSOM	Distribution System Operations Model
DST	Daylight Saving Time
EAI	Enterprise Application Integration
ECC	Energy Control Center
ECS	Energy Control System. When the term ECS is alone, it references both Prod1 and Prod 2.
ECS Prod 1, ECS Prod 2	Rather than have a primary and a backup control system, AE will be deploying two (2) control system (Prod 1 and 2), each with full capability. AE will alternate operations between the two systems on a regular basis, with the other acting as a backup control system.
EIA	Electronic Industries Association
EIB	Enterprise Integration Bus
EMS	Energy Management System
EPRI	Electric Power Research Institute
ESB	Enterprise Service Bus
ES-IAC	Electricity Sector Information Sharing and Analysis Center

EST	Eastern Standard Time
ETA	Estimated Time of Arrival
ETL -	Extract, transform, and load (ETL) in database usage and especially in data warehousing involves: • Extracting data from outside sources • Transforming it to fit operational needs (which can include quality levels) • Loading it into the end target (database or data warehouse)
ETOR	Estimated time of Restoration
ETR	Estimated Time of Restoration
ESP	Electronic Security Perimeter
FAT	Factory Acceptance Testing
FBI	Federal Bureau of Investigation
FDS	Functional Design Specification
Feeder Name	This field represents the utilities designation, either number or name of the feeder.
FEP	Front-End Processor
FISR	Fault Isolation and Service Restoration
FS	Functional Specification
FTP	File Transfer Protocol
Gazetteer	A geographic query tool that supplies attribute, location and coordinate information for sets of objetcs that meet a praticular criteria.
GIS	Geographical Information System
GLBP	Gateway Load Balancing Protocol

Go-back Order	Related to switching orders. A user initiated function in Switching Order Management to automatically generate the Go-back Switching Steps needed to reverse a switching order.
Go-back Switching Steps	Related to switching orders. Steps that reverse the order and operation of switching step entries in the switching order and change each of the "reversible" entries to its opposite. For example, an entry CLOSEBREAKER shall be reversed to OPEN BREAKER, an entry PLACE TAG shall be reversed to REMOVE TAG.
GPS	Global Positioning Satellite
GUI	Graphical User Interface
Header	A portion of a Switching Order Section. The header contains a sub-set of the information fields from the Cover Sheet and appears on the top of each page in the printed version of the Switching Order Section and on the switching order window in the OMI.
HIDS	Host-based Intrusion Detection System HMI – Human Machine Interface
Historian	Historical data storage system that uses compression techniques for storing large volumes of time-series data (similar to OSI Soft PI Historian)
HTML	Hyper Text Markup Language
IBM MQ	IBM Message Queue
ICCP	Inter-Control Center Communications Protocol
ID	Identifier
IDS	Intrusion Detection Software/System
IEC	International Electro-technical Commission
IED	Intelligent Electronic Device

IEEE	Institute of Electrical and Electronics Engineers
IHM	Independent Health Monitor
Increased Activity Day	A term used to describe an increased level of call and job volumes in the control room typically caused by weather or unusual system events.
Instance	Refers to one active session of the ADMS-SCADA application running on a workstation.
IOS	Internetwork Operating System
IP	Internet Protocol
IS	Information Services
IS	In Service. A non-outage trouble call.
ISMS	Information Security Management Standards
IT	Information Technology
IT	Information Technology support group
IS&R	Information Storage and Retrieval
ITU	International Telecommunications Union
IU	Incremental Update
IVR	Interactive Voice Response
JCAPS	Java Composite Application Platform Suite
KC	Key Call
KV	Kilovolt
KVA	Kilovolt-Ampere

KVAR	Kilovolt-Ampere Reactive
KVARH	Kilovolt-Ampere Reactive Hour
KVM	Keyboard, video, mouse
KWH	Kilowatt hour
LA	Load Allocation
LAN	Local Area Network
LB	Load Break
LCD	Liquid Crystal Display
Line Unloading	A DMS application that can recommend switching actions required to relieve a specified amount of load from a feeder and transfer it to adjacent feeders.
LI	Long Island
LS	Life Support
LSA	Life Support Apparatus
LSCA	Life Support Customer Management
LTC	Load Tap Changing Transformer
Macro	Related to switching steps – A macro is used to automatically expand out the full text of a switching step into a standard phraseology used by AE. The macro shall combine the equipment name, location and actions to be taken into the same field on the switch order step.
MAIFI	Momentary Average Interruption Frequency Index
*Materialized View	A materialized view is a database object that contains the results of a query. They are local copies of data located remotely, or are used to

	create summary tables based on aggregations of a table's data.
Monitor	An individual LCD display that makes up display capability of an Operator's console.
MPLS	Multiprotocol Label Switching
MQ	IBM MQ IBM Message Queue
MSSP	Managed Security Services Provider
MWM	Mobile Workforce Management
NA	Network Applications
NCC	Non-Customer Call
NEMA	National Electrical Manufacturers Association
NERC	North American Electric Reliability Corporation
AE	Austin Energy
NIDS	Network Intrusion Detection Scanner
NM	Network Manager
NMDMS	Network Manager DMS
NS	No Service (in section 16) An outage call or job.
ODBC	Open Database Connectivity
OE	Outage Engine
OEM	Original Equipment Manufacturer
OM	Outage Management
OMI	Operations Manager Interface

OMS	Outage Management System
Operator	The primary user of the NM-DMS working in the Control Room.
OS	Operating System
OTS	Operator Training Simulator
PDF	Portable Document Format
PDS	Program Development System
PF	Power Flow
PGP	Pretty Good Privacy
PI	Plant Information system from OSISoft. (PI Historian)
PIN	Personal Identification Number
POSIX	Portable Operating System Interface
PREMGF	Pre-Master Generator File
	PPS Primary Production System platform (PPS) .
Pre-FAT	Preliminary Factory Acceptance Testing
PSIM	SCADA Process Simulator Module
QA	Quality Assurance
QAS	Quality Assurance System
RAC	Real Application Cluster (Oracle) – Oracle RAC allows multiple computers to run Oracle RDBMS software simultaneously while accessing a single database, thus providing a clustered database.
RDBMS	Relational DataBase Management System

RF	Radio Frequency
RFI	Request For Information Document
RFP	Request for Proposal Document
RMAN	(Recovery Manager) is a backup and recovery manager supplied for Oracle databases
RMON	Resource Network Monitoring
RSA	Restoration Switching Analysis
RTDB	Real-Time Database
RTU	Remote Terminal Unit - With technology advancements, other devices have taken on functions traditionally performed by an RTU. For the purposes of this report, AE will use the term RTU to indicate this expanded group of devices such as data concentrators or any DNP slave device.
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
SAN	Storage Area Network
SAT	Site Acceptance Testing
SCADA	Supervisory Control and Data Acquisition
SCC	System Control Center
SCDB	SCADA Database
SDB	Source Data Base
SE	State Estimator

SE	System Engineering - Super Users, Will Perform load flows, provide ADMS-SCADA support
Sections	Related to switching orders – an organizational subset of the switching order that groups related switching steps together and includes the Header. For instance: Takeout (Switch Out), Restore (Return) Sections of a switching order can be individually approved. The Cover Sheet is a special type of Section that does not require its own approvals and does not require the Header.
Slave-device	Any device that may be controlled via the ADMS-SCADA. This would include RTU's and devices that Smart Comment Step – Related to switching orders – pseudo operations that may be defined for network objects that do not actually affect the network connectivity. These may be used, for example, to quickly enter steps to instruct personnel to perform some check on the network object.
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SOE	Sequence of Events
SQL	Structured Query Language
Storm Center	A web-based tool developed by iFactor Consulting that allows external customers to enter outage information and query current outage status.
SSH	Secure Shell
SSL	Secure Sockets Layer
SW	Switch

Switching Actions	Recommendations made by DMS applications such as RSA and line unloading that will recommend a sequence of actions that will isolate, isolate and restore the un-faulted portion of the feeder, or transfer a portion of load. Switching actions are turned into Switching Steps and incorporated into a Switching Order by a manual Operator initiated process “Save to Switching Plan”.
Switching Order	Also known as “Switching Plan”. A list of operations to be directed by the Operator when carrying out a procedure for switching elements of the power system. Switching orders contain a Cover Sheet and one or more Sections.
Switching Step(s)	One or more independent and sequential switching operations that make up a Switching Order. Typically used to instruct field personnel to perform a specific switching operation on a specific device at a specific location. Steps include the following fields: Substation, Feeder Name, device type, device name and location, detailed action to be taken, person that was instructed to perform the action, date and time action instructed, date and time executed, and free form comments.
Switching Template	Any Switching Order that is saved for future re-use in a directory structure within the Switching Order Management function of the DMS. Templates can either be Generic or Equipment Specific.
TASE.2	Telecontrol Application Service Element protocol – also known as ICCP
TBD	To Be Determined
TBP	To Be Provided
Template (equipment specific)	A switching template which contains the switching steps for operating on a piece of equipment that is device and location specific. For instance, an equipment specific template may be associated with a specific circuit breaker (device type
Template (generic)	A switching template that is associated with a specific device type that contains the switching steps for that device type and allows the user to enter the equipment ID. A generic template may be used more than once

	in a switching order. For instance, a generic template may exist for Device types such as Load Break Switches, or Network Protectors.
TOA	Transmission Outage Application (AE Application)
TFCC	Twenty First Century Communications – IVR service employed by AE
Trouble Call	Refers to the record created when a customer contacts AE to report a problem or an outage. This may have been captured by a CIS report or entered directly into Storm Center. Information included in the trouble call record may include customer name, street, address, phone number, account number, complaint type, and comments. The term may also refer to the phone call placed by the customer to report a problem.
Trouble Order	Refers to a record to which one or more Trouble Calls may be associated. It is the Trouble Order which is managed by the dispatcher by evaluating the situation, assigning a trouble shooter, and capturing completion information.
Trouble Shooters	First responders to outage events. They patrol the line, locate the problem and perform minor (<1 hr) repairs
TS	Test Specification
UBLF	Unbalanced Load Flow
UDW	Utility Data Warehouse
UI	User Interface
UID	User Identification
USSS	US Secret Service
UTC	Universal Time Coordinated
Vac	Voltage AC
VAR	Volt-Ampere Reactive.

VCB	Vacuum Circuit Breaker),
Verification Testing	Testing that is used when an additional system is being configured based on the same hardware and software platform(s) as another system that has already been through FAT. (e.g. Once the NE System has passed FAT, the NY system can undergo verification testing with the NY network model database)
VPN	Virtual Private Network
WAN	Wide Area Network
WMS	Work Management System
Workstation	The primary computer equipment used by the operator to run ADMS-SCADA. It will consist of multiple monitors, the CPU, the keyboard and mouse. The keyboard and mouse are shared between all monitors at the console.
WSDL	Web Service Definition Language
XML	Extensible Markup Language
XSD	XML Schema Definition Language